Erreurs de configuration d'un Windows supervisé pour le pack windows-by-WinRM__shinken

Sommaire

Contexte

Vous retrouverez dans cette page les erreurs rencontrées lors de la **configuration d'un Windows supervisé** pour le pack `windows-by-WinRM__shinken` : exécution du script, service WinRM, compte de supervision, permissions et Active Directory.

> Pour les erreurs remontées par les **checks** une fois la supervision en place (*Transport error*, *Authentication failed*, *AccessDenied*...), consultez la page Erreurs du pack windows-by-WinRM__shinken.

Les erreurs

Exécution du script

Impossible de charger le fichier <nom_du_script.ps1> car l'exécution de scripts est désactivée

Le script `Configure-Host.ps1` refuse de démarrer. PowerShell bloque par défaut les scripts non signés numériquement via sa stratégie d'exécution (*Execution Policy*). Aucune modification n'a été appliquée sur la machine.

```
Impossible de charger le fichier C:\<nom_du_script.ps1>, car l'exécution de scripts
est désactivée sur ce système.
    + CategoryInfo          : Erreur de sécurité : (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

Mots-clés : *UnauthorizedAccess · PSSecurityException · Execution Policy · l'exécution de scripts est désactivée · n'est pas signé numériquement*

> **Survient à l'étape :** Étape 3 — Autoriser l'exécution du script — voir Étape 3 — Autoriser l'exécution du script sur la page de configuration.

Résolution :

Autorisez l'exécution **pour la session courante uniquement** :

```
Set-ExecutionPolicy Unrestricted -Scope Process
```

> `-Scope Process` ne modifie que la fenêtre PowerShell ouverte : aucun impact persistant sur la machine, la stratégie d'origine est rétablie à la fermeture. Pour connaître la stratégie en vigueur :
>
> ```
> Get-ExecutionPolicy -List
> ```

WSManFault – Le type de connexion réseau défini sur cet ordinateur est Public

`winrm quickconfig` s'interrompt sans configurer WinRM. Windows refuse d'activer la gestion à distance tant qu'au moins une carte réseau est en profil **Public**. Le cas est fréquent sur Windows 10 et Windows 11, où une carte non identifiée bascule automatiquement dans ce profil.

```
WSManFault
    Message = Le client WinRM ne peut pas traiter la demande. Le type de connexion réseau
    défini sur cet ordinateur est Public. Dans ce type de réseau, le pare-feu bloque le
    pilote WinRM.
Error number:  -2144108183 0x80338169
```

Mots-clés : *WSManFault · 0x80338169 · -2144108183 · connexion réseau · Public · le pare-feu bloque le pilote WinRM*

> **Survient à l'étape :** Étape 4 — Lancer le script, ou B.1 en configuration manuelle — voir Prérequis sur la page de configuration.

Résolution :

Identifiez la carte concernée :

```
Get-NetConnectionProfile
```

La carte fautive est celle dont `NetworkCategory` vaut **Public** :

```
Name             : Network
InterfaceAlias   : Ethernet
InterfaceIndex   : 6
NetworkCategory  : Public
IPv4Connectivity : Internet
IPv6Connectivity : NoTraffic
```

Basculez-la en **Privé** (ou **Domaine** si la machine est jointe à un annuaire), en remplaçant le nom de l'interface :

```
Set-NetConnectionProfile -InterfaceAlias "Ethernet" -NetworkCategory Private
```

Relancez `Get-NetConnectionProfile` : `NetworkCategory` doit désormais afficher **Private**.

> Sur un serveur en production, ce changement de profil peut modifier les règles de pare-feu appliquées. Vérifiez vos politiques internes avant de le réaliser.

Service WinRM, compte et permissions

Le service WinRM est arrêté après chaque redémarrage

La supervision fonctionne, puis tous les checks de la machine tombent en erreur après un redémarrage. Sur Windows 10 et Windows 11, le service WinRM est configuré en démarrage **manuel** par défaut : il ne se relance pas tout seul.

```
Status   Name               DisplayName
------   ----               -----------
Stopped  WinRM              Gestion à distance de Windows (Gestion WS)
```

Mots-clés : *WinRM · Stopped · StartupType · Manual · connection refused · request timed out*

> **Survient à l'étape :** Prérequis — 3. Le service WinRM est actif — voir Prérequis sur la page de configuration.

Résolution :

```
Set-Service -Name WinRM -StartupType Automatic
Start-Service WinRM
Get-Service WinRM
```

Le service doit alors apparaître **Running** :

```
Status   Name               DisplayName
------   ----               -----------
Running  WinRM              Gestion à distance de Windows (Gest...
```

Côté Shinken, cette panne se manifeste par une erreur *Transport error : connection refused* ou *request timed out* sur tous les checks de l'hôte.

Le nom de groupe local spécifié est introuvable – net localgroup

L'ajout du compte de supervision au groupe *Utilisateurs de l'Analyseur de performances* échoue, alors que le nom paraît correct à l'écran. Sur un Windows en français, ce groupe s'écrit avec une **apostrophe typographique** `'` (U+2019) et **non** avec l'apostrophe droite `'` (U+0027) de la touche 4 du clavier. Retaper la commande à la main produit donc un nom que Windows ne reconnaît pas.

```
net localgroup "Utilisateurs de l'Analyseur de performances" shinken_user /ADD
L'erreur système 1376 s'est produite.

Le groupe local spécifié n'existe pas.
```

Mots-clés : *net localgroup · erreur système 1376 · Le groupe local spécifié n'existe pas · Analyseur de performances · Performance Monitor Users · apostrophe typographique · U+2019*

Survient à l'étape : B.6 — Ajouter l'utilisateur aux groupes — voir B.6 — Ajouter l'utilisateur aux groupes sur la page de configuration.

Résolution :

- Copiez-collez la commande depuis la page de configuration, dont le nom de groupe porte la bonne apostrophe, **ou**
- saisissez l'apostrophe avec **ALT + 0146** au pavé numérique — elle est différente de celle de la touche 4, **ou**
- utilisez le nom **anglais** du groupe, qui ne contient aucune apostrophe :

```
net localgroup "Performance Monitor Users" shinken_user /ADD
```

Ce piège ne concerne que les Windows en français. Les noms anglais — *Performance Monitor Users*, *Remote Management Users*, *Event Log Readers* — ne contiennent aucune apostrophe.

Pour lire le nom exact tel que Windows le stocke :

```
(Get-LocalGroup | Where-Object Name -like "*Analyseur*").Name
```

Pour vérifier l'appartenance effective du compte :

```
net user shinken_user
```

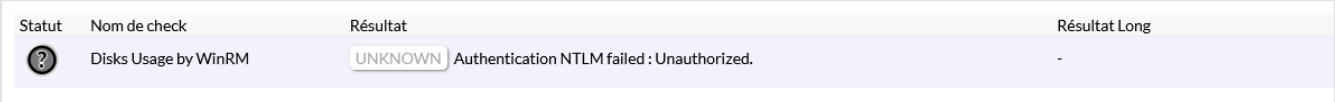
La supervision s'arrête brutalement du jour au lendemain

Tous les checks d'une machine — ou de l'ensemble du parc si le compte est partagé — passent en erreur simultanément, sans qu'aucune configuration n'ait été modifiée. Le mot de passe du compte de supervision a expiré conformément à la politique de sécurité du domaine ou de la machine.

```
UNKNOWN – Authentication NTLM failed : Unauthorized
```

Mots-clés : *Authentication failed · Unauthorized · mot de passe expiré · PasswordExpired · PasswordNeverExpires*

> **Survient à l'étape :** Étape 4 — Gérer l'expiration du mot de passe — voir Gérer l'expiration du mot de passe sur la page de configuration.



Résolution :

Vérifiez l'état du compte :

```
net user shinken_user | findstr /C:"expire"
```

Redéfinissez le mot de passe, puis empêchez son expiration :

```
$secPass = ConvertTo-SecureString "VotreMotDePasse" -AsPlainText -Force
.\Configure-Host.ps1 -UserName "shinken_user" -Password $secPass -PasswordNeverExpires
```

> Si le mot de passe est **déjà expiré**, activer `-PasswordNeverExpires` ne suffit pas à débloquer le compte : il faut **aussi** redéfinir le mot de passe. Pensez à le mettre à jour dans le Synchronizer côté Shinken.

Les permissions ne semblent pas prises en compte

Les droits viennent d'être accordés au compte de supervision, mais les checks échouent toujours avec une erreur d'accès refusé. Les jetons de connexion déjà ouverts conservent les anciennes autorisations tant que les services ne sont pas relancés.

```
UNKNOWN – Response fault error: Code: s:Sender, Subcode: w:AccessDenied
```

Mots-clés : *AccessDenied · Permission denied · accès refusé · winmgmt · WinRM · SDDL*

> **Survient à l'étape :** B.8 — Appliquer les permissions — voir B.8 — Appliquer les permissions sur la page de configuration.

Résolution :

Redémarrez les deux services concernés :

```
Restart-Service winmgmt -Force
Restart-Service WinRM -Force
```

> Si l'erreur persiste, patientez quelques minutes ou redémarrez la machine : certains jetons ne sont libérés qu'à l'expiration de leur cache. En Active Directory, laissez également le temps à la réplication de se propager entre contrôleurs de domaine.

Active Directory

Le conteneur cible « CN=Users » est inaccessible – création d'OU impossible

Le script s'arrête au moment de créer l'unité d'organisation dédiée « Shinken supervision users ». Le paramètre `-OUPath` pointe vers `CN=Users`, qui est un **conteneur** et non une unité d'organisation : Active Directory interdit d'y créer une OU.

```
[KO] Compte et groupe AD : Erreur : Impossible de créer l'OU 'Shinken supervision users' sous 'CN=Users,
DC=exemple,DC=local' : Exception calling "CommitChanges" with "0" argument(s): "There is a naming violation.
" Un conteneur tel que CN=Users ne peut pas héberger d'unité d'organisation ; visez une véritable OU avec -
OUPath.
```

Mots-clés : *CN=Users · -OUPath · naming violation · There is a naming violation · Impossible de créer l'OU · unité d'organisation · Shinken supervision users*

> **Survient à l'étape :** Étape 4 — Spécificités Active Directory — voir Spécificités Active Directory sur la page de configuration.

Dans le déroulé du script :

```
[3/11] Compte et groupe Active Directory
      Annuaire : DC=exemple,DC=local (via DC01.exemple.local)
Étape Compte et groupe AD échouée
======================================================================
RÉSUMÉ DES ÉTAPES
======================================================================
[OK] Langue en-US fr-FR : Étape réussie
[OK] WinRM quickconfig : Étape réussie
[KO] Compte et groupe AD : Erreur : Impossible de créer l'OU 'Shinken supervision users' sous 'CN=Users,
DC=exemple,DC=local' : ...
```

Résolution :

Visez une **véritable unité d'organisation** :

```
.\Configure-Host.ps1 -Default -Domain -OUPath "OU=Utilisateurs,DC=exemple,DC=local"
```

> Sans `-OUPath`, l'OU dédiée est créée à la **racine du domaine** : c'est le comportement par défaut, et il fonctionne dans la majorité des cas.

Aucun identifiant de domaine utilisable – échec en mode non interactif

Lancé à distance ou par tâche planifiée sur une machine du domaine, le script s'arrête avant toute modification. Il ne dispose pas d'identifiants pour écrire dans l'annuaire et ne peut pas les demander : une invite bloquerait l'exécution automatisée.

```
Aucun identifiant de domaine utilisable.
Fournissez-en un de l'une de ces façons :
  - paramètre -DomainCredential (recommandé pour un déclenchement distant) ;
  - exécution sous un compte de domaine habilité (tâche planifiée) ;
  - mode -Interactive, qui demandera les identifiants.
```

Mots-clés : *-DomainCredential · identifiant de domaine · annuaire · Invoke-Command · tâche planifiée · non interactif*

> **Survient à l'étape :** Étape 4 — Spécificités Active Directory — voir Spécificités Active Directory sur la page de configuration.

Résolution :

Fournissez explicitement des identifiants habilités à écrire dans l'annuaire :

```
$cred = Get-Credential
.\Configure-Host.ps1 -Default -Domain -DomainCredential $cred
```

> En mode `-Interactive`, ou lorsque la session courante dispose déjà des droits d'écriture dans l'annuaire, `-DomainCredential` est inutile.

Profil absent et ouverture de session refusée – langue du profil non configurée

Pour écrire la langue préférée dans le profil du compte de supervision, le script doit d'abord **matérialiser ce profil** : il ouvre une session courte sous ce compte. L'opération échoue lorsque le compte ne dispose pas d'un droit d'ouverture de session sur la machine — cas normal sur un **contrôleur de domaine**, où la stratégie par défaut ne l'accorde qu'aux administrateurs.

```
[4/11] Configuration de la langue pour l'utilisateur EXEMPLE\shinken_user
      Profil absent : ouverture d'une session pour le matérialiser...
      Ouverture de session refusée pour EXEMPLE\shinken_user : profil non matérialisé.
      Accordez-lui « Ouvrir une session en tant que tâche » sur cette machine,
      ou configurez la langue par GPO (Préférences > Options régionales).
```

Le message renvoyé par Windows sous cette étape est le suivant :

```
This command cannot be run due to the error: Logon failure: the user has
not been granted the requested logon type at this computer.
```

Mots-clés : *Logon failure · requested logon type · profil non matérialisé · Ouvrir une session en tant que tâche · SeBatchLogonRight · 1385 · PreferredUILanguages · contrôleur de domaine*

Survient à l'étape : Étape 4 — Configuration de la langue — voir Configuration de la langue sur la page de configuration.

Cette étape n'est pas bloquante. Le script la marque ignorée et poursuit jusqu'à la fin : WinRM, les permissions et les services sont configurés normalement. Seule la langue de session du compte de supervision reste indéfinie, ce qui fait échouer les checks `Ntp-Sync` et `Stats-CPU`, qui analysent une sortie localisée et exigent une session `en-US` ou `fr-FR`.

Résolution :

Option 1 — par GPO (recommandé). Définissez la langue sans jamais ouvrir de session sous le compte :

```
Configuration utilisateur
  -> Préférences
    -> Paramètres du Panneau de configuration
      -> Options régionales
```

Option 2 — accorder le droit d'ouverture de session, puis relancer le script. Dans `secpol.msc` :

```
Stratégies locales
  -> Attribution des droits utilisateur
    -> Ouvrir une session en tant que tâche
       (ajouter le compte de supervision)
```

Sur un **contrôleur de domaine**, préférez l'option 1. Accorder un droit d'ouverture de session à un compte de service sur un contrôleur de domaine élargit sa surface d'exposition, pour un gain limité à la localisation de deux checks.

Après la configuration

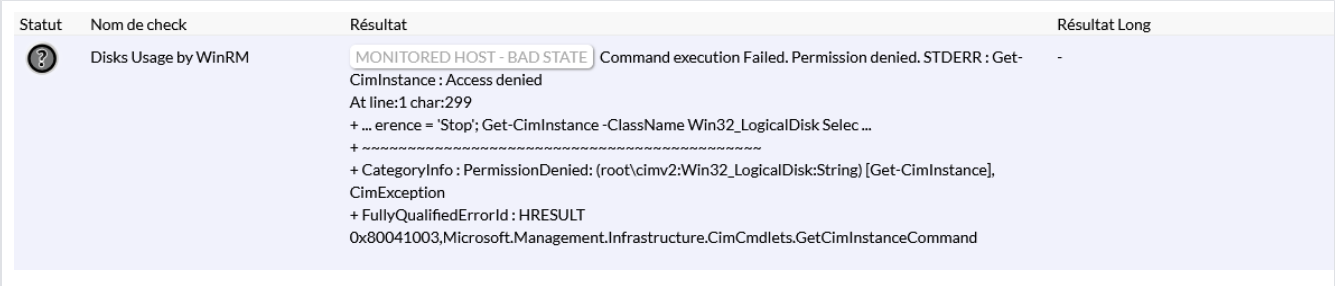
Le check *Service KEY State by WinRM* remonte une erreur

Les autres checks de la machine fonctionnent, mais la supervision d'un service précis échoue. Le compte de supervision n'a pas l'accès en lecture au service demandé : seuls `scmanager`, `W32Time` et `WinRM` sont autorisés par défaut.

```
UNKNOWN – Command execution Failed. Permission denied.
```

Mots-clés : *Service KEY State · Permission denied · -ServicesName · sc.exe sdshow · scmanager*

Survient à l'étape : Étape 4 — Configurer les services à superviser — voir Configurer les services à superviser sur la page de configuration.



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 :

Relancez le script en indiquant le ou les services à autoriser :

```
.\Configure-Host.ps1 -UserName "shinken_user" -Password $secPass -ServicesName "MonService","AutreService"
```

Pour vérifier les droits posés sur un service :

```
sc.exe sdshow MonService
```

Le nom à fournir est le **nom court** du service (colonne *Name*), pas son nom d'affichage. Pour le retrouver :

```
Get-Service | Where-Object DisplayName -like "*MonApplication*"
```