Ntp Sync 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
    - Statut
    - Résultat
    - Résultat Long
- Métriques
  - Définition
  - Exemple
- Erreurs et pré-requis
  - Ntp Sync by WinRM
    - MONITORED HOST - BAD STATE – Windows Time service is not running. Please start the w32time service
    - MONITORED HOST - BAD STATE – No external time server source is configured.
  - 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

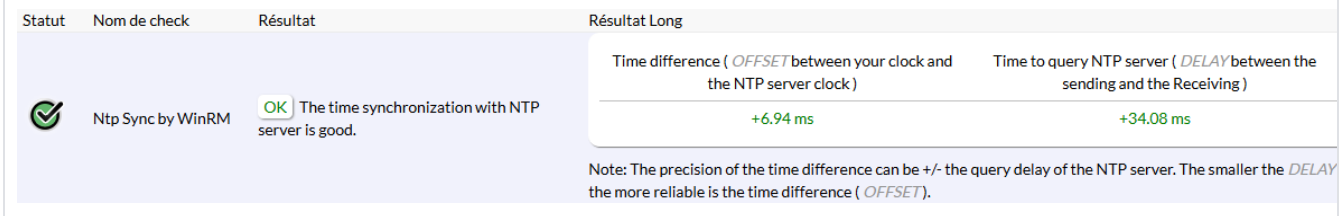
Contexte

Le check **Ntp Sync by WinRM** vérifie la date et l'heure du système, puis les compare à celles du serveur de temps configuré sur la machine.

- Si le serveur est accessible, les informations suivantes seront obtenues :
  - le temps d'aller-retour entre client et le serveur
  - le décalage d'horloge entre l'hôte supervisé et le serveur de temps de référence.
- Dans le cas contraire, un message invitera à démarrer le service concerné.

La vérification est basée sur 2 informations : l' **OFFSET** et le **DELAY**

- Pour savoir si le serveur est à l'heure, le serveur ntp local fait une requête au serveur ntp de référence.
  - Le temps d'aller-retour de la requête correspond au **DELAY** mesuré.
  - L'**OFFSET** correspond à la différence d'heure entre le serveur supervisé et le serveur **ntp** de référence.
- Les 2 valeurs sont nécessaires, car l'**OFFSET** peut avoir au pire la valeur de **DELAY** comme marge d'erreur (*le temps d'acheminement moyen de la requête au serveur de temps*).
  - C'est pour cela que le check **Ntp Sync by WinRM** mesure ces 2 valeurs et réagit en fonction des seuils de tolérance définis.



Statut	Nom de check	Résultat	Résultat Long	
	Ntp Sync by WinRM	OK The time synchronization with NTP server is good.	Time difference (*OFFSET* between your clock and the NTP server clock)	Time to query NTP server (*DELAY* between the sending and the Receiving)
			+6.94 ms	+34.08 ms

Note: The precision of the time difference can be +/- the query delay of the NTP server. The smaller the *DELAY* the more reliable is the time difference (*OFFSET*).

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check check_ntp_sync
    --hostname "$HOSTADDRESS$"
    --port "$_HOSTWINDOWS_BY_WINRM__PORT$"
    --username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"
    --password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
    --auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
    --timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"
    -c "$_HOSTWINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT$","$_HOSTWINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT$"
    -w "$_HOSTWINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN$","$_HOSTWINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN$"
```

Données utilisées provenant des modèles

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

Nom	Modifiable sur	Unité	Valeur par défaut	Description
`WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT`	l'Hôte *(Onglet Données)*	ms	*30*	Définit le décalage en millisecondes à partir duquel le check passe en **CRITIQUE** .
`WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN`	l'Hôte *(Onglet Données)*	ms	*10*	Définit le décalage en millisecondes à partir duquel le check passe en **ATTENTION**.

WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT	l'Hôte *(Onglet Données)*	ms	*200*	Définit le délai en millisecondes à partir duquel le check passe en **CRITIQUE** .
WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN	l'Hôte *(Onglet Données)*	ms	*100*	Définit le délai en millisecondes à partir duquel le check passe en **ATTENTION** .

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	Résultat Long
	Ntp Sync by WinRM	OK The time synchronization with NTP server is good.	Time difference (*OFFSET* between your clock and the NTP server clock) : +6.94 ms Time to query NTP server (*DELAY* between the sending and the Receiving) : +34.08 ms Note: The precision of the time difference can be +/- the query delay of the NTP server. The smaller the *DELAY* is, the more reliable is the time difference (*OFFSET*).

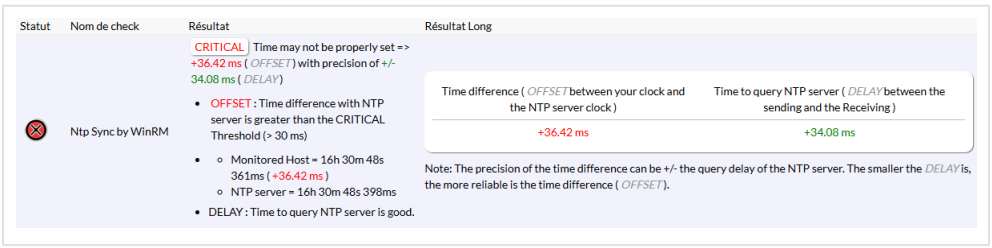
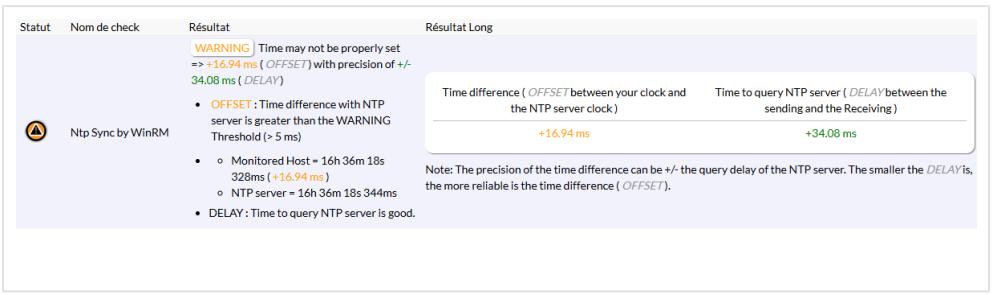
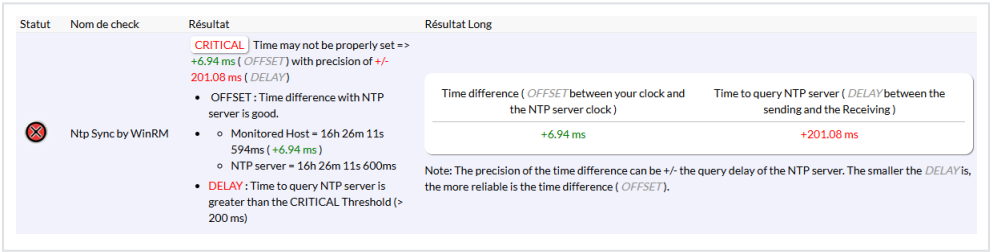
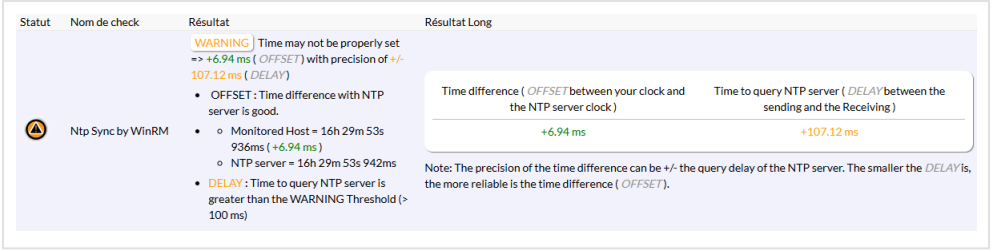
Interprétation

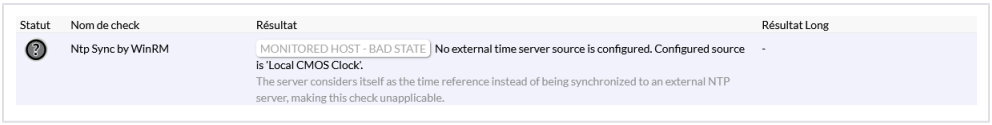
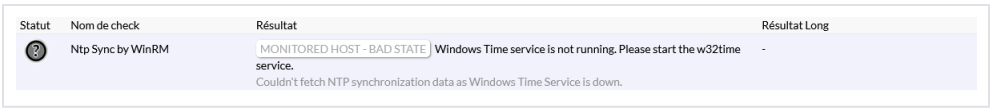
Statut

- Il peut prendre quatre valeurs ***OK*** / ***CRITIQUE*** / ***ATTENTION*** / ***INCONNU*** .
  - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
    - **WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT**
    - **WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN**
    - **WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT**
    - **WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN**
  - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

Le texte de la colonne "Affichage des seuils" montre les paramètres utilisés et leur valeur définie sur l'équipement supervisé.

	Critical	Warning
NTP offset in ms (*time gap with the NTP server*)	> 30 ms *WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT*	> 10 ms *WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN*
NTP delay in ms (*Communication time with the NTP server*)	> 200 ms *WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT*	> 100 ms *WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN*

Situation	*Statut*	*Exemple*
• Le décalage observé dépasse **WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT**	***CRITIQUE***	
• Le décalage observé dépasse **WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN**	***ATTENTION***	
• Le délai observé dépasse **WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT**	***CRITIQUE***	
• Le délai observé dépasse **WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN**.	***ATTENTION***	

• Aucun serveur de temps n'est configuré, l'hôte supervisé s'établit sur sa propre horloge.	*INCONNU*	
▪ Le service W32Time n'est pas démarré sur l'hôte supervisé.	*INCONNU*	

Résultat

Le résultat contient un message indiquant le statut du check.

Lors d'un passage en ***CRITIQUE*** ou ***ATTENTION*** , un message indique quel en est la cause.

Résultat Long

Le résultat long contient un tableau affichant la valeur de l'**OFFSET** et du **DELAY** en millisecondes.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
delay	ms	Temps aller-retour entre le client et le serveur	**WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN**	**WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT**
offset	ms	Décalage de temps entre le système et le serveur	**WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN**	**WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT**

Exemple

Métriques :

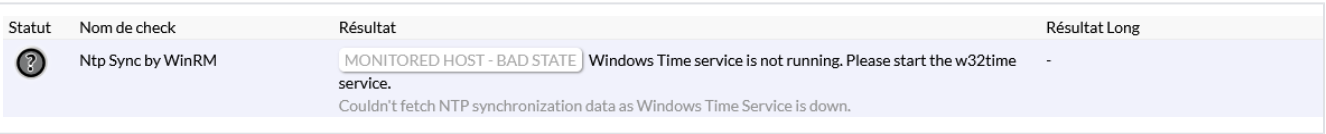
Métrique	Valeur	Seuil d'avertissement	Seuil critique
delay	27.85ms	100.00	200.00
offset	11.31ms	10.00	30.00

Erreurs et pré-requis

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.



La commande ci-dessous permet de le rallumer :

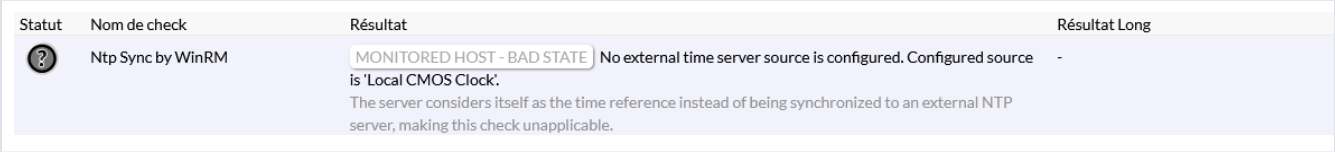
```
# Redémarrer le service WinRM :
Restart-Service W32Time
```

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)

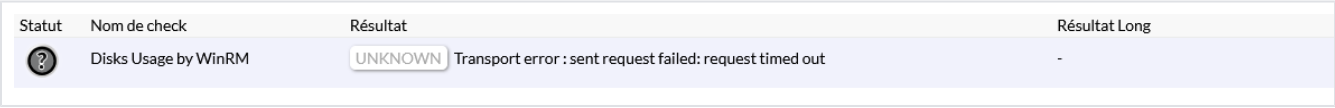
```
w32tm /resync
```

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**"

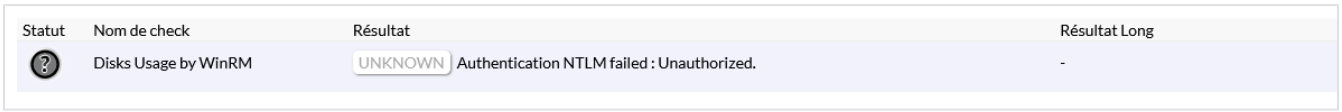
UNKNOWN – Authentication NTLM failed : Unauthorized

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



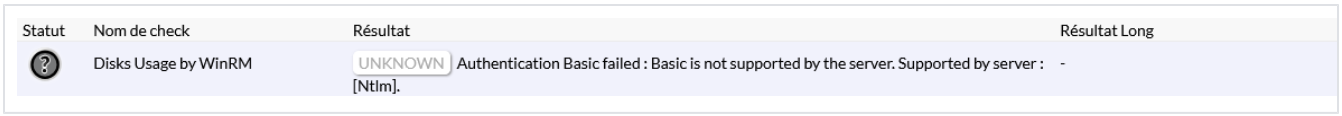
Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN Authentication NTLM failed : Unauthorized.	-

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**"

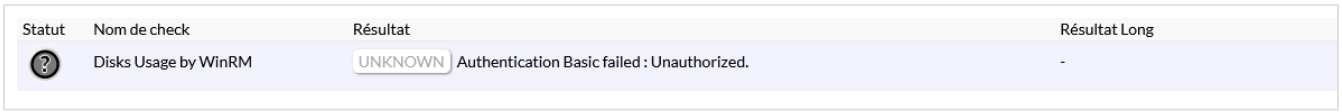
UNKNOWN – Authentication Basic failed : Unauthorized

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.