

# shinken-poller ( Modèle d'hôte )

## Sommaire

### Contexte

#### Description du modèle

##### Checks

##### Paramétrage des checks

##### Données de performances

##### Détail des commandes

#### Interprétation des données de l'état de santé du Poller ( Poller - \$KEY\$ - Running Well )

##### Statistiques de l'état de santé du Poller

##### Description des erreurs

Problème de surcharge des disques constaté lors de l'écriture de logs

Erreur d'un démon bloqué, qui doit être redémarré

Problème de conflits d'Arbiters

Les serveurs ne sont pas à la même heure

La dernière connexion de l'Arbiter remonte à trop longtemps

Le démon a bloqué une tentative de chargement d'objet malveillant

Le démon est en cours d'arrêt

##### Exemple d'un état de santé dégradé du Poller

##### Statistiques de l'état de santé du Poller

#### Interprétation des statistiques de performance du Poller ( Poller - \$KEY\$ - Performance )

##### Statistiques générales sur l'exécution des checks

##### Charge du Poller

##### Utilisation du CPU

##### Vol du CPU

##### Utilisation de la mémoire ( RAM )

Le nombre de processus dans la file d'attente du processeur

Erreur d'un démon bloqué, qui doit être redémarré

Le démon a bloqué une tentative de chargement d'objet malveillant

Le démon est en cours d'arrêt

## 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.

? Unknown Attachment

## Paramétrage

Le check utilise la ligne de commande suivante :

```

$WINDOWS-BY-WINRM__SHINKEN__PLUGINS__DIR$/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

**Error rendering macro 'excerpt-include'**

No link could be created for 'Modèle windows-by-WinRM\_\_base'.

### Données spécifiques pour ce check

| Nom                                     | Modifiable sur               | Unité | Valeur par défaut | Description   |
|---|------------------------------|-------|-------------------|---|
| WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT | l'Hôte<br>( Onglet Données ) | ms    | 30                | Définit le décalage en millisecondes à partir duquel le check passe en <b>CRITIQUE</b> .  |
| WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN | l'Hôte<br>( Onglet Données ) | ms    | 10                | Définit le décalage en millisecondes à partir duquel le check passe en <b>ATTENTION</b> . |
| WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT  | l'Hôte<br>( Onglet Données ) | ms    | 200               | Définit le délai en millisecondes à partir duquel le check passe en <b>CRITIQUE</b> .     |
| WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN  | l'Hôte<br>( Onglet Données ) | ms    | 100               | Définit le délai en millisecondes à partir duquel le check passe en <b>ATTENTION</b> .    |

### Données DFE ( Duplicate Foreach )

Pas de données DFE pour ce check

### Données utilisées provenant du check

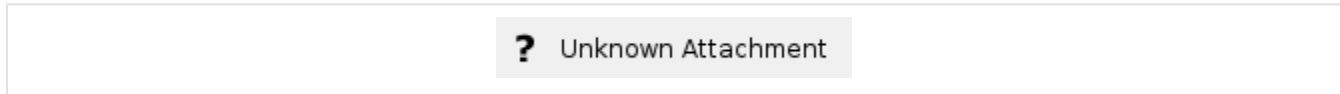
Pas de données provenant du check pour ce modèle

**Error rendering macro 'excerpt-include'**

No link could be created for 'Uptime by WinRM'.

## Résultat


### Exemple

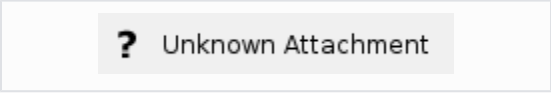








## Interprétation

### 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.



| <i>Situation</i>  | <i>Statut</i>    | <i>Exemple</i>  |
|---|------------------|---|
| <ul style="list-style-type: none"><li>• Le décalage observé dépasse <b>WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-CRIT</b></li></ul>                | <b>CRITIQUE</b>  |   |
| <ul style="list-style-type: none"><li>• Le décalage observé dépasse <b>WINDOWS_BY_WINRM__NTP-SYNC__OFFSET-WARN</b></li></ul>                | <b>ATTENTION</b> |  |
| <ul style="list-style-type: none"><li>• Le délai observé dépasse <b>WINDOWS_BY_WINRM__NTP-SYNC__DELAY-CRIT</b></li></ul>                    | <b>CRITIQUE</b>  |  |
| <ul style="list-style-type: none"><li>• Le délai observé dépasse <b>WINDOWS_BY_WINRM__NTP-SYNC__DELAY-WARN</b>.</li></ul>                   | <b>ATTENTION</b> |  |
| <ul style="list-style-type: none"><li>• Aucun serveur de temps n'est configuré, l'hôte supervisé s'établit sur sa propre horloge.</li></ul> | <b>INCONNU</b>   |  |
| <ul style="list-style-type: none"><li>▪ Le service W32Time n'est pas démarré sur l'hôte supervisé.</li></ul>                                | <b>INCONNU</b>   |  |

### 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

? Unknown Attachment

## Erreurs et pré-requis

### Ntp Sync by WinRM

**Windows Time service is not running. Please start the w32time service**

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

? Unknown Attachment

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
```

### No external source is configured

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

? Unknown Attachment

#### Résolution 1 :

Si ce comportement est normal, il est conseillé 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](http://pool.ntp.org) ou [time.windows.com](http://time.windows.com) ).

- aa

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

## 2. Redémarrer le service de temps Windows

```
Restart-Service w32time
```

```
3. w32tm /resync
```

**Error rendering macro 'excerpt-include'**

No link could be created for 'Erreurs du pack windows-by-WinRM\_\_shinken'.