

# Certificate Expiration \$KEY\$ 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

- Résultat
- Résultat long

### Métriques

#### Erreurs et pré-requis


- 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 **Certificate Expiration [ \$KEY\$ ] by WinRM** permet de superviser l'expiration

Il est configurable pour renvoyer un status **CRITIQUE** / **ATTENTION** si le nombre de jours restants avant l'expiration du certificat supervisé passe en dessous des seuils.

Le check utilise une donnée Duplicate Foreach ( DFE ) qui permet de générer plusieurs fois le check pour chaque certificat à superviser.

Statut	Nom de check	Résultat	Résultat Long
	Certificate Expiration [LocalWebsite] by WinRM	[OK] The certificate "mylocalsite.local" expire the "2036-02-10"	-

## Paramétrage

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINS__DIR$/check-windows-certificate-expiration.py
-H "$HOSTADDRESS$"
-u "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"
-p "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
-M "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
-m certificate_expiration
-T "$ARG1$"
-N "$ARG2$"
-w "$_SERVICEWINDOWS_BY_WINRM__CERTIFICATE-EXPIRATION__EXPIRATION-WARN$"
-c "$_SERVICEWINDOWS_BY_WINRM__CERTIFICATE-EXPIRATION__EXPIRATION-CRIT$"

```

## 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 : <ul style="list-style-type: none"> <li>mon_utilisateur</li> <li>mon_domaine\mon_utilisateur</li> <li>mon_utilisateur@mon_domaine</li> </ul>
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 <b>INCONNUE</b> .

### Données spécifiques pour ce check

Nom	Modifiable sur	Unité	Valeur par défaut	Description
WINDOWS_BY_WINRM__CERTIFICATE-EXPIRATION__EXPIRATION-CRIT	l'Hôte ( Onglet Données )	jours	30	Seuil d'expiration en jours en dessous duquel un status <b>CRITIQUE</b> est déclenché
WINDOWS_BY_WINRM__CERTIFICATE-EXPIRATION__EXPIRATION-WARN	l'Hôte ( Onglet Données )	jours	60	Seuil d'expiration en jours en dessous duquel un status <b>ATTENTION</b> est déclenché

### Données DFE ( Duplicate Foreach )

Donnée	Description	Exemple
WINDOWS_BY_WINRM__CERTIFICATE-EXPIRATION__STORE-AND-CERTIFICATE	Définit une paire KEY\$(VALUE_A)\$\$(VALUE_B)\$\$. <ul style="list-style-type: none"> <li><b>KEY</b> est utilisé pour adapter dynamiquement le nom du check</li> <li><b>VALUE_A</b> correspond au magasin de certificat dans lequel chercher le certificat à superviser. <ul style="list-style-type: none"> <li>Les valeurs possibles sont : <ul style="list-style-type: none"> <li>LocalMachine</li> <li>CurrentUser</li> </ul> </li> </ul> </li> <li><b>VALUE_B</b> correspond au nom du certificat à trouver.</li> </ul>	WindowsRootCert\$(LocalMachine)\$\$(Microsoft Root Certificate Authority 2010)\$,  Domain\$(LocalMachine)\$\$(MyDomainName.com)\$

- Dupliquer des checks en fonction d'une liste de valeurs présentes dans la Donnée d'un hôte (duplicate\_foreach)

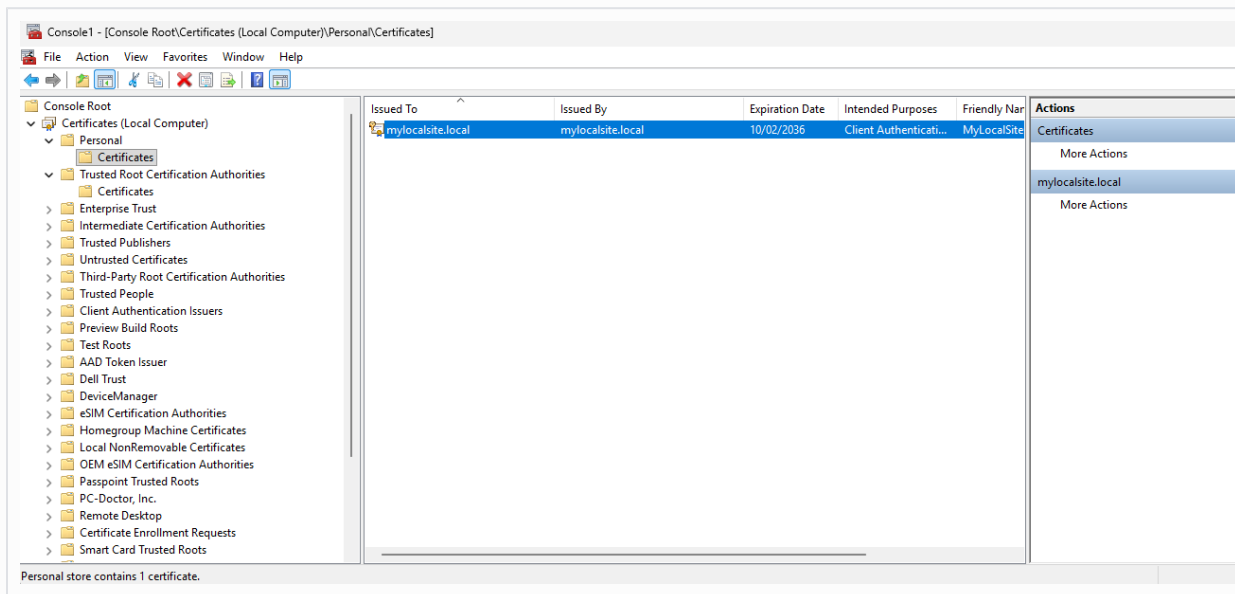
Modifier les données accrochées à l'hôte affectera l'ensemble des checks dupliqués.  
Afin de paramétrer individuellement chaque checks, il est possible de surcharger les données des checks.

- [La surcharge des propriétés pour un check](#)



En cas de difficulté pour identifier les certificats à superviser, ils peuvent être recherchés depuis la console MMC.

<https://learn.microsoft.com/en-us/windows-hardware/drivers/install/certificate-stores#how-to-use-the-contents-of-the-certificate-store>



## 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
USERPLUGINS DIR	Non modifiable ( Sauf Admin Shinken )	--	/var/lib/shinken/libexec	<b>/var/lib/shinken/libexec</b>	Chemin absolu contenant les sondes installés par Shinken
WINDOWS-BY-WINRM_SHINKEN_VENDOR	Non modifiable ( Sauf Admin Shinken )	--	shinken-additional-packs	<b>shinken-additional-packs</b>	Dossier fournit par shinken
WINDOWS-BY-WINRM_SHINKEN_PACKNAME	Non modifiable ( Sauf Admin Shinken )	--	windows-by-WinRM__shinken	<b>windows-by-WinRM__shinken</b>	Dossier contenant les sondes

WINDOWS-BY-WINRM__SHINKEN__PLUGIN__SDIR	Non modifiable ( Sauf Admin Shinken )	--	USERPLUGINS__DIR/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
	Certificates [LocalWebsite] by WinRM	[OK] The certificate "mylocalsite.local" expire the "2036-02-10"	-







## Interprétation

- 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\_CERTIFICATE-EXPIRATION\_EXPIRATION-CRIT**
    - WINDOWS\_BY\_WINRM\_CERTIFICATE-EXPIRATION\_EXPIRATION-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
Certificates remaining days ≤ 30	≤ 60
WINDOWS_BY_WINRM_CERTIFICATE-EXPIRATION-EXP...	WINDOWS_BY_WINRM_CERTIFICATE-EXPIRATION-EXP...

Situation	Statut	Exemple												
<ul style="list-style-type: none"> <li>La date d'expiration du certificat supervisé est inférieure ou égale à <b>WINDOWS_BY_WINRM_CERTIFICATE-EXPIRATION_EXPIRATION-CRIT</b></li> </ul>	<b>CRITIQUE</b>	<table border="1"> <thead> <tr> <th>Statut</th> <th>Nom de check</th> <th>Résultat</th> <th>Résultat Long</th> </tr> </thead> <tbody> <tr> <td></td> <td>Certificate Expiration [LocalWebsite] by WinRM</td> <td><b>[CRITICAL]</b></td> <td>-</td> </tr> <tr> <td></td> <td></td> <td>The certificate "mylocalsite.local" expire in "10" days, the "2026-02-20".</td> <td></td> </tr> </tbody> </table>	Statut	Nom de check	Résultat	Résultat Long		Certificate Expiration [LocalWebsite] by WinRM	<b>[CRITICAL]</b>	-			The certificate "mylocalsite.local" expire in "10" days, the "2026-02-20".	
Statut	Nom de check	Résultat	Résultat Long											
	Certificate Expiration [LocalWebsite] by WinRM	<b>[CRITICAL]</b>	-											
		The certificate "mylocalsite.local" expire in "10" days, the "2026-02-20".												
<ul style="list-style-type: none"> <li>La date d'expiration du certificat supervisé est inférieure ou égale à <b>WINDOWS_BY_WINRM_CERTIFICATE-EXPIRATION_EXPIRATION-WARN</b></li> </ul>	<b>ATTENTION</b>	<table border="1"> <thead> <tr> <th>Statut</th> <th>Nom de check</th> <th>Résultat</th> <th>Résultat Long</th> </tr> </thead> <tbody> <tr> <td></td> <td>Certificate Expiration [LocalWebsite] by WinRM</td> <td><b>[WARNING]</b></td> <td>-</td> </tr> <tr> <td></td> <td></td> <td>The certificate "mylocalsite.local" expire in "40" days, the "2026-03-22".</td> <td></td> </tr> </tbody> </table>	Statut	Nom de check	Résultat	Résultat Long		Certificate Expiration [LocalWebsite] by WinRM	<b>[WARNING]</b>	-			The certificate "mylocalsite.local" expire in "40" days, the "2026-03-22".	
Statut	Nom de check	Résultat	Résultat Long											
	Certificate Expiration [LocalWebsite] by WinRM	<b>[WARNING]</b>	-											
		The certificate "mylocalsite.local" expire in "40" days, the "2026-03-22".												

<ul style="list-style-type: none"> <li>Aucun certificat n'a été trouvé</li> </ul>	<b>INCONNU</b>	<table border="1"> <thead> <tr> <th>Statut</th> <th>Nom de check</th> <th>Résultat</th> <th>Résultat Long</th> </tr> </thead> <tbody> <tr> <td></td> <td>Certificate Expiration [NotACertificate] by WinRM</td> <td>[UNKNOWN] Certificate "not_a_certificate.com" not found in store "Cert:\LocalMachine"</td> <td>-</td> </tr> </tbody> </table>	Statut	Nom de check	Résultat	Résultat Long		Certificate Expiration [NotACertificate] by WinRM	[UNKNOWN] Certificate "not_a_certificate.com" not found in store "Cert:\LocalMachine"	-
Statut	Nom de check	Résultat	Résultat Long							
	Certificate Expiration [NotACertificate] by WinRM	[UNKNOWN] Certificate "not_a_certificate.com" not found in store "Cert:\LocalMachine"	-							
<ul style="list-style-type: none"> <li>Le magasin de certificat demandé n'est pas valide</li> </ul>	<b>INCONNU</b>	<table border="1"> <thead> <tr> <th>Statut</th> <th>Nom de check</th> <th>Résultat</th> <th>Résultat Long</th> </tr> </thead> <tbody> <tr> <td></td> <td>Certificate Expiration [LocalWebsite] by WinRM</td> <td>[UNKNOWN] Bad parameters. Expected one of [LocalMachine, CurrentUser]. Got "BadStore".</td> <td>-</td> </tr> </tbody> </table>	Statut	Nom de check	Résultat	Résultat Long		Certificate Expiration [LocalWebsite] by WinRM	[UNKNOWN] Bad parameters. Expected one of [LocalMachine, CurrentUser]. Got "BadStore".	-
Statut	Nom de check	Résultat	Résultat Long							
	Certificate Expiration [LocalWebsite] by WinRM	[UNKNOWN] Bad parameters. Expected one of [LocalMachine, CurrentUser]. Got "BadStore".	-							

## Résultat

Le résultat contient un message indiquant le status et la date d'expiration du certificat supervisé.

## Résultat long

*Pas de résultat long.*

## Métriques

*Pas de métriques.*

## 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.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	<b>UNKNOWN</b> 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 connexion ; ou bien son pare-feu.

- Il se peut que votre 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	<b>UNKNOWN</b> 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


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 [Ntlm].	Authentication Basic failed : Basic is not supported by the server. Supported by server : -

**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'exécution 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 exécuter 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 [Configurati on 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, nécessaire à la supervision de la machine.

Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	<b>MONITORED HOST - BAD STATE</b> 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 nécessaire 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	<b>UNKNOWN</b> 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.