

Files Matching \$KEY\$ LAST ACCESS by WinRM

Sommaire

- Contexte
- Paramétrage
 - Données utilisées provenant du modèle
 - Données communes pour les checks du modèle
 - Données spécifiques pour ce check
 - Les 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
 - Files Matching \$KEY\$ LAST ACCESS by WinRM
 - MONITORED HOST - BAD STATE – LastAccessTime updates are disabled.
 - 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 **File Matching [\$KEY\$] LAST ACCESS by WinRM** permet de vérifier la date de dernier accès des fichiers présents dans un répertoire, en fonction d'un filtre spécifique ou d'une liste de noms de fichiers.

Statut	Nom de check	Résultat	Résultat Long
	Files Matching [SHINKEN] LAST ACCESS by WinRM	 All files have been accessed recently.	-

Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINDIR$/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 "$ARG2$"

--last-access-warn "$ARG3$"
--last-access-crit "$ARG4$"

--recursive "$ARG5$"
--include_hidden "$ARG6$"

--kind "last_access"
```

Données utilisées provenant du modèle

Données communes pour les checks du modèle

Nom	Modifiable sur	Valeur par défaut	Description
WINDOWS_BY_WINRM__AUTHMET HOD	l'Hôte (<i>Onglet Données</i>)	ntlm	Méthode d'authentification utilisé. Valeurs possibles : basic, ntlm
WINDOWS_BY_WINRM__DOMAINP ASSWORD	l'Hôte (<i>Onglet Données</i>)	Ch4nge_Th1s_P4s sw0rd	Mot de passe de l'utilisateur de supervision
WINDOWS_BY_WINRM__DOMAINU SER	l'Hôte (<i>Onglet Données</i>)	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 (<i>Onglet Données</i>)	5985	Port de connexion au serveur WinRM de l'hôte à superviser.
WINDOWS_BY_WINRM__TIMEOUT	l'Hôte (<i>Onglet Données</i>)	20	Temps maximum sans réponse d'une requête WinRM pour que la sonde renvoi un statut <i>INCONNU</i> .

Données spécifiques pour ce check

Nom	Modifiable sur	Valeur par défaut	Description
WINDOWS_BY_WINRM__FILES-MATCHING-LAST- ACCESS__NO-ACCESS-SINCE-HOURS-WARN	l'Hôte (<i>Onglet Données</i>)	24	Délai en heures écoulées depuis le dernier accès à un fichier avant de passer le check en statut <i>ATTENTION</i> Utilisé par \$ARG3\$ de la DFE WINDOWS_BY_WINRM__FIL ES-MATCHING-LAST-ACCESS.

WINDOWS_BY_WINRM__FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-CRIT	l'Hôte (<i>Onglet Données</i>)	48	Délai en heures écoulées depuis le dernier accès à un fichier avant de passer le check en statut CRITIQUE Utilisé par \$ARG4\$ de la DFE WINDOWS_BY_WINRM__FILES-MATCHING-LAST-ACCESS.
--	-------------------------------------	----	--

Les données DFE (Duplicate Foreach)

Nom	Modifiable sur	Valeur par défaut	Description			Exemple
WINDOWS_BY_WINRM__FILES-MATCHING-LAST-ACCESS	l'Hôte (<i>Onglet Données</i>)	--	Valeur	Explication	Exemple	- Mode pattern : LOGS\$(C:\shinken)\$(*.log)\$(24)\$(48)\$(true)\$(true)\$ - Mode list : LOGS\$(C:\shinken)\$([fichier1.log, fichier2.log])\$(24)\$(48)\$(true)\$(true)\$
			\$KEY\$	Nom utilisé pour garantir l'unicité des checks DFE générés.	LOGS	
			\$ARG1\$	Répertoire principal à analyser.	C:\shinken	
			\$ARG2\$	Filtre à appliquer sur ce répertoire. Il peut prendre deux formes différentes : - un pattern - une liste de noms de fichiers	*.log [fichier1.log,fichier2.log] ou fichier1.log; fichier2.log	
			\$ARG3\$	Seuil à partir duquel le check passe en status ATTENTION . Hérite de WINDOWS_BY_WINRM__FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-WARN .	24	
			\$ARG4\$	Seuil à partir duquel le check passe en status CRITIQUE . Hérite de WINDOWS_BY_WINRM__FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-CRIT .	48	
			\$ARG5\$	Active ou désactive la recherche récursive dans le répertoire principal. Il peut accepter 2 types de données : - un booléen - un nombre entier	 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).	
			\$ARG6\$	Active ou désactive la prise en compte des fichiers cachés.	true/false	



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**.

Nom	Valeur	Venant des modèles
WINDOWS_BY_WINRM__FILES-MATCHING	SHINKEN\$(C:\shinken)\\$\$(log)\\$(1000)\\$(10000)\\$(KB)\\$(10)\\$(20)\\$(100)\\$(200)\\$(100)\\$(200)\\$	☐ Pas d'héritage exemple3(C:\logs)\\$(log)\\$ [Modèle windows-by-WinRM__files-many-properties-per-check] r-check]
Utilisé par le check [1 / 7]	Non utilisé par les checks [0 / 7]	

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

WINDOWS_BY_WINRM__FILES-MATCHING__INCLUDE-HIDDEN	true [Dans le modèle windows-by-WinRM__files-many-properties-per-check]	☒ Hérite du modèle true [Modèle windows-by-WinRM__files-many-properties-per-check] r-check]
WINDOWS_BY_WINRM__FILES-MATCHING__RECURSIVE	true [Dans le modèle windows-by-WinRM__files-many-properties-per-check]	☒ Hérite du modèle true [Modèle windows-by-WinRM__files-many-properties-per-check] r-check]

Nom	Surcharge / Exclusion	Duplicate Foreach	Groupes d'utilisateurs notifiés	Commande de vérification	Essayer ce check
Files Matching [SHINKEN] by WinRM		WINDOWS_BY_WINRM__FILES-MATCHING			
Files Matching [SHINKEN] by WinRM		SHINKEN	[Même comportement que son hôte]	cmd-check_Files-Matching_windows-by-WinRM__files-many-properties-per-check1C:\shinken?log:1000;10000;KB;10;20;100;200;0:100;200>true>true	

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

3. Si plusieurs instances ne déclarent pas **\$ARG12\$** et **\$ARG13\$**, les 2 utiliseront les mêmes 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** ferait basculer toutes les instances sans surcharge à **false**.

Nom	Valeur	Venant des modèles
WINDOWS_BY_WINRM__FILES-MATCHING	SHINKEN\$(C:\shinken)\\$\$(log)\\$(1000)\\$(10000)\\$(KB)\\$(10)\\$(20)\\$(100)\\$(200)\\$(100)\\$(200)\\$(false)\\$(false)\\$	☐ Pas d'héritage exemple3(C:\logs)\\$(log)\\$ [Modèle windows-by-WinRM__files-many-properties-per-check] r-check]
Utilisé par le check [1 / 7]	Non utilisé par les checks [0 / 7]	

Nom	Surcharge / Exclusion	Duplicate Foreach	Groupes d'utilisateurs notifiés	Commande de vérification	Essayer ce check
Files Matching [SHINKEN] by WinRM		WINDOWS_BY_WINRM__FILES-MATCHING			
Files Matching [SHINKEN] by WinRM		SHINKEN	[Même comportement que son hôte]	cmd-check_Files-Matching_windows-by-WinRM__files-many-properties-per-check1C:\shinken?log:1000;10000;KB;10;20;100;200;0:100;200>false>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
USERPLUGINS DIR	Non modifiable <i>(Sauf Admin Shinken)</i>	--	/var/lib/shinken/libexec	/var/lib/shinken/libexec	Chemin absolu contenant les sondes installés par Shinken
WINDOWS-BY-WINRM__SHINKEN__VENDOR	Non modifiable <i>(Sauf Admin Shinken)</i>	--	shinken-additional-packs	shinken-additional-packs	Dossier fournit par shinken
WINDOWS-BY-WINRM__SHINKEN__PACKNAME	Non modifiable <i>(Sauf Admin Shinken)</i>	--	windows-by-WinRM__shinken	windows-by-WinRM__shinken	Dossier contenant les sondes
WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR	Non modifiable <i>(Sauf Admin Shinken)</i>	--	USERPLUGINDIR/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 (<i>n on modifiable</i>)

Propriétés de l'hôte

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut	Description
HOSTADDRESS	l'Hôte <i>(Onglet Général)</i>	--	Nom de l'hôte	Nom de l'hôte	Adresse de l'hôte

Résultat

Exemple

Statut	Nom de check	Résultat	Résultat Long
	Files Matching [LASTACC=OK] LAST ACCESS by WinRM	 All files have been accessed recently.	-

Interprétation

Statut

- Il peut prendre quatre valeurs **OK** / **CRITIQUE** / **ATTENTION** / **INCONNU**.
 - Le statut dépend du retour de sonde et de la configuration spécifique du check pour les données suivantes :
 - WINDOWS_BY_WINRM_FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-WARN** ou DFE position **\$ARG3\$**
 - WINDOWS_BY_WINRM_FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-CRIT** ou DFE position **\$ARG4\$**
 - 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
Last Access (H) > 48 DFE (\$ARG4\$)	> 24 DFE (\$ARG3\$)
or WINDOWS_BY_WINRM_FILES-MATCHING-LAST-ACC...	or WINDOWS_BY_WINRM_FILES-MATCHING-LAST-ACC...

Situation	Statut	Exemple																		
Au moins un fichier n'a pas été accédé depuis un délai dépassant la valeur de WINDO_WS_BY_WINRM_FILES-MATCHING-LAST-ACCESS_NO-ACCESS-SINCE-HOURS-WARN (ou DFE position \$ARG3\$)	ATTENTION	Statut Nom de check Résultat Résultat Long Files Matching [SHINKEN] LAST ACCESS by WinRM WARNING 3 files exceed LAST ACCESS (≥ 24h00). List of warning files: (> 24H) <table><thead><tr><th>Name</th><th>Last Access (≥ 24 H)</th></tr></thead><tbody><tr><td>C:\shinken\</td><td>-</td></tr><tr><td> brokers\</td><td>-</td></tr><tr><td> broker-03.log</td><td>31h29 (19/05 08:47)</td></tr><tr><td> synchronizer\</td><td>-</td></tr><tr><td> sync-01.log</td><td>37h29 (19/05 02:47)</td></tr><tr><td> sync-02.log</td><td>73h29 (17/05 14:47)</td></tr></tbody></table>	Name	Last Access (≥ 24 H)	C:\shinken\	-	brokers\	-	broker-03.log	31h29 (19/05 08:47)	synchronizer\	-	sync-01.log	37h29 (19/05 02:47)	sync-02.log	73h29 (17/05 14:47)				
Name	Last Access (≥ 24 H)																			
C:\shinken\	-																			
brokers\	-																			
broker-03.log	31h29 (19/05 08:47)																			
synchronizer\	-																			
sync-01.log	37h29 (19/05 02:47)																			
sync-02.log	73h29 (17/05 14:47)																			
Au moins un fichier n'a pas été accédé depuis un délai dépassant la valeur de WINDO_WS_BY_WINRM_FILES-MATCHING-LAST-ACCESS_NO-ACCESS-SINCE-HOURS-CRIT (ou DFE position \$ARG4\$)	CRITIQUE	Statut Nom de check Résultat Résultat Long Files Matching [SHINKEN] LAST ACCESS by WinRM CRITICAL 1 file exceed LAST ACCESS (≥ 48h00). WARNING 2 files exceed LAST ACCESS (≥ 24h00). List of critical files: (> 48H) <table><thead><tr><th>Name</th><th>Last Access (≥ 48 H)</th></tr></thead><tbody><tr><td>C:\shinken\synchronizer\</td><td>-</td></tr><tr><td> sync-02.log</td><td>73h27 (17/05 14:47)</td></tr></tbody></table> List of warning files: (> 24H) <table><thead><tr><th>Name</th><th>Last Access (≥ 24 H)</th></tr></thead><tbody><tr><td>C:\shinken\</td><td>-</td></tr><tr><td> brokers\</td><td>-</td></tr><tr><td> broker-03.log</td><td>31h27 (19/05 08:47)</td></tr><tr><td> synchronizer\</td><td>-</td></tr><tr><td> sync-01.log</td><td>37h27 (19/05 02:47)</td></tr></tbody></table>	Name	Last Access (≥ 48 H)	C:\shinken\synchronizer\	-	sync-02.log	73h27 (17/05 14:47)	Name	Last Access (≥ 24 H)	C:\shinken\	-	brokers\	-	broker-03.log	31h27 (19/05 08:47)	synchronizer\	-	sync-01.log	37h27 (19/05 02:47)
Name	Last Access (≥ 48 H)																			
C:\shinken\synchronizer\	-																			
sync-02.log	73h27 (17/05 14:47)																			
Name	Last Access (≥ 24 H)																			
C:\shinken\	-																			
brokers\	-																			
broker-03.log	31h27 (19/05 08:47)																			
synchronizer\	-																			
sync-01.log	37h27 (19/05 02:47)																			
Aucun fichier ne correspond au filtre dans le répertoire ciblé	CRITIQUE	Statut Nom de check Résultat Résultat Long Files Matching [SHINKEN] LAST ACCESS by WinRM CRITICAL No files found matching 'Pattern: "ghost" in 'C:\shinken'. -																		
Mode liste — au moins un fichier attendu est absent du répertoire ciblé	CRITIQUE	Statut Nom de check Résultat Résultat Long Files Matching [SHINKEN] LAST ACCESS by WinRM CRITICAL 1 file is missing. CRITICAL 1 file exceed LAST ACCESS (≥ 48h00). WARNING 1 file exceed LAST ACCESS (≥ 24h00). Missing 1 file: <table><thead><tr><th>Name</th><th>Status</th></tr></thead><tbody><tr><td>ghost.log</td><td>MISSING</td></tr></tbody></table> Present 3 files: <table><thead><tr><th>Name</th><th>Last Access (H)</th></tr></thead><tbody><tr><td>C:\shinken\</td><td>-</td></tr><tr><td> brokers\</td><td>-</td></tr><tr><td> broker-01.log</td><td>2h29 (20/05 13:47)</td></tr><tr><td> broker-03.log</td><td>31h29 (19/05 08:47)</td></tr><tr><td> synchronizer\</td><td>-</td></tr><tr><td> sync-02.log</td><td>73h29 (17/05 14:47)</td></tr></tbody></table>	Name	Status	ghost.log	MISSING	Name	Last Access (H)	C:\shinken\	-	brokers\	-	broker-01.log	2h29 (20/05 13:47)	broker-03.log	31h29 (19/05 08:47)	synchronizer\	-	sync-02.log	73h29 (17/05 14:47)
Name	Status																			
ghost.log	MISSING																			
Name	Last Access (H)																			
C:\shinken\	-																			
brokers\	-																			
broker-01.log	2h29 (20/05 13:47)																			
broker-03.log	31h29 (19/05 08:47)																			
synchronizer\	-																			
sync-02.log	73h29 (17/05 14:47)																			

Résultat

Selon le statut, une ou plusieurs lignes :

- CRITIQUE** : N fichier(s) non accédé(s) depuis la durée critique (V heures).
- ATTENTION** : N fichier(s) non accédé(s) depuis la durée d'avertissement (V heures).
- OK** : Tous les fichiers ont été accédés récemment.
- Mode liste**, si au moins un fichier manquant : ligne supplémentaire en tête N fichier(s) manquant(s).
- 0 fichier trouvé (mode pattern) : Aucun fichier trouvé correspondant à '<filtre>' dans '<chemin>'.
- UNKNOWN** (host en mauvais état) si les mises à jour de LastAccessTime sont désactivées sur le host : LastAccessTime updates are disabled. Run fsutil behavior set disablelastaccess 0 to enable (NTFS perf impact). (cas par défaut sur tout Windows Server)

Le détail fichier par fichier est dans le résultat long.

Résultat Long

Affiche un tableau arborescent par sévérité (critique puis attention) avec pour chaque fichier dépassant un seuil le nombre d'heures écoulées depuis son dernier accès (ex : 168 H, accompagné de la date au format yyyy-MM-dd HH:mm).

En mode liste (**\$ARG2\$** sous la forme **[fichier1.log, fichier2.log, ...]**), le résultat long est toujours émis :

- Une table **MISSING** en tête si au moins un nom de la liste est absent du répertoire.
- Puis, pour les fichiers présents, les tables critique/attention si des seuils sont dépassés.

Note : si les mises à jour de LastAccessTime sont désactivées sur le host (cas par défaut sur tout Windows Server), le check passe en UNKNOWN et aucun tableau n'est produit.

Métriques

Définition

Nom	Unité	Description	Seuil d'avertissement	Seuil critique
files_accessed_elapsed_h_(NOM_FICHIER)	H	Retourne le nombre d'heures écoulées depuis le dernier accès au fichier.	WINDOWS_BY_WINRM_FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-WARN (ou DFE position \$ARG3\$)	WINDOWS_BY_WINRM_FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-CRIT (ou DFE position \$ARG4\$)

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
files_accessed_elapsed_h_broker-01.log	97.91H	100.00	200.00
files_accessed_elapsed_h_broker-02.log	97.91H	100.00	200.00
files_accessed_elapsed_h_broker-03.log	97.91H	100.00	200.00
files_accessed_elapsed_h_sync-01.log	97.91H	100.00	200.00
files_accessed_elapsed_h_sync-02.log	97.91H	100.00	200.00

Erreurs et pré-requis

Files Matching \$KEY\$ LAST ACCESS by WinRM

MONITORED HOST - BAD STATE – LastAccessTime updates are disabled.

Statut	Nom de check	Résultat	Résultat Long
	Files Matching [LASTACC-OK] LAST ACCESS by WinRM	MONITORED HOST - BAD STATE LastAccessTime updates are disabled. Run fsutil behavior set disablelastaccess 0 to enable (NTFS perf impact).	-

Résolution

Le check supervise la date de dernier accès aux fichiers via l'horodatage NTFS **LastAccessTime**. Si les mises à jour de cet horodatage sont désactivées sur l'hôte Windows, la valeur retournée par le système n'est plus fiable et le check passe en statut **INCONNU**.

Par défaut, les mises à jour de LastAccessTime sont :

- **Désactivées** sur tous les **Windows Server** (2012 R2, 2016, 2019, 2022, 2025)
- **Activées** sur **Windows 10 build 2004+** et **Windows 11**

1. Vérifier l'état actuel sur l'hôte supervisé

```
fsutil behavior query disablelastaccess
```





- 0x80000000 (0) ou 0x80000002 (2) mises à jour **activées**
- 0x80000001 (1) ou 0x80000003 (3) mises à jour **désactivées**

2. Activer les mises à jour (commande à exécuter en administrateur sur l'hôte supervisé)

```
fsutil behavior set disablelastaccess 0
```



Impact performance NTFS : activer les mises à jour de LastAccessTime déclenche une écriture disque à chaque lecture de fichier. À tester avant activation, en particulier sur les serveurs accédant à un grand nombre de fichiers (file servers, environnements de build, partages applicatifs, etc.).

3. Alternative si l'activation n'est pas envisageable

- Utiliser **Files Matching [\$KEY\$] LAST ACCESS by WinRM**.
- Pour le check **Files Matching [\$KEY\$] by WinRM** : positionner les seuils **\$ARG10\$** et **\$ARG11\$** (ou les variables **WINDOWS_BY_WINRM__FILES-MATCHING-LAST-ACCESS__NO-ACCESS-SINCE-HOURS-WARN / ...-CRIT**) à **NONE** pour désactiver la dimension *last_access*.

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 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	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.

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 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 synchroniser.
- 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 : - [Ntim].

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 quickconf

- 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'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 [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, nécessaire 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 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 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.