Processes Memory Matching KEY by WinRM

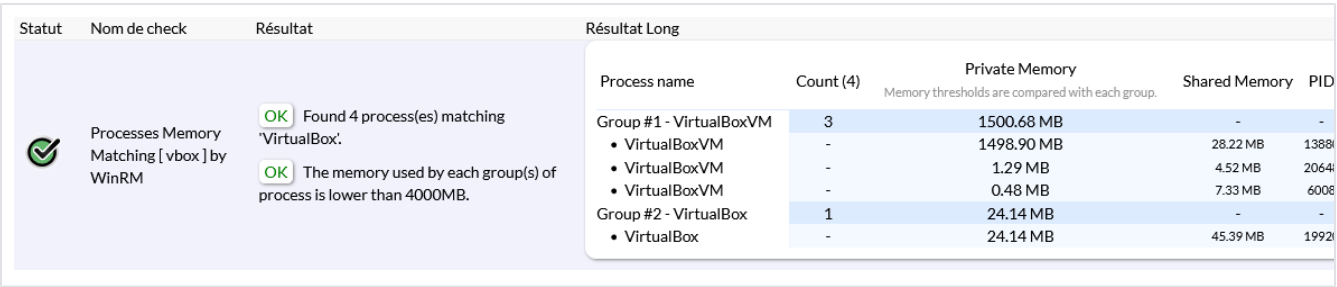
Sommaire

Contexte

Le check **Processes Memory Matching [KEY] by WinRM** permet de vérifier la consommation de la mémoire d'un seul ou plusieurs processus. Il permet donc de garder un œil sur le ou les processus choisis.

Le check peut être configuré pour renvoyer un status ***INCONNU*** si un nombre de processus trouvés minimum ou maximum est dépassé.

Le check utilise une donnée Duplicate Foreach qui permet de générer plusieurs fois le check pour chaque processus ou ensemble de processus à superviser.



Statut	Nom de check	Résultat	Résultat Long
✓	Processes Memory Matching [vbox] by WinRM	OK Found 4 process(es) matching 'VirtualBox'. OK The memory used by each group(s) of process is lower than 4000MB.	

Process name	Count (4)	Private Memory Memory thresholds are compared with each group.	Shared Memory	PID
Group #1 - VirtualBoxVM	3	1500.68 MB	-	-
• VirtualBoxVM	-	1498.90 MB	28.22 MB	1388
• VirtualBoxVM	-	1.29 MB	4.52 MB	2064
• VirtualBoxVM	-	0.48 MB	7.33 MB	6008
Group #2 - VirtualBox	1	24.14 MB	-	-
• VirtualBox	-	24.14 MB	45.39 MB	1992

Paramétrage

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check
check_processes_memory_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 "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"
    -n "$ARG1$"
    -m "$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-
WARN$,$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT$"
    -F "$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__HIDE-ALL$"
    -S "$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON$"
    -r "$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-REGEX-TO-MATCH-PROCESS$"
    --min-count "$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MIN-PROCESS-COUNT$"
    --max-count "$_SERVICEWINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MAX-PROCESS-COUNT$"
```

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__PROCESSES-MEMORY-MATCHING__MEMORY-WARN`	l'Hôte *(Onglet Données)*	MB	*100*	Seuil de consommation mémoire au-dessus duquel un status ***ATTENTION*** est déclenché

`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT`	l'Hôte *(Onglet Données)*	MB	*200*	Seuil de consommation mémoire au-dessus duquel un *status* ***CRITIQUE*** est déclenché
`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MIN-PROCESS-COUNT`	l'Hôte *(Onglet Données)*	--	*1*	Seuil du nombre de processus trouvés au-dessous duquel un ***INCONNU*** est déclenché
`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MAX-PROCESS-COUNT`	l'Hôte *(Onglet Données)*	--	*NONE*	Seuil du nombre de processus trouvés au-dessus duquel un ***INCONNU*** est déclenché
`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__HIDE-ALL`	l'Hôte *(Onglet Données)*	--	*false*	Active/désactive l'affichage des métriques de ce check
`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-REGEX-TO-MATCH-PROCESS`	l'Hôte *(Onglet Données)*	--	*false*	Active ou désactive l'utilisation de regex pour l'usage de la variable DFE **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__PROCESSES-TO-CHECK**
`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON`	l'Hôte *(Onglet Données)*	--	*group*	Détermine le niveau d'agrégation utilisé pour évaluer les seuils de mémoire. • **sum** : compare les seuils à la mémoire totale consommée par l'ensemble des processus. • **group** : compare les seuils à la mémoire utilisée par chaque groupe de processus. • **process** : compare les seuils à la mémoire consommée individuellement par chaque processus.

Données DFE (Duplicate Foreach)

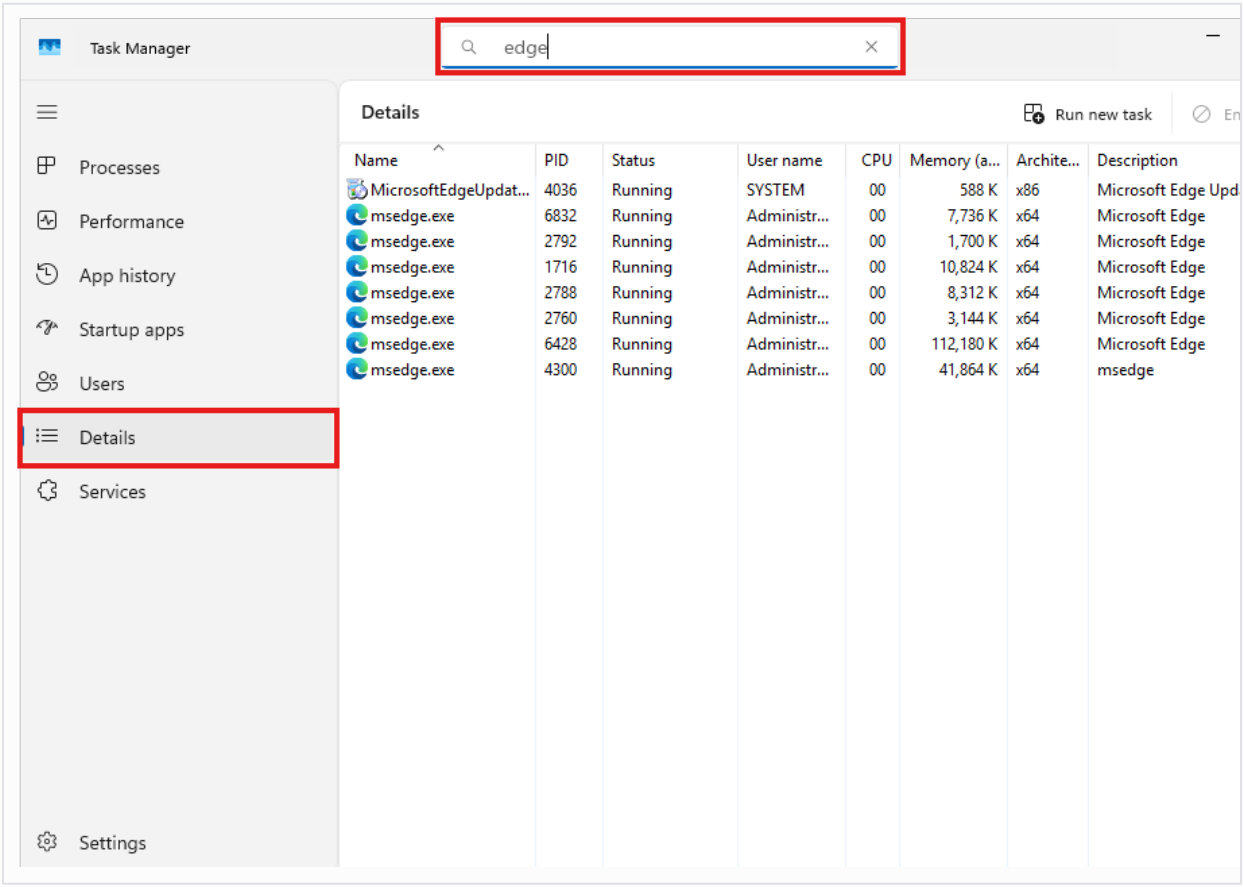
Donnée	Description	Exemple
`WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__PROCESSES-TO-CHECK`	Définit une paire KEY$(VALUE)$, la KEY correspond à la description du processus à vérifier et la VALUE au nom du processus.	VirtualBox $(VBox)$

- 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 processus à superviser, ils peuvent être recherchés via le **Gestionnaire des Tâches Windows**.



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

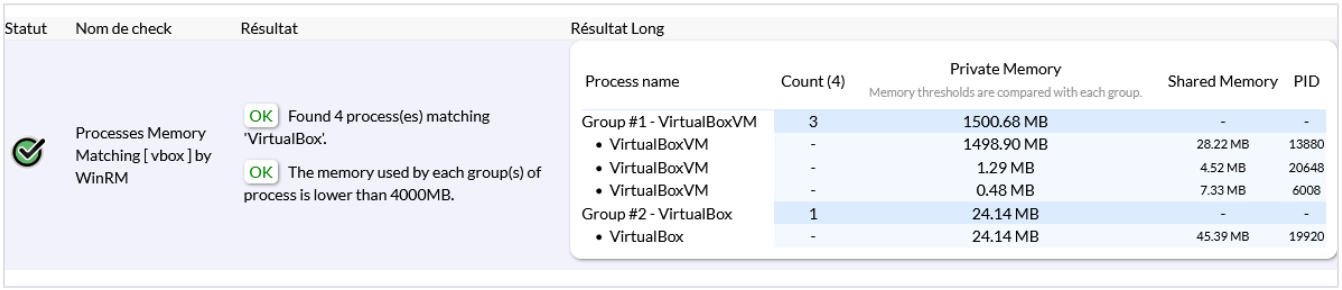
`WINDOWS-BY-WINRM__SHINKEN__PACKNAME`	Non modifiable *(Sauf Admin Shinken)*	--	windows-by-WinRM__shinken	**windows-by-WinRM__shinken**	Dossier contenant les sondes
`WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR`	Non modifiable *(Sauf Admin Shinken)*	--	`USERPLUGINSDIR/WINDOWS-BY-WINRM__SHINKEN__VENDOR/WINDOWS-BY-WINRM__SHINKEN__PACKNAME`	**/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

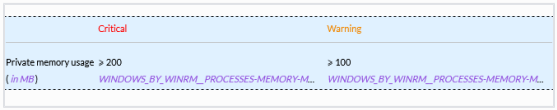
Exemple



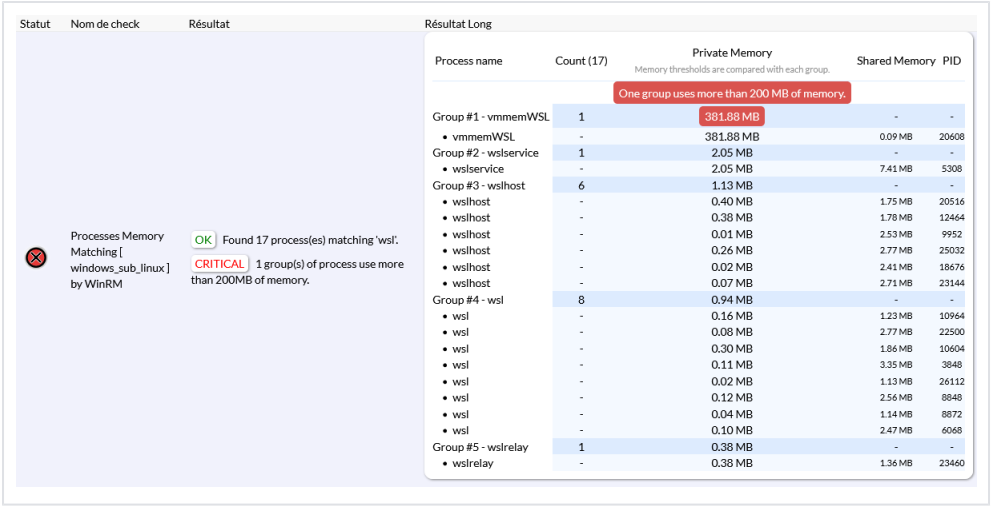
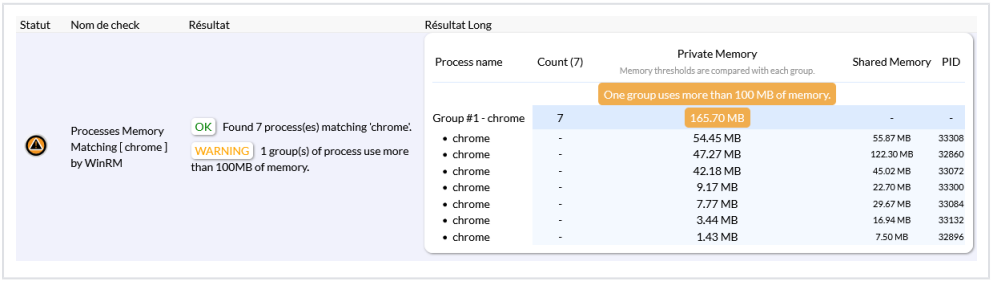
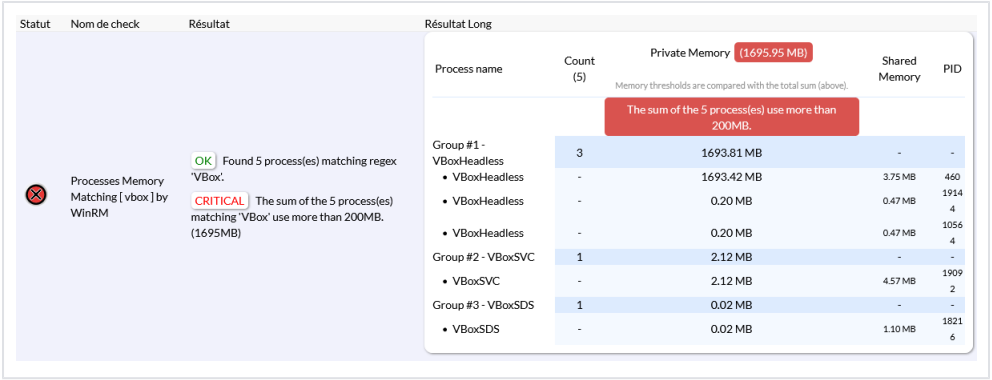
Interprétation

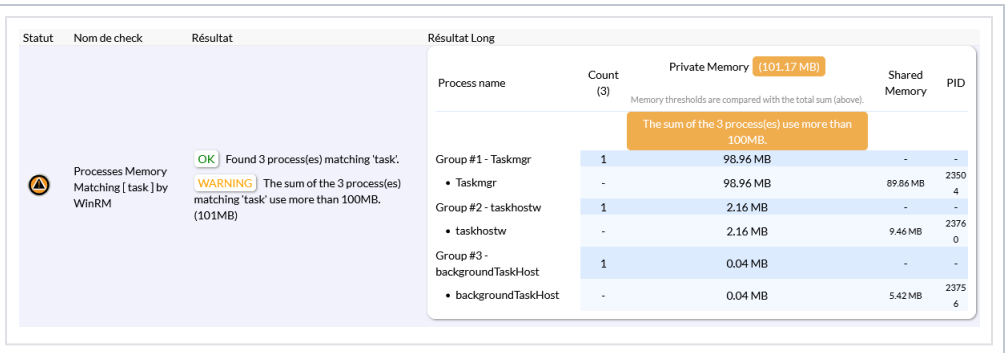
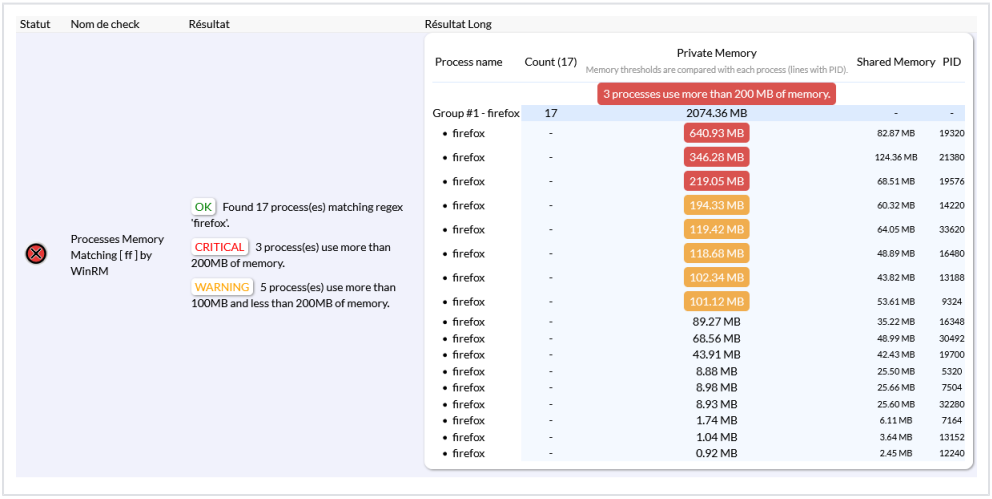
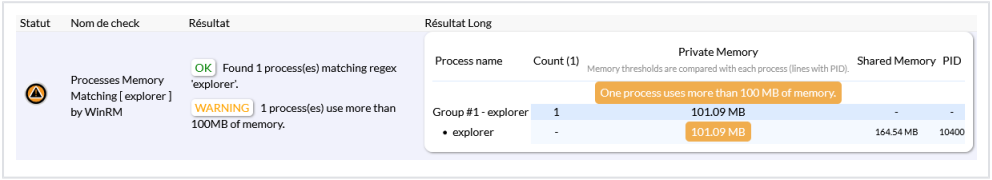
- Il peut prendre quatre valeurs ***OK*** / ***CRITIQUE*** / ***ATTENTION*** / ***INCONNU***
  - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
    - **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-WARN**
    - **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT**
    - **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MIN-PROCESS-COUNT**
    - **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MAX-PROCESS-COUNT**
  - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

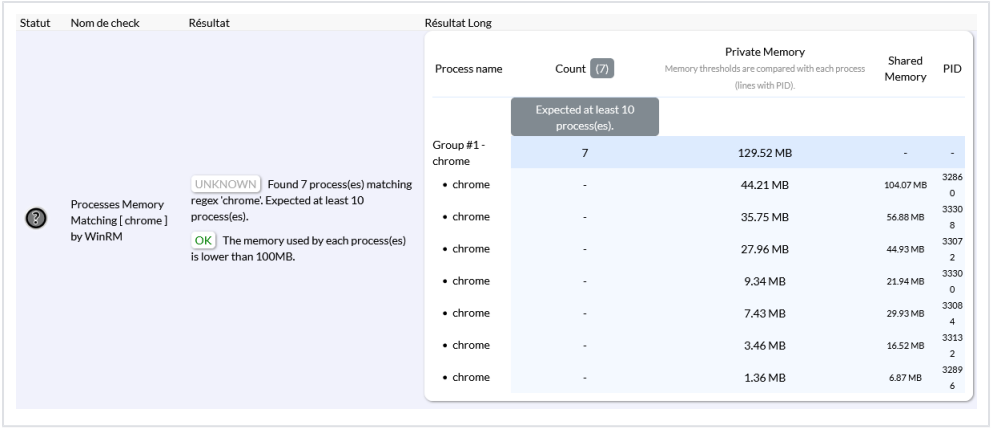
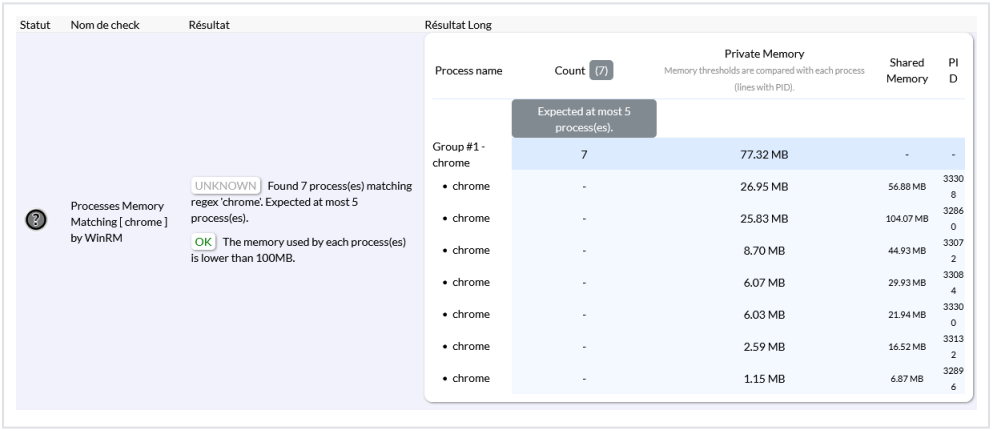
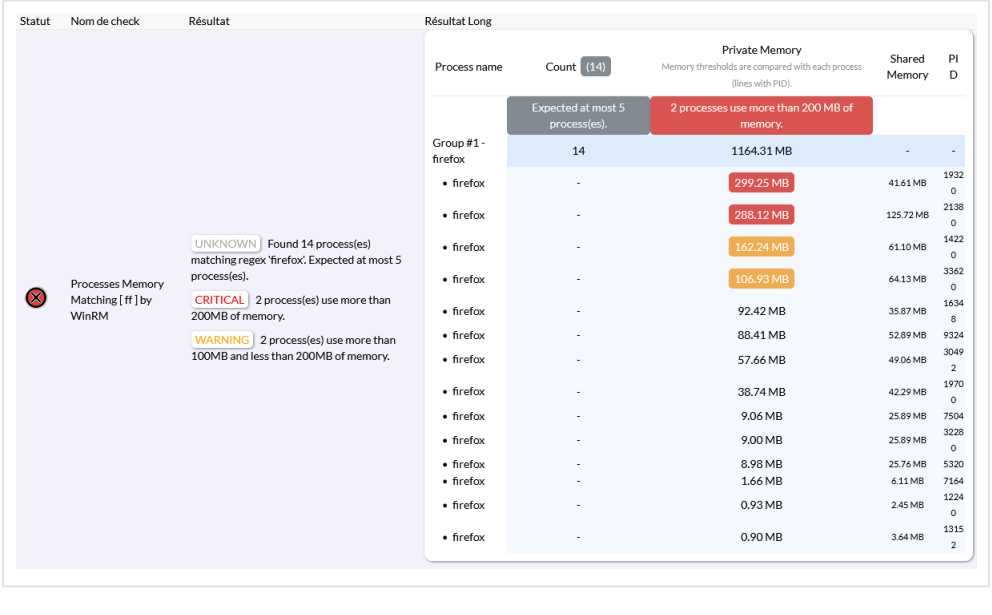
Le texte de la colonne "Affichage des seuils" montre les paramètres utilisés et leur valeur définie sur l'équipement supervisé.



Situation	*Statut*	*Exemple*

• **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "**group**", et la consommation mémoire d'un ou plusieurs groupes de processus dépasse **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT**	***CRITIQUE***	
• **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "**group**", et la consommation mémoire d'un ou plusieurs groupes de processus dépasse **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-WARN**	***ATTENTION***	
• **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "**sum**" et la somme de la consommation mémoire des processus dépasse **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT**	***CRITIQUE***	

• **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "**sum**" et la somme de la consommation mémoire des processus dépasse **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-WARN**	***ATTENTION***	
• **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "**process** " et la consommation mémoire d'un ou plusieurs processus dépasse **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT**	***CRITIQUE***	
• **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "**process** " et la consommation mémoire d'un ou plusieurs processus dépasse **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-WARN**	***ATTENTION***	

• Le nombre de processus trouvés correspondant aux filtres est inférieur à **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MIN-PROCESS-COUNT**	***INCONNU***	
• Le nombre de processus trouvés correspondant aux filtres est supérieur à **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MAX-PROCESS-COUNT**	***INCONNU***	
• Aucun processus correspondant aux filtres n'a été trouvé	***INCONNU***	
• Le nombre de processus trouvés correspondant aux filtres est supérieur à **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MAX-PROCESS-COUNT** et le seuil **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT** est dépassé. (*Le seuil de mémoire est prioritaire sur le retour de la sonde*).	***CRITIQUE***	

Résultat

Le résultat contient un message indiquant le status, si le ou les processus ont été trouvés, si la somme, les groupe ou les processus ne dépassent pas les limites de consommation mémoire fixés et si assez ou trop peu de processus trouvés correspondent aux filtres.

Résultat long

Le résultat long affiche un tableau de la consommation mémoire des processus trouvés correspondant aux filtres.

Le tableau regroupe chaque processus ayant le même nom dans des groupes numérotés, ainsi que la somme de leur mémoire privée.

Le tableau affiche sous chaque groupe, les processus trouvés avec leur consommation de mémoire privée, partagée ainsi que leur PID.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
--_PROCESS_MEMORY_SUM_--	MB	Somme de la consommation mémoire des processus surveillés en MB. Métrique uniquement générée lorsque **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "sum"	**WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-WARN**. Généré si **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "sum"	**WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT**. Généré si **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "sum"
(nom_du_groupe_de_processus)	MB	Consommation mémoire d'un groupe de processus en MB. Calculé à partir de la somme de la mémoire privée de chaque processus au sein du groupe. Généré pour chaque groupe de processus trouvé.	**WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-WARN**. Généré si **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "group"	**WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__MEMORY-CRIT**. Généré si **WINDOWS_BY_WINRM__PROCESSES-MEMORY-MATCHING__USE-MEMORY-THRESHOLD-ON** vaut "group"

Remarque

Il est possible de ne retourner aucune métrique en configurant l'option **PROCESS_HIDE_ALL** du check.

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
firefox	1983.34MB	100.00	200.00

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	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 :

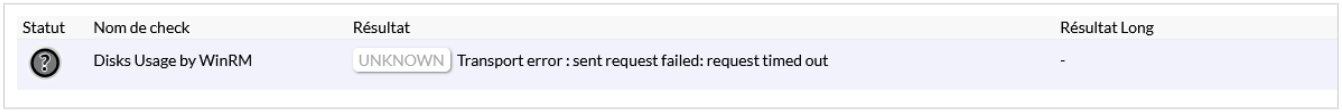
```
# Redémarrer le service WinRM :
Restart-Service WinRM

# 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.

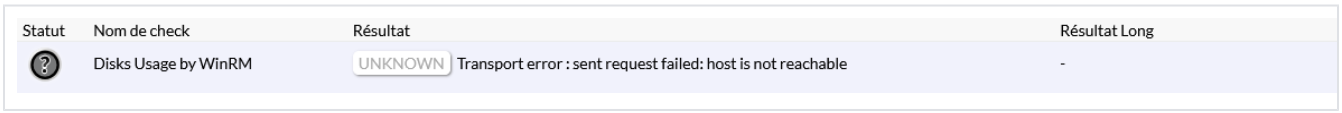
- Il se peut que vôte service WinRM ne soit pas lancé
- ou que votre pare-feu ne soit pas configuré.



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

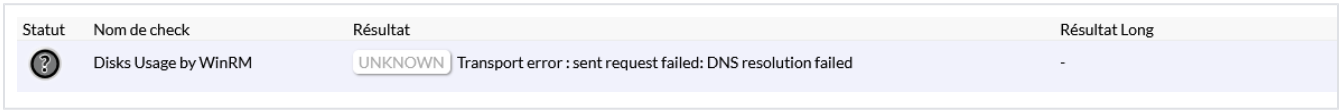
L'hôte n'a pas pu recevoir la requête. Vérifiez votre réseau, routeur, pare-feu et nom d'hôte.



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

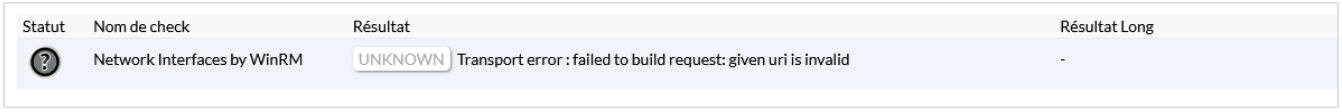
Le nom de l'hôte n'a pas pu être résolu. Vérifiez que l'adresse renseignée est correcte et que le serveur DNS est accessible.



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

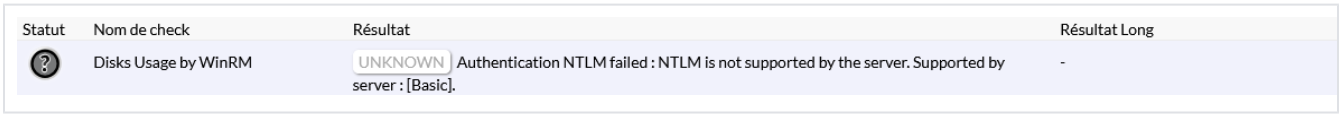
Le nom de l'hôte n'est pas une URI valide. Vérifiez que l'adresse renseignée est correcte.



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**"

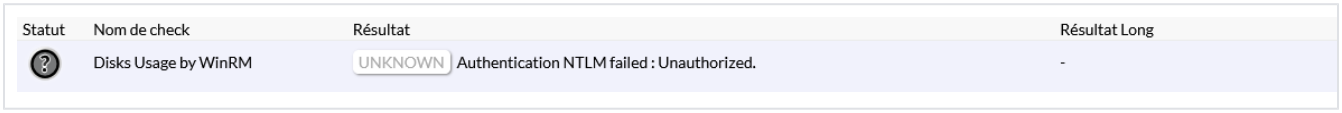
UNKNOWN – Authentication NTLM failed : Unauthorized

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



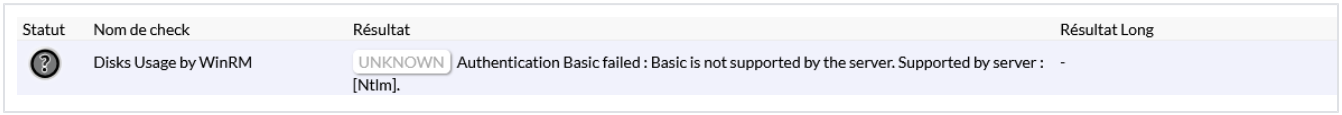
Statut	Nom de check	Résultat	Résultat Long
	Disks Usage by WinRM	UNKNOWN Authentication NTLM failed : Unauthorized.	-

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**"

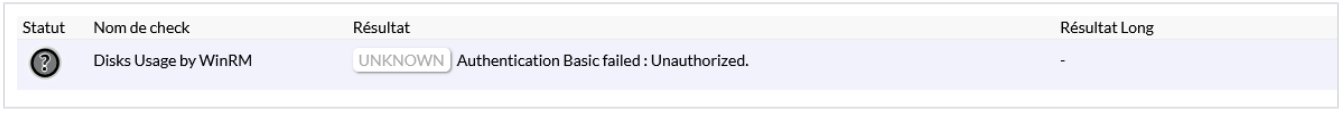
UNKNOWN – Authentication Basic failed : Unauthorized

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.	-

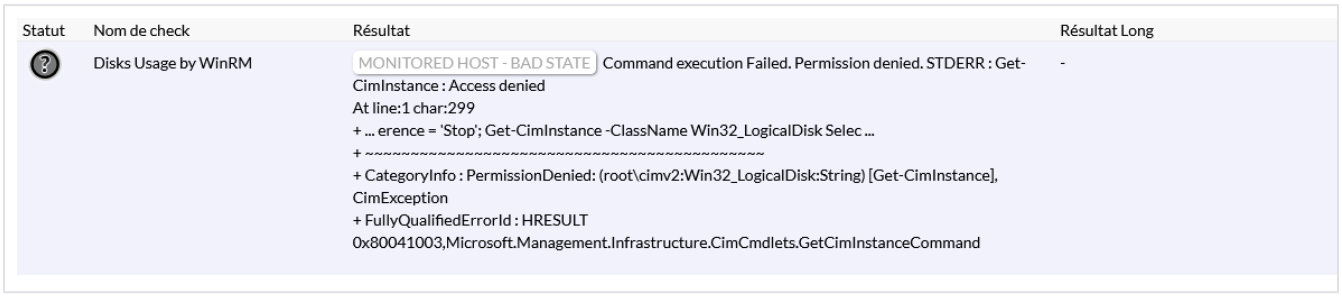
Résolution :

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	-

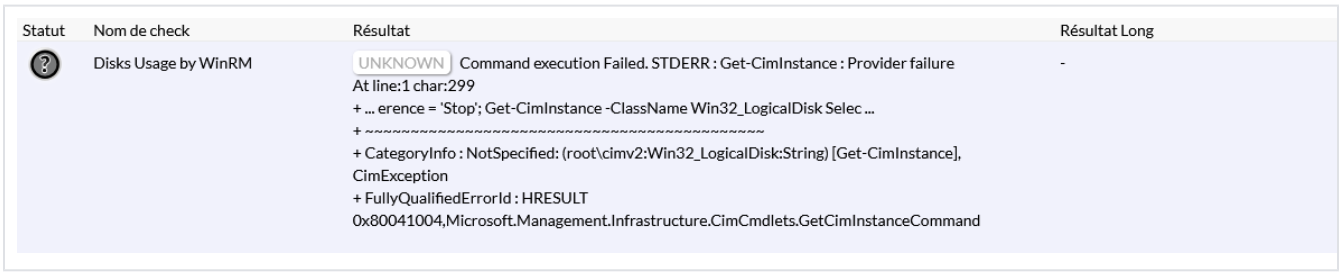
Résolution :

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.