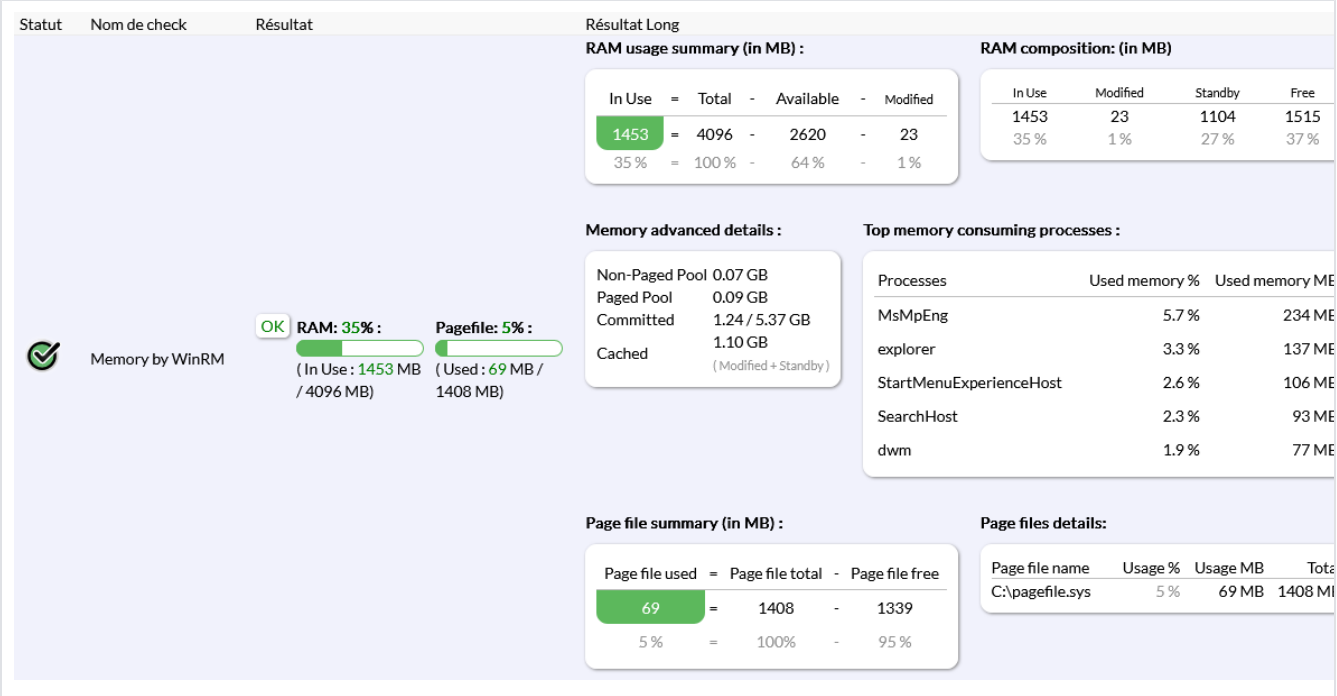
Memory by WinRM

Sommaire

Contexte

Le check **Memory by WinRM** va récupérer des informations concernant la mémoire vive et la mémoire des fichiers d'échange (*autrement appelé PAGEFILE ou SWAP sous linux*) de la machine supervisée, comme le pourcentage utilisé ainsi que le top 5 des processus consommant le plus de mémoire.

- Le statut de ce check possède 2 raisons de changer de statut :
  - Soit la consommation de mémoire **RAM** est trop élevée,
  - Soit la consommation de mémoire des fichiers d'échange (**PAGEFILE**) est trop élevée.
- Le statut du check sera donc le pire état des deux.



Paramétrage

Le check utilise la ligne de commande suivante :

```
$WINDOWS-BY-WINRM__SHINKEN__PLUGINSDIR$/check_windows_health_by_winrm_rust --check check_memory
    --hostname "$HOSTADDRESS$"
    --port "$_HOSTWINDOWS_BY_WINRM__PORT$"
    --username "$_HOSTWINDOWS_BY_WINRM__DOMAINUSER$"
    --password "$_HOSTWINDOWS_BY_WINRM__DOMAINPASSWORD$"
    --auth_method "$_HOSTWINDOWS_BY_WINRM__AUTHMETHOD$"
    --timeout "$_HOSTWINDOWS_BY_WINRM__TIMEOUT$"
    -w "$_HOSTWINDOWS_BY_WINRM__MEMORY__RAM-WARN$"
    -c "$_HOSTWINDOWS_BY_WINRM__MEMORY__RAM-CRIT$"
    -W "$_HOSTWINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN-WHEN-RAM-IS-
CRIT$,$_HOSTWINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN$"
    -S "$_HOSTWINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT-WHEN-RAM-IS-
CRIT$,$_HOSTWINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT$"
    -s
    -a
```

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__MEMORY__RAM-CRIT`	l'Hôte *(Onglet Données)*	%	*95*	Définit le pourcentage de mémoire **RAM** utilisée à partir duquel le check passe en **CRITIQUE**.
`WINDOWS_BY_WINRM__MEMORY__RAM-WARN`	l'Hôte *(Onglet Données)*	%	*90*	Définit le pourcentage de mémoire **RAM** utilisée à partir duquel le check passe en **ATTENTION** .
`WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT`	l'Hôte *(Onglet Données)*	%	*90*	Définit le pourcentage d'utilisation de mémoire des **fichiers d'échange** à partir duquel le check passe en **CRITIQUE** .
`WINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN`	l'Hôte *(Onglet Données)*	%	*70*	Définit le pourcentage d'utilisation de mémoire des **fichiers d'échange** à partir duquel le check passe en **ATTENTION** .
`WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT-WHEN-RAM-IS-CRIT`	l'Hôte *(Onglet Données)*	%	*20*	Définit le pourcentage d'utilisation de mémoire des **fichiers d'échange** à partir duquel le status des fichiers d'échange passe en **CRITIQUE** si la mémoire **RAM** est à plus de **WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**. Cela ne va pas influer le status de la sonde, car il sera **CRITIQUE** à cause du status de la **RAM**, cependant un affichage montrera l'état empiré des fichiers d'échange.
`WINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN-WHEN-RAM-IS-CRIT`	l'Hôte *(Onglet Données)*	%	15	Définit le pourcentage d'utilisation de mémoire des **fichiers d'échange** à partir duquel le status des fichiers d'échange passe en **ATTENTION** si la mémoire **RAM** est à plus de **WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**. Cela ne va pas influer le status de la sonde, car il sera **CRITIQUE** à cause du status de la **RAM**, cependant un affichage montrera l'état empiré des fichiers d'échange.

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

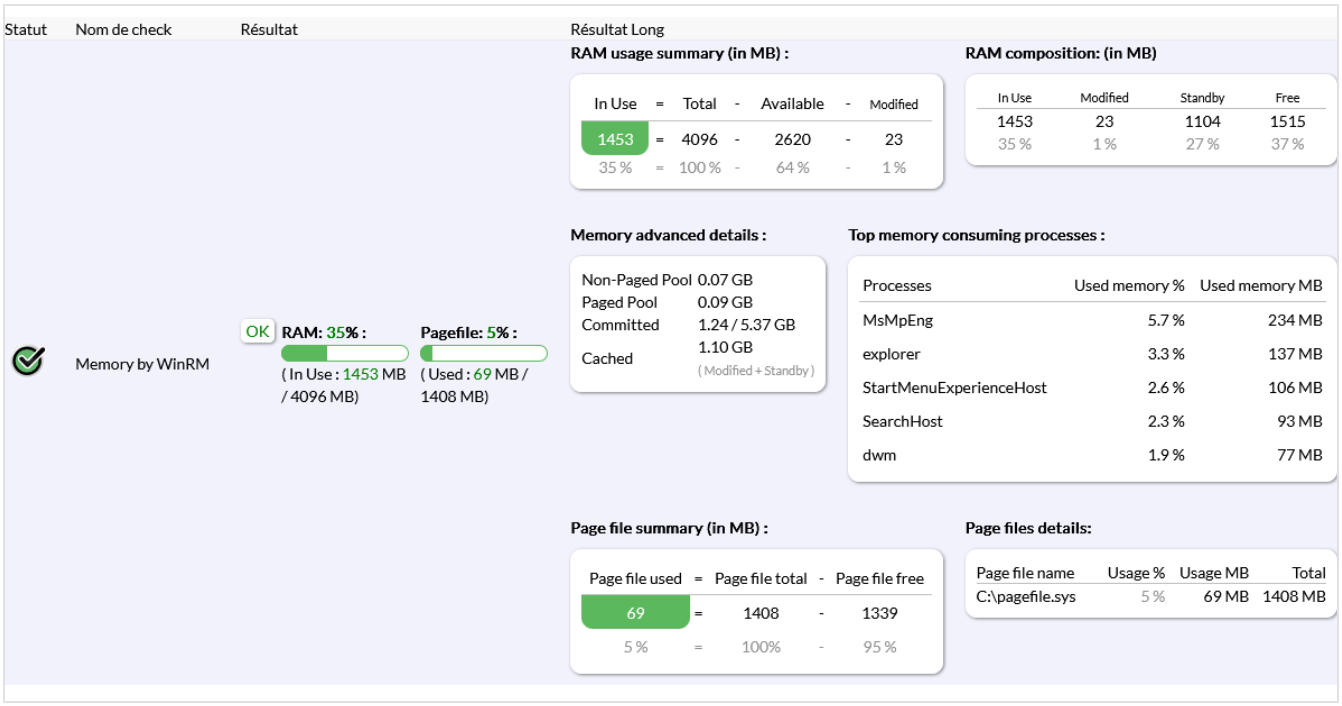
Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation	Description
`USERPLUGINSDIR`	Non modifiable *(Sauf Admin Shinken)*	--	/var/lib/shinken/libexec	**/var/lib/shinken/libexec**	Chemin absolu contenant les sondes installés par Shinken
`WINDOWS-BY-WINRM__SHINKEN__VENDOR`	Non modifiable *(Sauf 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

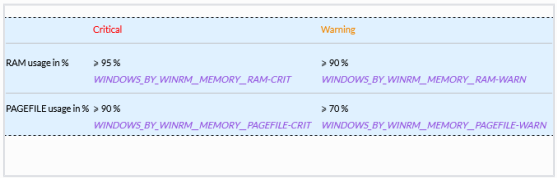
Exemple



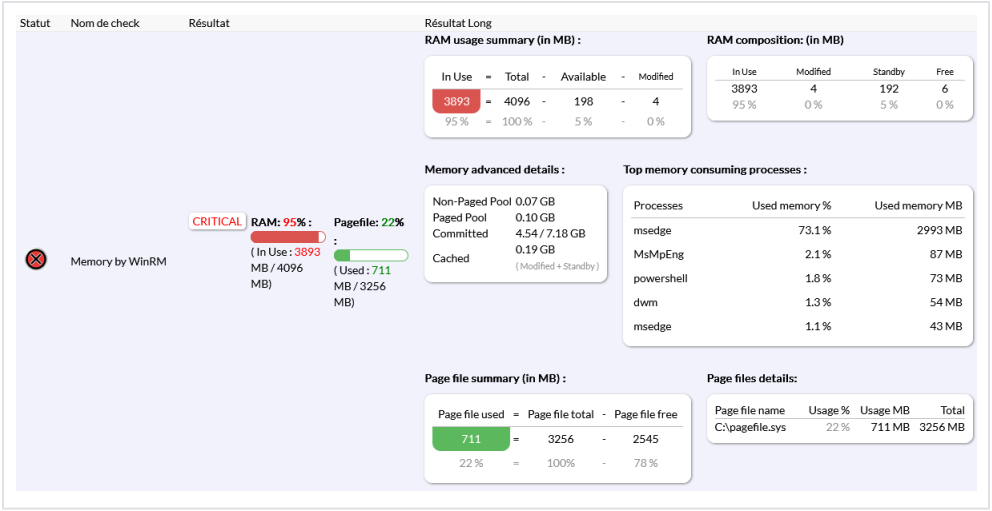
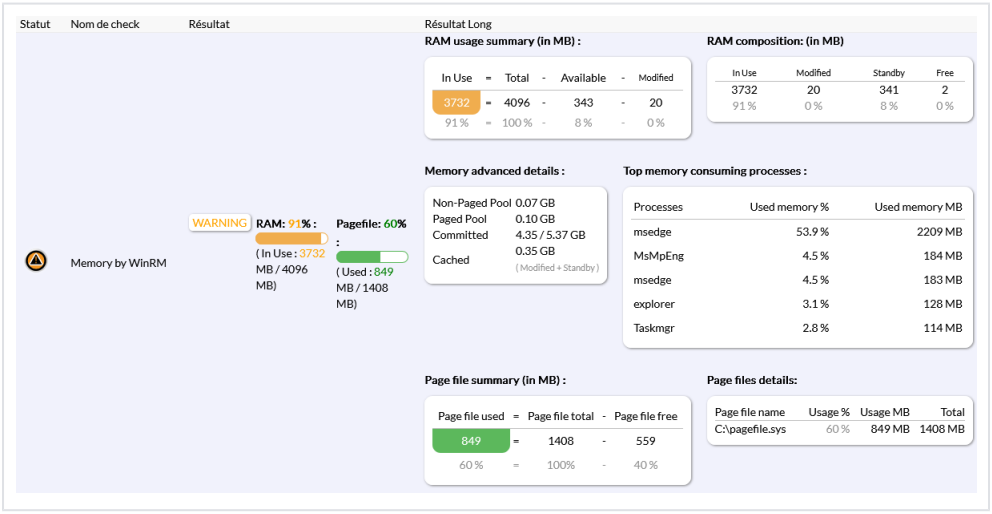
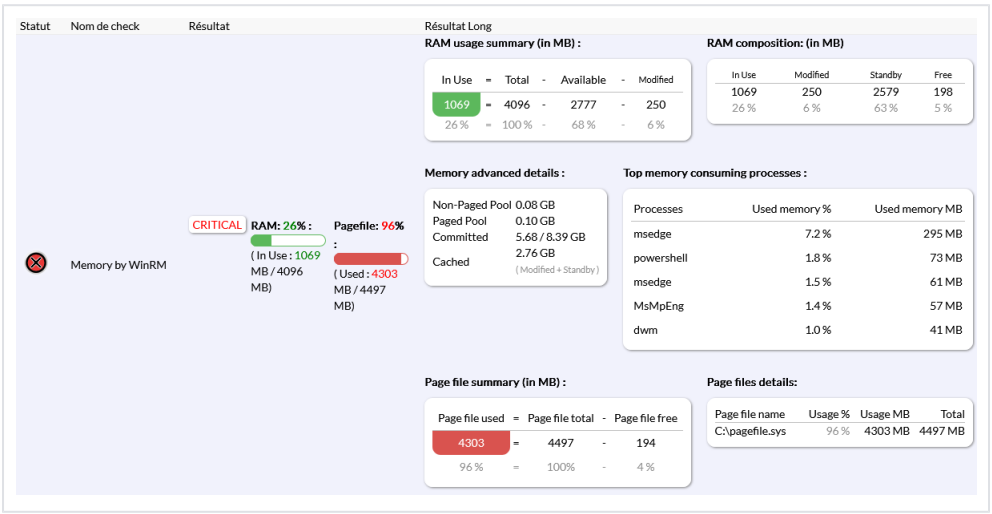
Interprétation

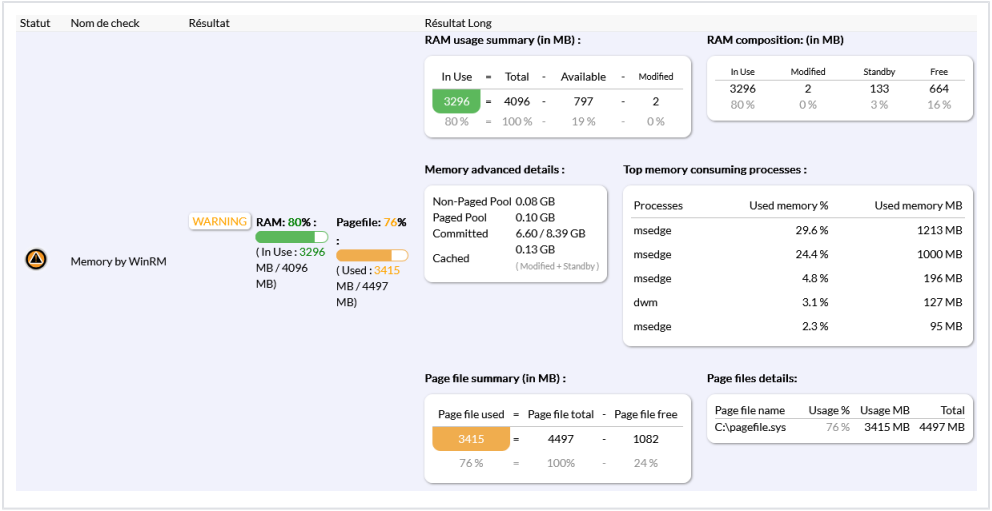
Statut

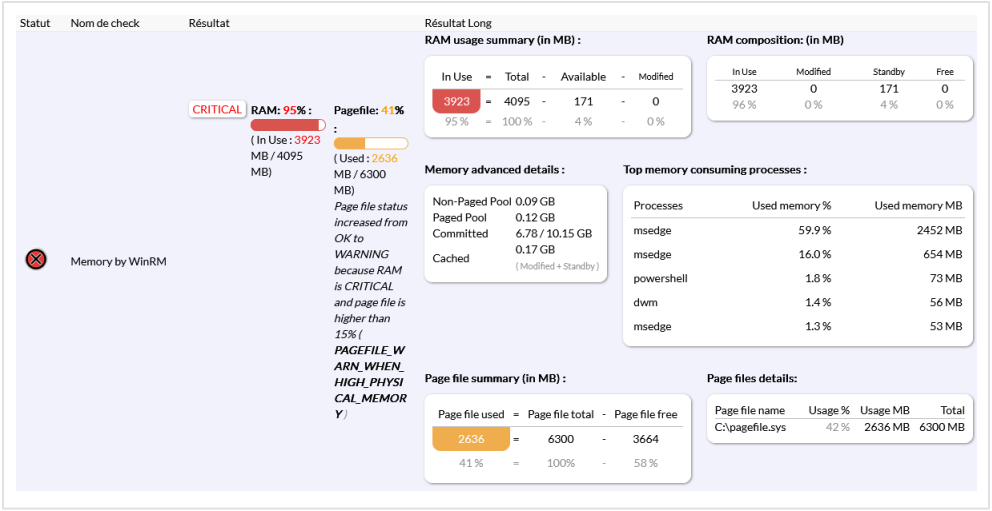
- Il peut prendre quatre valeurs ***OK*** / ***CRITIQUE*** / ***ATTENTION*** / ***INCONNU*** .
    - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
        - **WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**
        - **WINDOWS_BY_WINRM__MEMORY__RAM-WARN**
        - **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT**
        - **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-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.
>
> 
>

Situation	*Statut*	*Exemple*

• Le pourcentage de **RAM** dépassent la valeur de **WINDOWS_BY_WINRM__RAM-CRIT**.	***CRITIQUE***	
▪ Le pourcentage de **RAM** dépassent la valeur de **WINDOWS_BY_WINRM__MEMORY__RAM-WARN**.	***ATTENTION***	
• Le pourcentage de **PAGEFILE** dépasse la valeur de **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT**.	***CRITIQUE***	

• Le pourcentage de **PAGEFILE** dépasse la valeur de **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN**.	***ATTENTION***	
• Le pourcentage de **RAM** dépassent la valeur de **WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**.et le pourcentage de **PAGEFILE** est supérieur à **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT-WHEN-RAM-IS-CRIT.** (*Cela n'a pas d'effet direct sur le status de la sonde, car elle est déjà en* ***CRITIQUE*** *. Cependant, une indication visuelle montre l'état aggravé des fichiers d'échange.*)	***CRITIQUE***	

• Le pourcentage de **RAM** dépassent la valeur de **WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**.et le pourcentage de **PAGEFILE** est supérieur à **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN-WHEN-RAM-IS-CRIT.** (*Cela n'a pas d'effet direct sur le status de la sonde, car elle est déjà en **CRITIQUE** . Cependant , une indication visuelle montre l'état aggravé des fichiers d'échange.*)	***CRITIQUE***	

Résultat

Le résultat contient un message indiquant le statut ainsi que le pourcentage d'utilisation de la RAM et des fichiers d'échange.

Résultat Long

Le résultat long affiche :

- Un résumé de l'utilisation de la RAM, et comment la métrique "in_use" est calculée.
- La composition de la RAM : Comment l'ensemble de la mémoire disponible est répartie.
- Des détails avancés sur l'utilisation de la mémoire où les métriques suivantes sont affichées :
  - "non_paged_pool"
  - "paged_pool"
  - "committed"
  - "commit_limit"
  - "cached"
- Un tableau des cinq processus utilisant le plus de mémoire. C'est la mémoire privée de chaque processus qui est affichée ici.
- Un résumé de l'utilisation globale des fichiers d'échanges (*PAGEFILE*).
- Un tableau des fichiers d'échanges et de leur utilisation individuelle.

Métriques

Définition

Nom de la métrique	Unité	Description	Seuil d'avertissement	Seuil critique
in_use	%	Quantité de mémoire utilisés par les processus, pilotes ou système d'exploitation	**WINDOWS_BY_WINRM__MEMORY__RAM-WARN**	**WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**
available	%	Quantité de mémoire directement disponible à l'utilisation.	--	--
modified	%	Quantité de mémoire modifié. Cette mémoire necessite d'être écrite en disque avant d'être libérée.	--	--
standby	%	Quantité de mémoire en attente. Elle contient de la mémoire cache et des programmes qui ne sont pas activement utilisés.	--	--
free	%	Quantité de mémoire inutilisé.	--	--
committed	%	Quantité de mémoire virtuellement alloué aux processus, pilotes et système d'exploitation. Cette mémoire n'est pas forcément attribué physiquement. Le pourcentage est relatif à la limite "commit_limit_abs".	--	--
cached	%	Quantité de mémoire en cache par le système. C'est la somme de standby + modified	--	--

in_use_abs	MB	Quantité de mémoire utilisés par les processus, pilotes ou système d'exploitation	total_abs * **WINDOWS_BY_WINRM__MEMORY__RAM-WARN** / 100	total_abs * **WINDOWS_BY_WINRM__MEMORY__RAM-CRIT**/ 100
total_abs	MB	Quantité de mémoire disponible au système.	--	--
available_abs	MB	Quantité de mémoire directement disponible à l'utilisation.	--	--
modified_abs	MB	Quantité de mémoire modifié. Cette mémoire necessite d'être écrite en disque avant d'être libérée.	--	--
standby_abs	MB	Quantité de mémoire en attente. Elle contient de la mémoire cache et des programmes qui ne sont pas activement utilisés.	--	--
free_abs	MB	Quantité de mémoire inutilisé.	--	--
non_paged_pool_abs	MB	Quantité de mémoire du noyau windows et des pilotes de périphériques qui ne peut pas déborder dans la mémoire des fichiers d'échanges.	--	--
paged_pool_abs	MB	Quantité de mémoire du noyau windows et des pilotes de périphériques qui peut déborder dans la mémoire des fichiers d'échanges.	--	--
committed_abs	MB	Quantité de mémoire virtuellement alloué aux processus, pilotes et système d'exploitation. Cette mémoire n'est pas forcément attribué physiquement.	--	--
commit_limit_abs	MB	Quantité de mémoire attribuable. C'est la somme de la mémoire RAM total et la mémoire totale des fichiers d'échanges.	--	--
cached_abs	MB	Quantité de mémoire en cache par le système. C'est la somme de standby et modified.	--	--
page_file_used	%	Quantité de mémoire utilisés dans les fichiers d'échanges	**WINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN**	**WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT**
page_file_free	%	Quantité de mémoire disponible dans les fichiers d'échanges	--	--
page_file_total_abs	MB	Quantité de mémoire totale dans les fichiers d'échanges.	--	--
page_file_used_abs	MB	Quantité de mémoire utilisés dans les fichiers d'échanges	page_file_total_abs * **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-WARN** / 100	page_file_total_abs * **WINDOWS_BY_WINRM__MEMORY__PAGEFILE-CRIT** / 100
page_file_free_abs	MB	Quantité de mémoire disponible dans les fichiers d'échanges	--	--

Exemple

Métriques :

Métrique	Valeur	Seuil d'avertissement	Seuil critique
in_use	27.02%	90.00	95.00
available	71.06%		
modified	1.91%		
standby	18.73%		
free	52.34%		
committed	20.29%		
cached	20.64%		
in_use_abs	1106.65MB	3686.00	3890.77
total_abs	4095.55MB		
available_abs	2910.48MB		
modified_abs	78.43MB		
standby_abs	766.96MB		
free_abs	2143.52MB		
non_paged_pool_abs	58.27MB		
paged_pool_abs	74.20MB		
committed_abs	974.04MB		
commit_limit_abs	4799.55MB		
cached_abs	845.39MB		
page_file_used	0.00%	70.00	90.00
page_file_free	100.00%		
page_file_total_abs	704.00MB		
page_file_used_abs	0.00MB	492.80	633.60
page_file_free_abs	704.00MB		

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 :

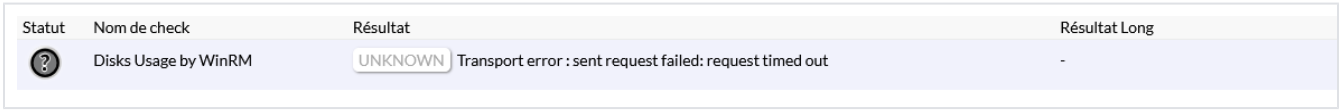
```
# Redémarrer le service WinRM :
Restart-Service WinRM

# 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.

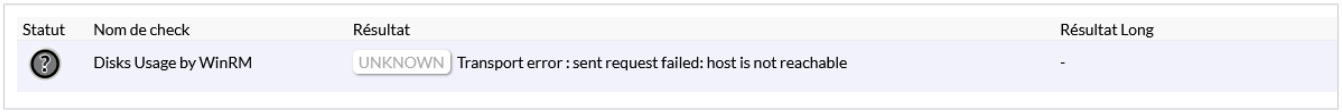
- Il se peut que vôte service WinRM ne soit pas lancé
- ou que votre pare-feu ne soit pas configuré.



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

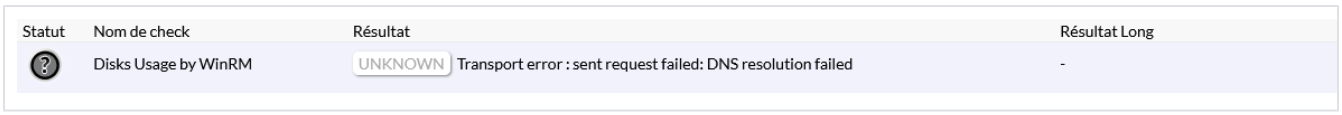
L'hôte n'a pas pu recevoir la requête. Vérifiez votre réseau, routeur, pare-feu et nom d'hôte.



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

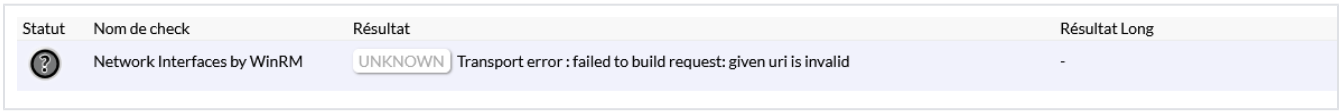
Le nom de l'hôte n'a pas pu être résolu. Vérifiez que l'adresse renseignée est correcte et que le serveur DNS est accessible.



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

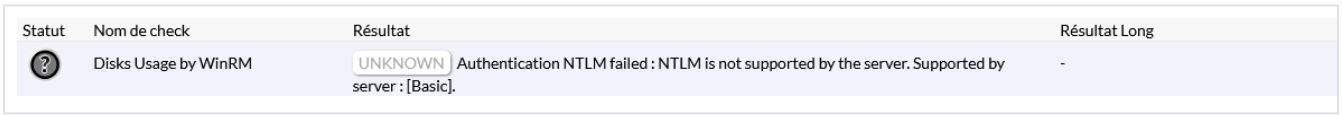
Le nom de l'hôte n'est pas une URI valide. Vérifiez que l'adresse renseignée est correcte.



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.