Mise en place du Pack windows

Procédure de mise en place du pack

Installation des sondes du pack

Les sondes du pack (*et leurs dépendances*) sont installées et mis à jour automatiquement par Shinken si votre source "**cfg-file-shinken**" est activée.

Import des modifications suite à une mise à jour de Shinken

Suite à une mise à jour de Shinken, et si le pack switch a été modifié, la source "cfg-file-shinken" sera réimporter (*si active*) :

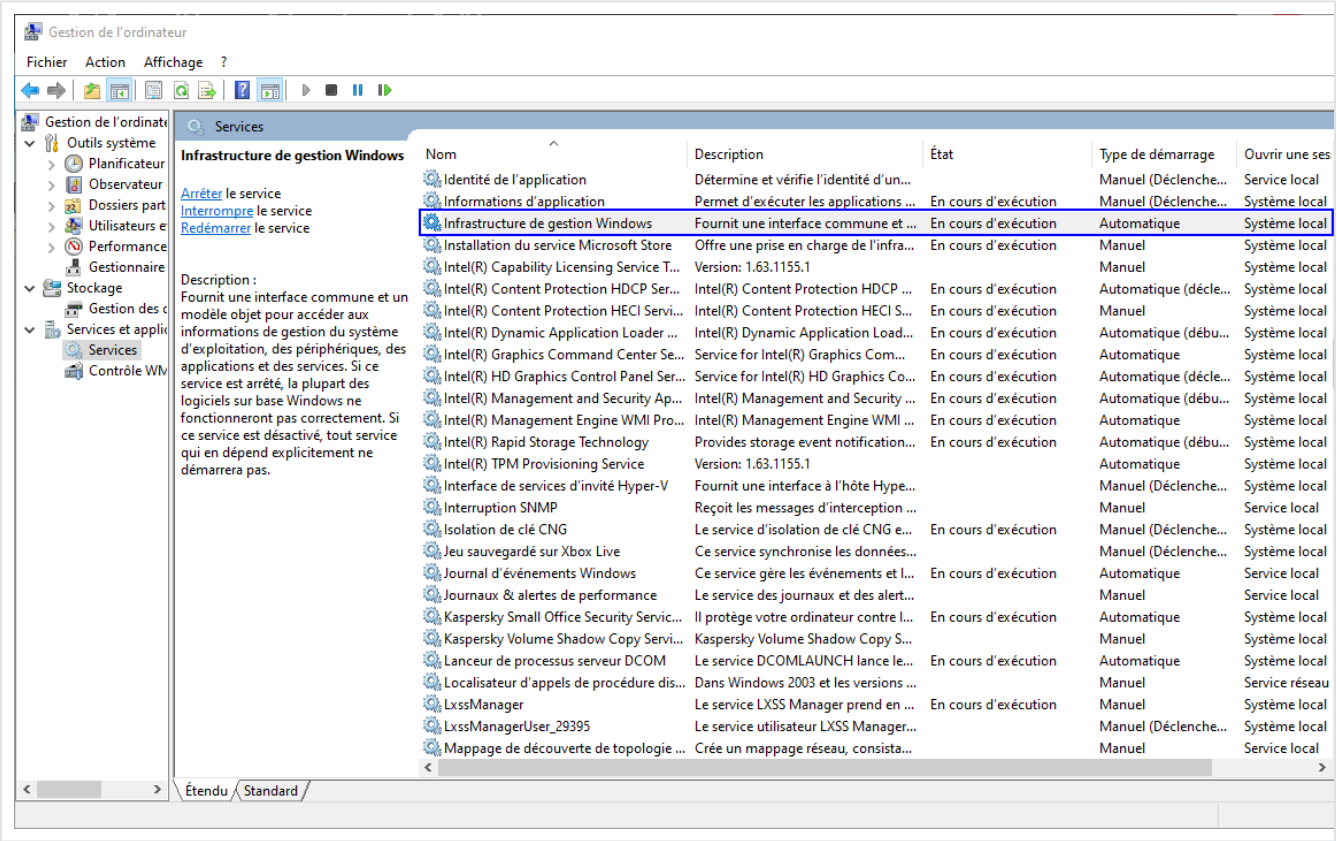
- Des différences vous seront proposées pour mettre à jour les éléments du pack (*modèles d'hôtes, checks, commande, etc..*).
- Nous vous conseillons d'accepter les nouveaux éléments et les différences de cette source afin de profiter des dernières mises à jour.

Fonctionnement WMI sur poste client ou serveur Windows

Windows Management Instrumentation (*infrastructure de gestion Windows*)

Le service **WMI** est installé et démarré par défaut sur les systèmes d'exploitations Windows.

Vous pouvez aller vérifier si ce service est bien démarré en vous rendant dans le gestionnaire de service Windows :



Si vous utilisez des firewall :

- Le Poller doit être autorisé à communiquer avec l'hôte supervisé.
- Les ports **WMI** de cet hôte doivent être ouverts : les ports TCP 135 et 445 ainsi que des ports dynamiques, typiquement dans le range de 1024 à 1034, doivent être accessibles.

WMI Avancé - gestion de la sécurité

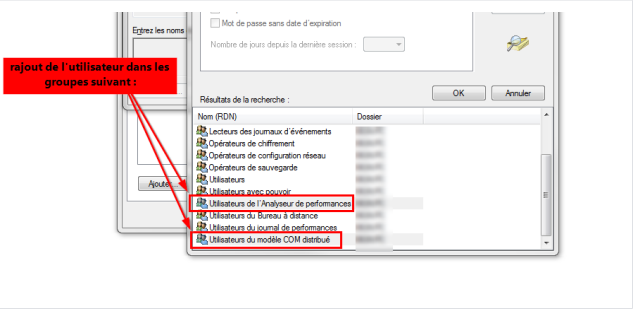
Comme on l'a vu précédemment, les commandes **WMI** requièrent une authentification au préalable afin de récupérer des informations de supervision sur l'hôte windows. (*-u "$_HOSTDOMAINUSER$" -p "$_HOSTDOMAINPASSWORD$"*)

L'utilisation du compte d'administrateur du poste Windows permet facilement d'obtenir ces informations avec succès, car ce compte à tous les droits d'accès (*WMI, DCOM, etc.*).

Cependant, pour des raisons de sécurité, il se peut que vous préfériez utiliser un compte avec des droits plus restreints.

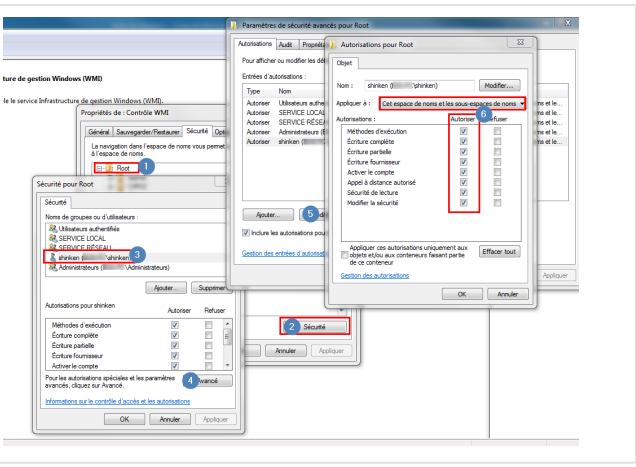
Voici donc la procédure à suivre pour rajouter des droits à un utilisateur basique qui vous servira à récupérer les informations **WMI** souhaitées.

Une fois que vous avez créé votre utilisateur sur le poste client ou sur votre domaine, ouvrez la console de "gestion de l'ordinateur" (*compmgmt.msc*) sur le poste à superviser, et rajoutez à l'utilisateur les droits suivants : Utilisateurs du modèle COM distribué (*Distributed COM Users*) et Utilisateurs de l'Analyseur de performance (*Performance Monitor Users*) :



Il faut à présent rajouter les droits sur le contrôle **WMI**, pour cela, depuis la console de "gestion de l'ordinateur" :

- cliquez sur Services & Applications,
- cliquez sur Contrôle WMI,
- clic droit - Propriété,
- sélectionnez l'onglet Sécurité,
- sélectionnez Root (***1***),
- cliquez sur le bouton de Sécurité en bas (***2***),
- rajoutez votre utilisateur (***3***),
- allez dans les propriétés avancées (***4***),
- modifiez la sécurité de l'utilisateur (***5***),
- rajoutez-lui toutes les autorisations et l'application doit se faire à "Cet espace de noms et les sous-espaces de noms" (***6***),
- cliquez sur OK sur toutes les fenêtres.



Veuillez ouvrir la console des services (*services.msc*) et redémarrez le service gérant la partie **WMI** : "Infrastructure de gestion Windows".

Votre check (*via l'utilisateur spécifique passé en paramètre*) doit maintenant pouvoir passer une requête **WMI** à cet ordinateur depuis votre commande Shinken.

Sur les neuf, un seul check peut poser un problème, c'est la requête qui interroge les services Windows via le check "Services". Ce check va vous renvoyer une erreur :

```
UNKNOWN - The WMI query had problems. The error
text from wmic is: [wmi/wmic.c:212:main()] ERROR:
Retrieve result data. NTSTATUS: NT code 0x80041003
- NT code 0x80041003
```

Voyons comment résoudre ce problème dans la prochaine section.

Déléguer des droits d'accès minimum à un utilisateur ou un groupe sur les services Windows

Ce paragraphe aborde les problèmes liés au check "Services" du pack windows lorsqu'un utilisateur non administrateur est utilisé. Veuillez vous référer au paragraphe précédent pour la mise en place d'un tel utilisateur sur Windows.

Ce check supervise l'état de tous les services configurés pour un démarrage automatique et bascule en état CRITIQUE si l'un de ces services n'est pas en cours d'exécution en raison d'une pause ou d'un arrêt.
Cependant, pour des raisons de sécurité, Windows restreint les droits d'interrogation de l'état des services pour les utilisateurs qui ne sont pas administrateurs. Initialement votre utilisateur ne devrait pas avoir le droit de consulter le statut des services.
Par conséquent, dans cette configuration, la gamme des services supervisés check est incomplète.

Les étapes suivantes permettent de completer le nombre de services supervisés pour un utilisateur non administrateur.

L'ensemble des étapes suivantes nécessite d'utiliser l'interpréteur Powershell comme administrateur.

Lancer l'interpréteur de commande comme administrateur :

- Dans la barre de recherche Windows, tapez PowerShell pour trouver l'interpréteur de commande PowerShell.
- Faite : Exécuter en tant qu'administrateur

Étape 1 : Trouver le SID de l'utilisateur

Le SID (*identifiant de sécurité*) d'un utilisateur est l'identifiant utilisé par Windows pour la gestion des autorisations. Les commandes suivantes permettent de retrouver le SID de l'utilisateur auquel vous souhaitez ajouter le privilège d'interroger les services. Initialement un utilisateur non-administrateur ne dispose pas des droits pour questionner ,démarrer, stopper ou mettre en pause les statuts des services.

Lister les utilisateurs :

```
Get-LocalUser
```

Exemple :

```
PS C:\WINDOWS\system32> Get-LocalUser

Name Enabled Description
---- ------- -----------
Administrateur False Compte d’utilisateur d’administration
b.martin True
DefaultAccount False Compte utilisateur géré par le système.
Invité False Compte d’utilisateur invité
support True
WDAGUtilityAccount False Compte d’utilisateur géré et utilisé par le système pour les
scénarios Windows Defender Application Guard.
```

Déterminer le SID (*identifiant de sécurité*) de l'utilisateur auquel ajouter les autorisations : Le SID est nécessaire dans la gestion des autorisations des services.

```
Get-LocalUser -Name "nom de l'utilisateur" | Select sid
```

Exemple :

```
PS C:\WINDOWS\system32> Get-LocalUser -Name 'b.martin' | Select sid

SID
---
S-1-5-21-2162771329-948085556-1632624503-1001
```

Étape 2 : Accorder à votre utilisateur les droits d'interroger le service 'Scmanager'

Le service SCManager est un composant du système d'exploitation Windows qui est responsable de la gestion des services. Il est chargé de créer, supprimer et contrôler les services présents sur un ordinateur exécutant Windows. Ce service permet d'interroger l'état des autres services sur la machine. Toutefois, pour des raisons de sécurité, Windows limite la sortie de ce service pour un utilisateur non-administrateur et il faudra par la suite ajouter à la main les services exclus.

Lister les autorisation du service scmanager :

```
sc.exe sdshow scmanager
```

La sortie de cette commande liste les autorisations accordées aux utilisateurs du service scmanager.

Exemple :

```
PS C:\Users\Administrator> sc.exe sdshow scmanager

D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(A;;CCLCRPRC;;;
LA)(A;;CCLCRPRC;;;LA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

Voir le paragraphe **Interpréter le Security Descriptor Definition Language (SDDL)** si vous souhaitez comprendre la sortie de la commande.

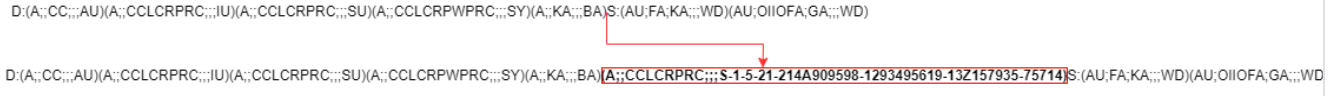
Accorder les permissions à votre utilisateur :

En utilisant l'invite commande :

- Copier l'output (*SDDL*) et coller-le dans un éditeur de texte.
  - Le résultat devrait ressembler à la ligne suivante :
    - D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
- Ajouter la permission suivante : **(A;;CCLCRPRC;;;SID de l'utilisateur)**.
  - Le résultat devrait ressembler à la ligne suivante :
    - D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)**(A;;CCLCRPRC;;;S-1-5-21-214A909598-1293495619-13Z157935-75714)**S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
- Puis utiliser la commande "sc.exe sdset" pour mettre à jour les permissions.

Le format d'une autorisation est le suivant : **(A;;Pairs d'autorisation;;; SID)**

Exemple




```
sc.exe sdset scmanager "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)
(A;;CCLCRPRC;;;S-1-5-21-214A909598-1293495619-13Z157935-75714)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
```

Si vous pensez avoir fait une erreur, il vous suffit de d'appliquer la commande avec l'état initial des autorisations pour annuler les modifications que vous auriez pu faire.

A la fin de cette étape, la supervision des services réalisée par votre check n'est pas exhaustive. Les étapes suivantes vous permettront de déterminer les services non pris en compte par le check et de les superviser.

Étape 3 : Determiner les services non superviser

Lister les services en démarrage automatique de votre machine Windows :

```
Get-Service | Where-Object { $_.StartType -eq 'Automatic' }
```

Exemple:

```
PS C:\Windows\system32> Get-Service | Where-Object { $_.StartType -eq 'Automatic' }

Status   Name               DisplayName
------   ----               -----------
Running  ApHidMonitorSer... AlpsAlpine HID Monitor Service
Running  AudioEndpointBu... Générateur de points de terminaison...
Running  Audiosrv           Audio Windows
Running  AVP21.9            Kaspersky Small Office Security Ser...
Running  BFE                Moteur de filtrage de base
Running  BITS               Service de transfert intelligent en...
Running  BrokerInfrastru... Service d’infrastructure des tâches...
Running  CDPSvc             Service de plateforme des appareils...
Running  CDPUserSvc_27ed576 Service pour utilisateur de platefo...
Running  CoreMessagingRe... CoreMessaging
Running  cplspcon           Intel(R) Content Protection HDCP Se...
...
```

Lister les services supervisés par votre check :

Depuis une machine où vous avez installé Shinken, lancer la commande suivante

```
/var/lib/shinken/libexec/wmic -U [domain/]adminuser%password //host  "select
Caption,  Name  from  Win32_Service where StartMode='Auto'"
```

Exemple

```
/var/lib/shinken/libexec/wmic -U 'SHINKEN\nonAdminUser%nonAdminUser' //integrationwin-1  "select Caption,
Name  from  Win32_Service where StartMode='Auto'"


[librpc/rpc/dcerpc_connect.c:329:dcerpc_pipe_connect_ncacn_ip_tcp_recv()] failed NT status (c00000b5) in
dcerpc_pipe_connect_ncacn_ip_tcp_recv
[librpc/rpc/dcerpc_connect.c:790:dcerpc_pipe_connect_b_recv()] failed NT status (c00000b5) in
dcerpc_pipe_connect_b_recv
CLASS: Win32_Service
Caption|Name
Active Directory Web Services|ADWS
Background Tasks Infrastructure Service|BrokerInfrastructure
DCOM Server Process Launcher|DcomLaunch
DFS Namespace|Dfs
DHCP Client|Dhcp
DNS Client|Dnscache
Windows Event Log|EventLog
Kerberos Key Distribution Center|Kdc
```

Les services retournés par la première commande et non par la seconde sont les services exclus par Windows. Il faut donc rajouter les autorisations de les interroger.

Étape 4 : Accorder à votre utilisateur les droits d'interroger le statut d'un service

Cette étape est à répéter pour chaque service auquel vous souhaitez rajouter les droits d'interroger le statut.

Lister les autorisations du service :

(Le nom du service est son nom cours qui correspond à la seconde colonne 'Name' des commandes précédentes)

```
sc.exe sdshow 'nom du service'
```

Exemple :

(Le nom ADWS correspond au service Active Directory Web Services)

```
PS C:\Users\Administrator> sc.exe sdshow ADWS


D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;
SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Voir le paragraphe **Interpréter le Security Descriptor Definition Language (SDDL)** si vous souhaitez comprendre la sortie de la commande.

Accorder les permissions à votre utilisateur:

En utilisant l'invite commande :

- Copier l'output (*SDDL*) et collez-le dans un éditeur de texte.
  - Le résultat devrait ressembler à la ligne suivante :
    - D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
- Ajouter la permission suivante : **(A;;CCLCLO;;;SID de l'utilisateur)**.
  - Le résultat devrait ressembler à la ligne suivante :
    - D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)**(A;;CCLCLO;;;S-1-5-21-214A909598-1293495619-13Z157935-75714)**S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
- Puis utiliser la commande "sc.exe sdset" pour mettre à jour les permissions.

Pour rappel le format d'une autorisation est le suivant : **(A;;Pairs d'autorisation;;; SID)**

```
sc.exe sdset ADWS "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;
CCLCLO;;;S-1-5-21-214A909598-1293495619-13Z157935-75714)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
```

Si vous pensez avoir fait une erreur, il vous suffit d'appliquer la commande avec l'état initial des autorisations pour annuler les modifications que vous auriez pu faire.

Désormais le statut du service ADWS et superviser par le check. **Cette étape est à répéter pour tous les services que vous souhaitez superviser.**

Interpreter le Security Descriptor Language (SDDL)

Interpréter le résultat de la commande :

Il y a deux sections :

- 'D:' qui correspond aux listes de contrôle d'accès discrétionnaire (*DACL*).
  - Les listes de contrôle d'accès discrétionnaire (*DACL*) sont utilisées pour contrôler les autorisations accordées ou refusées à un utilisateur pour l'accès à un objet sécurisable (*dans notre cas, un service*).
- 'S:' qui correspond aux listes de contrôle d'accès au système (*SACL*).
  - Les listes de contrôle d'accès au système (*SACL*) sont utilisées pour contrôler les tentatives d'accès qui sont enregistrées.

Le résultat de la section DACL est écrit selon langage de définition de descripteur de sécurité (*SDDL*), qui décrit un descripteur de sécurité en tant que chaîne de texte.

```
A;;CCLCSWRPWPDTLOCRRC;;;SY
```

Le premier caractère est soit :

- A pour 'Allow' (*autoriser*)
- D pour 'Deny' (*refuser*).

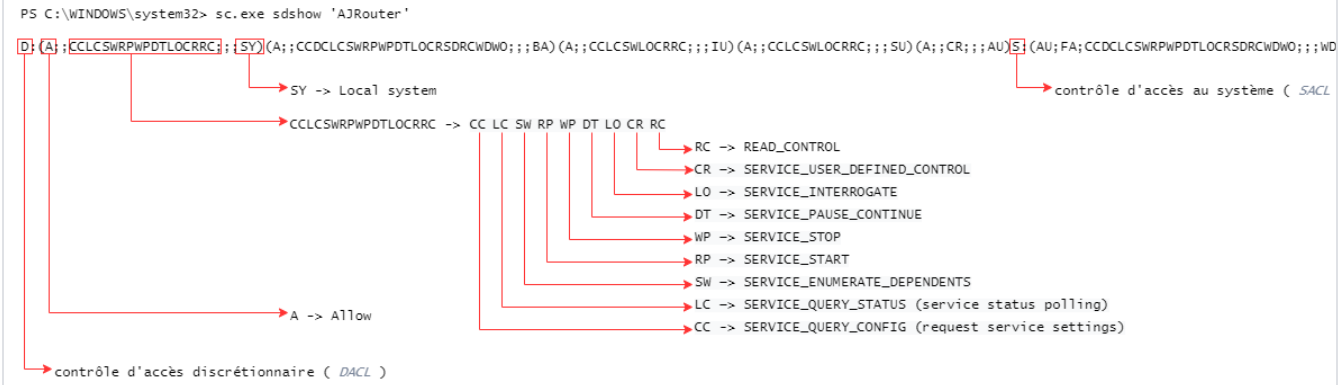
Les caractères du milieu se lisent par paire et correspondent à l'ensemble des permissions selon la relation suivante :

- CC — SERVICE_QUERY_CONFIG (*request service settings*)
- LC — SERVICE_QUERY_STATUS (*service status polling*)
- SW — SERVICE_ENUMERATE_DEPENDENTS
- LO — SERVICE_INTERROGATE
- CR — SERVICE_USER_DEFINED_CONTROL
- RC — READ_CONTROL
- RP — SERVICE_START
- WP — SERVICE_STOP
- DT — SERVICE_PAUSE_CONTINUE

Les deux derniers caractères précise pour quel groupe ou utilisateur la section s'applique selon la relation suivante :

- AU - Authenticated Users
- AO - Account operators
- RU - Alias to allow previous Windows 2000
- AN - Anonymous logon
- AU - Authenticated users
- BA - Built-in administrators
- BG - Built-in guests
- BO - Backup operators
- BU - Built-in users
- CA - Certificate server administrators
- CG - Creator group
- CO - Creator owner
- DA - Domain administrators
- DC - Domain computers
- DD - Domain controllers
- DG - Domain guests
- DU - Domain users
- EA - Enterprise administrators
- ED - Enterprise domain controllers
- WD - Everyone
- PA - Group Policy administrators
- IU - Interactively logged-on user
- LA - Local administrator
- LG - Local guest
- LS - Local service account
- SY - Local system
- NU - Network logon user
- NO - Network configuration operators
- NS - Network service account
- PO - Printer operators
- PS - Personal self
- PU - Power users
- RS - RAS servers group
- RD - Terminal server users
- RE - Replicator
- RC - Restricted code
- SA - Schema administrators
- SO - Server operators
- SU - Service logon user

Exemple



Résolutions des problèmes

Les checks n'arrivent pas à récupérer les informations alors que l'utilisateur utilisé est Administrateur

Après avoir mis en place le modèle dans Shinken et donné les bons droits à l'utilisateur Windows utilisé par le check, il se peut que les données de performances remontées par les checks ne puissent pas être remontées.

Il est possible dans ce cas que les valeurs de la bibliothèque du compteur de performances Windows soit corrompu ou contienne des valeurs incorrectes.

Dans ce cas, les checks Windows peuvent retourner les erreurs suivantes :

```
UNKNOWN - The WMI query had problems. The
error text from wmic is: [wmi/wmic.c:212:main()]
ERROR: Retrieve result data.
NTSTATUS: NT code 0x80041017 - NT code
0x80041017
```

```
UNKNOWN - The WMI query had problems. The plugin is having trouble finding the required WMI Classes on the
target host (172.16.0.132). There can be multiple reasons for this (please go through them and check)
including permissions problems (try using an admin login) or software that creates the class is not
installed (eg if you are trying to checkiis but IIS is not installed). It can also happen if your version of
Windows does not support this check (this might be because the WMI fields are named differently in different
Windows versions). Sometimes, some systems 'lose' WMI Classes and you might need to rebuild your WMI
repository. Sometimes the WMI service is not running, other times a reboot can fix it. Other causes include
mistyping the WMI namesspace/class/fieldnames. There may be other causes as well. You can use wmic from the
command line to troubleshoot. Wmic error text on the next line.
[wmi/wmic.c:212:main()] ERROR: Retrieve result data.
NTSTATUS: NT code 0x80041010 - NT code 0x80041010
```

Il est possible de recréer manuellement les valeurs de la bibliothèque du compteur de Performance avec la commande suivante :

```
lodctr /r
```

Plus d'informations sur la commande et ses possibilités peuvent être trouvées sur la page de documentation dédiée : https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/lodctr

Erreur : "Error: Can't locate perl58.dll"

Si un script retourne l'erreur :

```
Error: Can't locate perl58.dll" ou "Error: Can't locate perlXX.dll
```

Il faut installer/réinstaller ActivePerl

Erreur : "ERROR: Login to remote object."

Si le script retourne l'erreur suivante :

```
UNKNOWN - The WMI query had problems. The error text from wmic is: [wmi/wmic.c:196:main()] ERROR: Login to
remote object.
NTSTATUS: NT code 0x80010111 - NT code 0x80010111
```

C'est une erreur dû à l'élévation de sécurité imposée sur les dernières mises à jour de Windows.

- La mise à jour de Shinken Entreprise avec la dernière version disponible (*elle contient une version des modèles, des checks et de la commande **WMIC** qui corrige ce problème*).