Zone d'entête - Météo

Sommaire

Introduction

Le pack "**Windows**", permet de superviser des hôtes sur lesquels est installé le système d'exploitation Windows (*serveur ou client*).

Il contient :

- 15 commandes,
- 1 modèle d'hôte,
- 9 modèles de checks.

Les commandes du modèle Windows de notre pack se basent sur le script perl **check_wmi_plus.pl** présent dans le répertoire des scripts shinken **/var/lib/shinken/libexec** (*ou **$PLUGINSDIR$** depuis l'Interface de Configuration*).

WMI (*Windows Management Instrumentation*) est un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle de ressources systèmes via un ensemble d'interfaces. Le script perl permet d'interroger ces interfaces via un nom d'utilisateur et un mot de passe. Si l'utilisateur a les droits suffisants, alors le système d'exploitation Windows retournera l'information demandée.

Il utilise le modèle "**windows-base**" (*voir la page* Pack Windows-Base) pour obtenir les quatre données nécessaires pour la connexion à la machine Windows.

Le modèle d'hôte Windows et ses données héritées

Ce modèle contient des données (*locales*) qui seront utilisés par ses checks. Ces données seront utilisées par ses checks et leurs commandes en définissant **$_HOST** suivi du nom de la donnée.

> Exemple : **$_HOSTWINDOWS_ALL_CPU_CRIT$** utilisera la donnée nommée **WINDOWS_ALL_CPU_CRIT** (*qu'elle soit locale ou héritée d'un modèle*).

Si vous souhaitez modifier de manière globale ces données, ou en rajouter, faîtes le directement sur le modèle "**windows**".

? Unknown Attachment

Connexion et arguments de sécurité

Donnée	Valeur par défaut	Description
DOMAINUSERSHORT		Nom d'utilisateur utilisé, sans le domaine
DOMAINPASSWORD		Mot de passe de l'utilisateur
DOMAIN		Nom du domaine Active Directory du compte. Si vide, alors c'est le domaine du serveur qui sera utilisé, ou un compte local s'il n'est pas dans un domaine Active Directory.
DOMAINUSER		Nom complet utilisé pour se connecter, il faut par défaut DOMAINE\DOMAINUSERSHORT. • À n'utiliser que si vous ne souhaitez pas utiliser les variables DOMAINUSERSHORT et DOMAIN, et que votre connexion se fait sur un autre format que Domaine/utilisateur.

WINDOWS_SECURITY_MECANISMS	integrity	Niveau de sécurité utilisé pour se connecter sur le serveur Windows : • **integrity** : (*par défaut*) valeur de sécurité élevée • **connect**: valeur de sécurité faible, qui sera **bloquée** sur les serveurs Windows à partir de **mi-2022** (*voir la page l'article de microsoft sur le sujet*), à partir des serveurs windows 2008. ◦ Cette valeur ne doit être utilisée que sur de vieux serveurs qui ne gèrent pas les connexions au niveau *integrity*.

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 :

? Unknown Attachment

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*) :

? Unknown Attachment

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

? Unknown Attachment

- 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

Étape 1 : Trouver le SID de l'utilisateur ou du groupe

Pour que l'utilisateur puisse interroger les différents services Windows, il faut au préalable l'autoriser.

Par défaut, les utilisateurs locaux et les comptes non-administrateurs ne disposent pas des droits pour agréger les services locaux, ni pour interroger leurs statuts ou les redémarrer.

Lancer l'interpréteur de commande comme administrateur :

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

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.
```

Lister les groupes :

```
Get-WmiObject win32_group
```

Exemple :

```
PS C:\WINDOWS\system32> Get-WmiObject win32_group

Caption                                          Domain   Name                                    SID
-------                                          ------   ----                                    ---
B-MARTIN\Administrateurs                         B-MARTIN Administrateurs                         S-
1-5-32-544
B-MARTIN\Administrateurs Hyper-V                 B-MARTIN Administrateurs Hyper-V                 S-
1-5-32-578
B-MARTIN\Duplicateurs                            B-MARTIN Duplicateurs                            S-
1-5-32-552
B-MARTIN\IIS_IUSRS                               B-MARTIN IIS_IUSRS                               S-
1-5-32-568
B-MARTIN\Invités                                 B-MARTIN Invités                                 S-
1-5-32-546
B-MARTIN\Lecteurs des journaux d’événements      B-MARTIN Lecteurs des journaux d’événements      S-
1-5-32-573
...
```

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

Pour un **utilisateur**

```
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
```

Pour un **groupe**

```
(Get-WmiObject win32_group | Where-Object { $_.Name -eq "nom du groupe"} ).SID
```

Exemple:

```
PS C:\WINDOWS\system32> (Get-WmiObject win32_group | Where-Object { $_.Name -eq "Utilisateurs"} ).SID
S-1-5-32-545
```

Étape 2 : Trouver le service à modifier

Lister les services :

```
Get-Service
```

Exemple:

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

Status   Name               DisplayName
------   ----               -----------
Running  AarSvc_497de23     Agent Activation Runtime_497de23
Stopped  AJRouter           Service de routeur AllJoyn
Stopped  ALG                Service de la passerelle de la couc...
Stopped  AppIDSvc           Identité de l’application
Running  Appinfo            Informations d’application
...
```

Étape 3 : Modifier les permissions du service

Lister les autorisations d'un service :

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

Exemple:

```
PS C:\WINDOWS\system32> sc.exe sdshow 'AJRouter'

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

La commande précédente affiche le descripteur de sécurité d'un service en utilisant le Security Descriptor Definition 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
? Unknown Attachment

Exemple : Lister les permissions de scmanager

```
sc.exe sdshow
```

Accorder des permissions à utilisateur ou un groupe sur un service :

En utilisant l'invite commande :

- Copie 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;;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.

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

Exemple

? Unknown Attachment

```
sc.exe sdset 'nom du service' "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)"
```

Retirer des permissions à utilisateur ou un groupe sur un service :

Reprendre les étapes de la partie précédente et retirer les permissions.

```
sc.exe sdset 'nom du service' "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)"
```

Exemples d'utilisation :

- Autoriser un utilisateur à énumérer les services locaux Windows :

```
Get-LocalUser -Name 'utilisateur' | Select sid
sc.exe sdshow scmanager
sc.exe sdset scmanager "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)
(A;;CCLCRPRC;;;'SID')S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
```

- Autoriser un utilisateur à démarrer, stopper, mettre en pause et interroger un service Windows :

```
Get-LocalUser -Name 'utilisateur' | Select sid
sc.exe sdshow 'nom du service'
sc.exe sdset 'nom du service' "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;
KA;;;BA)(A;;RPWPDTLO;;;'SID')S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
```

Étape 4 : Utilisation dans le cadre de Shinken

Contrairement à l'utilisation du compte administrateur pour la vérification des services (*qui permet une vue exhaustive et totale*), **rajouter uniquement le droit d'énumerer les services pour un utilisateur ne permet pas de lister et vérifier tous les services.** Dans ce cas, il est nécessaire d'ajouter individuellement des droits pour interroger les services qui ne sont pas pris en compte.

Si vous utiliser un compte autre qu'un compte administrateur il faut procéder en deux étapes :

- Ajouter les droits **CCLCRPRC** sur le service scmanager pour votre utilisateur, ce qui autorisera cet utilisateur à énumérer les services locaux Windows
- Pour les services qui ne seront pas intégrés (*par exemple le service "Pare feu Windows"*), il faut leurs ajouter spécifiquement les droits **CCL CRPRC**.

La commande du pack Windows **check_windows_auto_services** retournera alors l'état des services (*en démarrage "automatique"*) pour un certain nombre de services Windows, ainsi que pour ceux sur lesquels vous avez rajouté les droits manuellement.

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 (*voir la page* https://www.activestate.com/products/perl/)

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*).