Actions de masse (Administrateur de SI)

Sommaire

Fonctionnement WinRM sur poste Windows client ou serveur

Windows Remote Management

Le service **WinRM** est installé par défaut sur les systèmes d'exploitations Windows, mais celui-ci n'est pas nécessairement démarré et configuré.

Voici la commande à exécuter via PowerShell pour vérifier si le service est bien démarré :

```
Get-Service WinRM
```

Exemple :

```
C:\Users\Administrateur> Get-Service WinRM

Status   Name               DisplayName
------   ----               -----------
Running  WinRM              Gestion à distance de Windows (Gest...
```

WinRM dispose d'une commande de configuration intégrée qui permet entre autres de :

- Démarrer le service
- Activer le démarrage automatique de celui-ci
- Mettre en place l'écouteur (HTTP ou HTTPS) pour recevoir les requêtes des sondes Shinken
- Configurer le Firewall Windows pour autoriser les accès vers l'écouteur

Pour effectuer les actions de configuration, il suffit d'exécuter la commande suivante :

```
winrm quickconfig
```

Exemple :

```
C:\Users\Administrateur> winrm quickconfig

WinRM n'est pas configuré pour la gestion à distance de cet ordinateur.
Les modifications suivantes doivent être effectuées :

Créez un écouteur WinRM sur HTTP://* pour accepter les demandes de la gestion des services Web sur toutes
les adresses IP de cet ordinateur.

Activez l'exception de pare-feu WinRM.
Configurez LocalAccountTokenFilterPolicy pour attribuer des droits d'administration à distance à des
utilisateurs locaux.

Effectuer ces modifications [y/n] ? y

WinRM a été mis à jour pour la gestion à distance.

Écouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestion des services Web sur toutes les
adresses IP de cet ordinateur.

Exception de pare-feu WinRM activée.
LocalAccountTokenFilterPolicy configuré pour attribuer des droits d'administration à distance à des
utilisateurs locaux.
```

WinRM - gestion de la sécurité

À l'image des commandes WMI (*voir la page Modèle windows-by-WMI__ntlmv2*), les commandes WinRM requièrent une authentification au préalable afin de récupérer les informations de supervision sur l'hôte windows. (*-u "$_HOSTDOMAINUSER$" -p "$_HOSTDOMAINPASSWORD$"*)

L'utilisation du compte administrateur du poste Windows permet d'obtenir toutes les informations du système, car celui-ci possède par défaut tous les droits d'accès (*WMI, DCOM, WinRM, etc.*).

Cependant, pour des raisons de sécurité, il n'est pas conseillé de l'utiliser pour effectuer la supervision.

Qu'il s'agisse d'un compte local ou d'un compte AD, voici la procédure pour créer un nouvel utilisateur dédié au monitoring avec les droits suffisant pour collecter les informations nécessaires au fonctionnement des sondes fournies par Shinken.

Création de l'utilisateur

La création est possible directement sur le poste local Windows, ou sur l'Active Directory.

Cela s'effectue dans la console de "**Gestion de l'ordinateur**" (*compmgmt.msc*) puis dans **Utilisateurs et groupes locaux > Utilisateurs,** clic droit et **Nouvel utilisateur...**

? Unknown Attachment

Configuration des groupes

Une fois le nouvel utilisateur créé sur le poste client ou sur le domaine, il faut ajouter l'utilisateur dans les groupes suivants : **Utilisateurs de gestion à distance** et **Utilisateurs de l'Analyseur de performances** sur le poste Windows concerné.

Cela s'effectue dans la console de "**Gestion de l'ordinateur**" (*compmgmt.msc*) puis dans **Utilisateurs et groupes locaux > Groupes,** clic droit sur le groupe puis **Propriétés**. Une nouvelle fenêtre s'ouvre, cliquer sur **Ajouter…** :

> Sur certaines distributions inférieures à Windows 2012, le groupe "**Utilisateurs de gestion à distance**" et sa fonction n'existent pas.

? Unknown Attachment

Configuration de la langue

Pour assurer l'interprétation des commandes Windows par la sonde, il est nécessaire de configurer la langue du nouvel utilisateur.

Tout d'abord, il faut changer de compte Windows pour se connecter à celui du nouvel utilisateur. Il est ensuite possible de configurer la langue par interface ou par ligne de commande.

Par interface

Lancer les paramètres Windows puis accéder à la catégorie "Time & Language".

? Unknown Attachment

Ensuite accéder à la sous-catégorie "**Language**".

Maintenant dans la section "**Windows display language**", sélectionner "**English (United States)**".

Ensuite dans la section "**Preferred languages**", ajouter la lange "**English (United States)**". Déplacer la en première position de la liste.

? Unknown Attachment

Par ligne de commande

Après avoir ouvert un PowerShell, exécuter les commande suivante :

```
Install-Language -Language en-US
Set-WinUserLanguageList en-US -Force
```

Ensuite, il est nécessaire de **se déconnecter puis se reconnecter** au nouvel utilisateur afin de correctement appliquer le changement de langue.

Une fois fait, vous pouvez vous reconnecter à votre compte administrateur Windows et continuer la configuration.

Autorisations systèmes

Autorisation WinRM

Attribuer au nouvel utilisateur les droits d'accès aux ressources WinRM.

Dans une console PowerShell, exécuter la commande suivante :

```
winrm configSDDL default
```

Une nouvelle fenêtre s'ouvre. Dans celle-ci, ajouter le nouvel utilisateur et cliquer sur **Ajouter...** et attribuer les droits :

- Lecture(Get,Enumerate,Subscribe)
- Exécution(Invoke)

En cochant les cases correspondantes dans le tableau des droits situé en dessous de la liste des utilisateurs (*cliquer sur l'utilisateur au préalable*).

? Unknown Attachment

Autorisation aux objets CIM

La sonde va demander les informations systèmes via les objets CIM, il est nécessaire d'ajouter les droits à l'utilisateur.

> Cette section n'est pas nécessaire si vos machines supervisées sont configurées avec un Active Directory.

Il faut en premier temps lancer la fenêtre de contrôle WMI avec la commande :

```
wmimgmt.msc
```

Une fois lancé, clic droit sur **Contrôle WMI (local)** puis sélectionner **Propriétés**.

? Unknown Attachment

Accéder à la section Sécurité, puis dans l'arborescence ci-dessous, sélectionner **Root > CIMV2** puis cliquer sur le bouton **Sécurité** situé en bas à droite.

? Unknown Attachment

Enfin, ajouter l'utilisateur afin de lui appliquer de nouveaux droits, puis cocher **Activer le compte** et **Appel à distance autorisé**.

? Unknown Attachment

Autorisation de l'identification Basique

Par défaut, le service WinRM n'est pas configuré pour autoriser les connexions "*Basiques*", considérées comme non sécurisées.

> Nous ne recommandons pas l'utilisation de ce protocole, si un plus sécurisé est déjà disponible sur le système.

Configuration de WinRM pour accepter une connexion "Basique"

Dans une console Windows autre que PowerShell, exécuter les commandes suivantes pour :

- Activer l'authentification "*Basique*"

```
winrm set winrm/config/service/auth @{Basic="true"}
```

- Autoriser les connexions non chiffrées

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

L'authentification "*Basique"* est désormais configurée pour être utilisée par WinRM.