Base de métrologie (Graphite)

Sommaire

Contexte

Cette page a pour but de décrire la mise en place d'une configuration minimale nécessaire pour un Windows dans un domaine (*Active Directory*) supervisé par le pack **windows-by-WinRM__shinken.**

Configuration de WinRM pour domaine (Active Directory)

L'entièreté de la configuration de vos machines Windows se fera depuis une seule machine, votre contrôleur de domaine.

Autant que possible, la configuration sera définie avec des GPO (*Global Policy Object*) et sera déployée automatiquement à l'ensemble des machines voulu.

Les **GPOs** sont dès objets logiques où l'on attache des règles de configurations. Les **GPOs** sont appliqués à des serveurs ou utilisateurs. Ils ont l'avantage de se déployer facilement et d'être désactivable, contrairement aux scripts.

⚠ Toutes les étapes suivantes doivent être appliquées depuis votre **contrôleur de domaine**, avec un **compte Administrateur**.

Configuration depuis l'Active Directory

La première étape est d'organiser votre **Active Directory** avec des **UOs** (*Unité d'organisation*) pour shinken. Ces **UOs** vont regrouper les éléments de votre **Active Directory** (utilisateurs, serveurs et contrôleurs de domaine) afin d'appliquer les configuration de supervisions.

- Ouvrir "**Utilisateurs et ordinateurs Active directory**" (*dsa.msc*)

Organiser ses machines par UO

Organiser ses serveurs et postes de travail par UO

- Cliquer sur son domaine
- Repérer dans quels dossiers sont les ordinateurs à superviser.
- Si tous les serveurs sont dans le dossier "**Computers**", il est nécessaire de les déplacer dans un nouveau dossier **UO**. Le dossier "**Computers** ", présent par défaut, ne permet pas d'appliquer des **GPOs** ou de créer de sous-dossiers.

  ? Unknown Attachment

  - Clic-Droit sur le nom de domaine, Sélectionner "**Nouveau**" > "**Unité d'organisation**" et lui donner un nom tel que "**Serveurs**".
  - Se déplacer dans le dossier "**Computers**", sélectionner et déplacer les ordinateurs dans la nouvelle **UO** créée.
- Pour chacun des **UO** où sont vos **serveurs à superviser**, créer un **UO** et nommer le par exemple "**Shinken supervised server**".
- Déplacer les serveurs dans la nouvelle **UO**.
  - ? Unknown Attachment

Organiser ses contrôleurs de domaine par UO

Il est également possible de superviser ses contrôleurs de domaine. Pour cela, il faut tout comme les autres serveurs tout d'abord les ranger dans une UO.

- Dans le dossier "**Domain Controllers**", Clic-Droit, Sélectionner "Nouveau" > "Unité d'organisation" et nommer le par exemple "**Shinken supervised server**".
- Déplacer les contrôleurs de domaine dans la nouvelle **UO**.
  - ? Unknown Attachment

Créer ses utilisateurs de supervision Shinken

Créer une UO pour les utilisateurs

- Cliquer sur son domaine
- Repérer dans quels dossiers sont les utilisateurs.
- Si tous les utilisateurs sont dans le dossier "**Users**", il est nécessaire de créer un nouveau dossier **UO**. Le dossier "**Users**", présent par défaut, ne permet pas d'appliquer des **GPOs** ou de créer de sous-dossiers.
    - Clic-Droit sur le nom de domaine, Sélectionner "Nouveau" > "Unité d'organisation" et lui donner un nom tel que "**Utilisateurs**".
    - ? Unknown Attachment
- Dans cette **UO** où sont tous les utilisateurs, créer un **UO** où seront les utilisateurs et groupes de supervision shinken, nommer là par exemple "**Shinken supervision users**".
    - ? Unknown Attachment

Créer un ou plusieurs utilisateurs de supervision

- Dans la nouvelle **UO** pour utilisateurs shinken de supervision, Clic-Droit, Sélectionner "**Nouveau**" > "**Utilisateur**"
- Remplir :
    - "Nom complet"
    - "Nom d'ouverture de session de l'utilisateur"
    - ? Unknown Attachment
- Sur la page suivante :
    - Remplir le mot de passe
    - Décocher "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session"
    - Cocher "L'utilisateur ne peut pas changer de mot de passe"
    - ? Unknown Attachment
- Finaliser ensuite la création de l'utilisateur.

OPTIONNELLEMENT, vous pouvez créer plusieurs utilisateurs de supervision en répétant l'étape précedente, et restreindre aux serveurs seléctionnés chaque utilisateur.

- Clic-Droit sur un utilisateur de supervision shinken puis cliquer sur "**Propriétés**"
- Dans l'onglet "**Compte**", cliquer sur "**Se connecter à...**"
- Une nouvelle fenêtre s'ouvre, Cliquer sur "**Les ordinateurs suivants**" et remplir la liste d'ordinateurs auquel l'utilisateur a le droit de se connecter (*parmi ceux qui seront configurés pour WinRM, dans les UOs précédentes*).
    - ? Unknown Attachment

Créer un groupe de supervision

Dans la nouvelle **UO** pour utilisateurs shinken de supervision, Clic-Droit, Sélectionner "**Nouveau**" > "**Groupe**"

- Remplir le "**Nom de groupe**", avec par exemple "**GRP_SHINKEN**".
- Garder la propriété "**Globale**" cochée.
    - Elle permet de définir la visibilité du nouveau groupe au sein d'un ou plusieurs domaines.
    - "**Domaine locale**" limite l'utilisation du groupe au domaine actuel.
    - "**Globale**" limite l'utilisation du groupe au domaine actuel, et aux autres domaines s'ils sont approuvés.
    - "**Universelle**" autorise l'utilisation du groupe dans tous les domaines de la forêt.
- Garder la propriété "**Sécurité**" cochée.
    - ? Unknown Attachment
- Ensuite, pour chaque utilisateur de supervision crée, Clic-Droit puis "**Ajouter à un groupe**"
- Remplir le nom du groupe de supervision (*GRP_SHINKEN*)
- Cliquer sur "Vérifier les noms" puis valider.

- Unknown Attachment

Configurer des permissions pour le contrôleur de domaine

La configuration du groupe pour le contrôleur de domaine se fait dans le même outil : "**Utilisateurs et ordinateurs Active Directory**" :

- Dans l'arborescence de votre domaine, sélectionner "**Builtin**"
- Clic-Droit sur le groupe "**Utilisateur de gestion à distance**", puis "**Propriétés**".
- Dans l'onglet "**Membres**", Cliquer sur "**Ajouter...**"
- Remplir le nom du groupe de supervision shinken (*GRP_SHINKEN*) et valider.
- Répéter l'opération pour le groupe "**Utilisateur de l'Analyseur de performance**".
- Unknown Attachment

En anglais, les groupes se nomment :

- `Remote Management Users`
- `Performance Monitor Users`

Configuration par GPO

La seconde étape est de créer une GPO (*Global Policy Object*), l'appliquer aux serveurs windows à superviser puis la configuer.

- Ouvrir "**Gestion de stratégie de groupe**" (*gpmc.msc*)

Créer une GPO

- Dans l'arborescence, Clic-Gauche sur votre "**Forêt: DOMAINE**" > "**Domaines**" > "**DOMAINE**" > "**Objets de stratégie de groupe**"
- Unknown Attachment
- Clic-Droit sur "**Objets de stratégie de groupe**" > "**Nouveau**" puis nommer la nouvelle **GPO** avec, par exemple, "**Shinken - windows-by-WinRM**"
- Une fois crée, Cliquer-Glisser votre **GPO** dans les **UOs** de vos serveurs à superviser précédemment créés.
  - La liste des liaisons s'affiche à droite de la fenêtre lorsque la **GPO** est sélectionnée.
  - Unknown Attachment

Configuration de la GPO

Une fois créé et lié aux Windows à superviser, il faut configurer la **GPO**. C'est-à-dire lui accrocher des règles qui modifieront la configuration des ordinateurs liés

- Clic-Droit sur la nouvelle **GPO**, puis "Modifier"
- Les règles à appliquer se trouvent dans cette arborescente de configuration.

Configuration de WSM

Activer la gestion à distance WSM (*WS-Management*) est essentiel pour la connexion à distance et la collecte d'information pour **WinRM**.

- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Paramètres de sécurité**" > "**Services système**" > "**Gestion à distance Windows (Gestion WSM)**"
- Unknown Attachment
- Double-Clic, Une nouvelle fenêtre s'ouvre.
  - Cocher "**Définir ce paramètre de stratégie**"
  - Cocher "**Automatique**"

- Unknown Attachment

Configuration de WinRM

Dans cette section, il faudra activer le démarrage automatique de **WinRM** et configurer le mode d'authentification.

- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Modèle d'administration : définition de stratégies**" > "**Composants Windows**" > "**Gestion à distance Windows (WinRM)**" > "**Service WinRM**"
  - Unknown Attachment
- Double-Clic sur "**Autoriser la gestion de serveurs à distance via WinRM**", une nouvelle fenêtre s'ouvre
  - Cocher "Activer"
  - Remplir la zone "**Filtre IPv4**" avec : *****
  - Remplir la zone "**Filtre IPv6**" avec : *****

    Attention il est impératif de remplir ces zones de "**Filtres IP**". Sans cela le **service WinRM** n'écoutera sur AUCUNE interface réseau et ne **RÉPONDERA PAS**.

    Une fois votre configuration terminée et la sonde fonctionnelle, vous pourrez changer ce masque réseau afin de limiter l'accès à WinRM selon l'IP.

    - Unknown Attachment

Configurer l'authentification NTLM

L'authentification **NTLM** est conseillé. Si vous utilisez l'authentification **Basic**, passez à l'étape suivante.

- Double-Clic sur "**Ne pas autoriser l'authentification par négociation**", une nouvelle fenêtre s'ouvre.
- Cocher "**Désactivé**", puis valider.
  - Unknown Attachment

- Double-Clic sur "**Autoriser le trafic non chiffré**", une nouvelle fenêtre s'ouvre.
- Cocher "**Désactivé**", puis valider.
  - Unknown Attachment

Résumé de la configuration NTLM:

- Unknown Attachment

Configurer l'authentification Basic

Si vous utilisez l'authentification **NTLM**, assurez-vous d'avoir fait l'étape précédente, puis continuez.

- Double-Clic sur "**Autoriser l'authentification de base**", une nouvelle fenêtre s'ouvre.
- Cocher "**Désactivé**", puis valider.

- Unknown Attachment

- Double-Clic sur "**Autoriser le trafic non chiffré**", une nouvelle fenêtre s'ouvre.
- Cocher "**Activé**", puis valider.
- Unknown Attachment

Résumé de la configuration Basic :

Unknown Attachment

Configuration des groupes locaux

Afin de compléter la configuration d'accès à distance, et l'accès aux ressources (notamment necessaire pour le check **Uptime by WinRM**), il est nécessaire de configurer la GPO pour qu'elle ajoute le groupe de supervision aux groupes locaux suivants, présent sur chaques machines :

- **Utilisateurs de gestion à distance**
- **Utilisateurs de l'Analyseur de performances**

Pour cela :

- Dans l'arborescence : "**Configuration ordinateur**" > "**Préférences**" > "**Paramètres du Panneau de configuration**" > "**Utilisateurs et groupes locaux**"
- Clic-Droit, "**Nouveau**" > "**Groupe local**". Une nouvelle fenêtre s'ouvre.
- Unknown Attachment

  - Sélectionner "Mettre à jour"
  - Cliquer dans la zone "Nom du groupe", et sélectionner "**Utilisateurs de l'Analyser de performance (intégré)**" dans la liste.
  - Unknown Attachment

    Unknown Attachment

    Attention, il faut sélectionner, le groupe depuis la liste. Remplir le nom du groupe à la main ne fonctionnera pas.

  - Cliquer sur "**Ajouter**", puis dans la nouvelle fenêtre la case "**...**" après la zone "**Nom**"
  - Remplir le nom du groupe de supervision puis valider.
    - Unknown Attachment
  - Répéter l'opération pour le groupe "**Utilisateurs de gestion à distance"**

    Attention le groupe "**Utilisateurs de gestion à distance**" ne se trouve pas dans la liste "Intégré", il faudra taper le nom à la main sans faute.

    - Unknown Attachment

Configuration du Pare-Feu

Dans cette section, il faudra ajouter au Pare-Feu une règle pour autoriser le trafic **WinRM**.

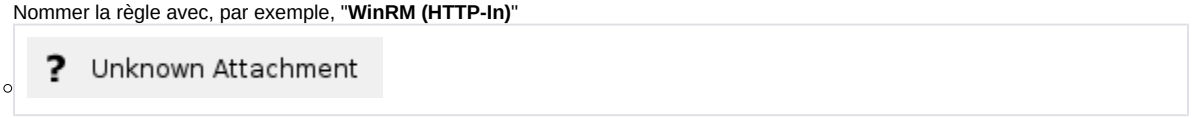
- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Paramètres de sécurité**" > "**Pare-feu Windows Defender avec fonctions avancées de sécurité**" > "**Règles de trafic entrant**"
- Clic-Droit, "Nouvelle Règle", une nouvelle fenêtre s'ouvre
  - 

    - Cocher "**Port**"
      - 

    - Sur la page suivante :
    - Cocher "**TCP**"
    - Cocher "**Ports locaux spécifiques**", et remplissez "**5985**"
      - 

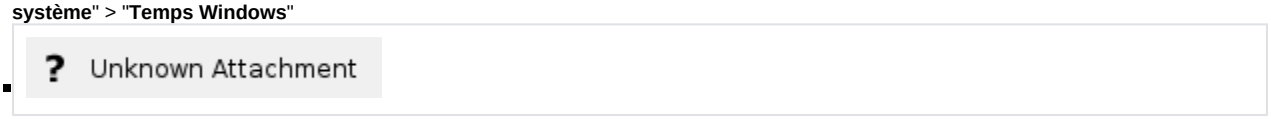
    - Sur la page suivante :
    - Cocher "**Autoriser la connexion**"
      - 

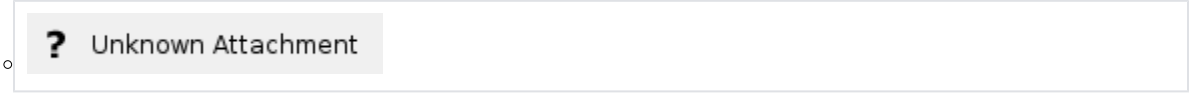
    - Sur la page suivante :
    - Sélectionner les types d'interfaces réseau à exposer.
      - 

    - Sur la page suivante :
    - Nommer la règle avec, par exemple, "**WinRM (HTTP-In)**"
      - 

Configuration de Windows Time (OPTIONNEL)

Nécessaire au fonctionnement du check "**Ntp Sync by WinRM**", si le temps de votre machine est géré par Windows Time (*W32Time*), il est nécessaire de donner les permissions suivantes :

- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Paramètres de sécurité**" > "**Services système**" > "**Temps Windows**"
  - 

- Double-Clic, Une nouvelle fenêtre s'ouvre.
  - Cocher "**Définir ce paramètre de stratégie**"
  - Cocher "**Automatique**"
    - 

- Cliquer ensuite sur "**Modifier la sécurité...**", une nouvelle fenêtre s'ouvre.
  - Cliquer sur ajouter
  - Remplir le nom du groupe de supervision shinken (*GRP_SHINKEN*)
  - Vérifier le nom et confirmer
    - 

- Une fois le groupe ajouté, le sélectionner :
  - Cocher "**Autoriser**" / "**Lecture**"
  - Décocher "**Autoriser**" / "**Démarrage, arrêt et pause**"

- ? Unknown Attachment

Configuration par Script et GPO

La dernière étape de la configuration est d'accrocher deux scripts à une nouvelle **GPO** qui va déployer ces scripts et les exécuter aux prochains démarrages de vos machines.

Ces deux scripts vont configurer les permissions **WinRM** et l'accès aux objets **WMI / CIM** essentiel à la supervision de vos serveurs Windows.

- Ouvrir "**Gestion de stratégie de groupe**" (*gpmc.msc*)

Créer une GPO

- Dans l'arborescence, Clic-Gauche sur votre "**Forêt: DOMAINE**" > "**Domaines**" > "**DOMAINE**" > "**Objets de stratégie de groupe**"
- Clic-Droit sur "**Objets de stratégie de groupe**" > "**Nouveau**" puis nommer la nouvelle **GPO** avec, par exemple, "**Shinken - windows-by-WinRM Permissions Script**"
- Une fois crée, Cliquer-Glisser votre **GPO** dans les **UOs** de vos serveurs à superviser précédemment créés, aux mêmes endroits où est lié la précédente **GPO**.
  - La liste des liaisons s'affiche à droite de la fenêtre lorsque la **GPO** est sélectionnée.
  - ? Unknown Attachment

Configuration de la GPO

Une fois créé et lié aux Windows à superviser, il faut configurer la **GPO**.

- Clic-Droit sur la nouvelle **GPO**, puis "Modifier"
- Les règles à appliquer se trouvent dans cette arborescente de configuration.

Téléchargement des scripts

Tout d'abord, **télécharger les scripts** ci-dessous sur votre **contrôleur de domaine**.

Ces scripts se retrouvent aussi dans le dossier "**supervised-host**" du pack livré.

Permissions WinRM	Autorisation aux objets WMI/CIM
Télécharger le script ICI AddSecurityPrincipalonDefaultWinRMSDDL.ps1	**Télécharger le script ICI** Set-WMINameSpaceSecurity.ps1

Accrocher les scripts

- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Scripts (démarrage/arrêt)**"
- Double-Clic sur "Démarrage", une nouvelle fenêtre s'ouvre
- ? Unknown Attachment
- Dans la nouvelle fenêtre, aller dans l'onglet "**Scripts PowerShell**"
- Clic sur "**Afficher les fichiers...**".
  - ? Unknown Attachment
  - Une nouvelle fenêtre s'ouvre. Dans ce dossier (*... > Machine > Scripts > Startup*), déposer les scripts téléchargés précédemment.
  - ? Unknown Attachment
  - Fermer le dossier.
- Toujours dans l'onglet "**Scripts PowerShell**", cliquer sur "Ajouter"
  - Une nouvelle fenêtre s'ouvre pour ajouter un script.

- Cliquer sur parcourir et ajouter le 1er script : "AddSecurityPrincipalonDefaultWinRMSDDL.ps1", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
- Dans la zone "Paramètre de scripts", remplissez :
  - `-user "MON_DOMAINE\GRP_SHINKEN"`

> Ici, remplacez "MON_DOMAINE" par le nom de votre domaine.

- Répéter l'opération avec le 2 script : "Set-WMINameSpaceSecurity.ps1", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
- Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :
  - `-user "MON_DOMAINE\GRP_SHINKEN"`

> Ici, remplacez "MON_DOMAINE" par le nom de votre domaine.

Appliquer la configuration

Une fois toutes les étapes précédentes effectuées, il faut appliquer la configuration.

La configuration par **GPO** va se déclencher sur tous les serveurs configurés

- Après un redémarrage de la machine.
- Après 1H à 1H30 d'attente (*Application automatique des GPO*).
- Après avoir exécuté sur une machine la commande :

```
gpupdate.exe /Force
```

> Attention, au moins un redémarrage de chaque machine à superviser est nécessaire afin que les scripts de démarrage se lancent.
>
> Pour les machines qui ne peuvent pas être mise hors service un instant, il est possible de EXECUTER A LA MAIN ou CONFIG ADMIN.