

# Synchronizer - Les logs d'authentification

## 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 déployé automatiquement à l'ensemble des machines voulus.



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

## Étapes préliminaires

La première étape est d'organiser votre **Active Directory** avec des **UO** ( Unité d'organisation ) pour shinken. Ces **UO** vont regrouper de nouveaux groupes, utilisateurs de supervisions, serveurs et contrôleurs de domaine.

- 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**".



- 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**".



### 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"



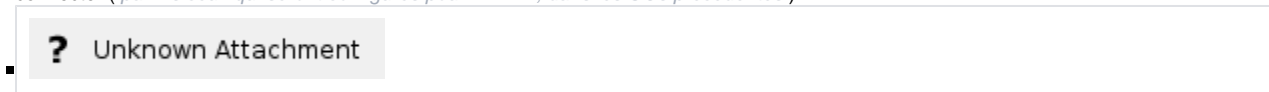
- Sur la page suivante :
  - Remplir le mot de passe
  - Décocher "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session"
  - Cocher "L'utilisateur ne peut pas changer de mot de passe"



- Finaliser ensuite la création de l'utilisateur.

**Optionnellement**, vous pouvez créer plusieurs utilisateurs de supervision en répétant l'étape précédente, et restreindre aux serveurs sélectionnés 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 ( *parmis ceux qui seront configurés pour WinRM, dans les UOs précédentes* ).



### Créer un groupe de supervision



Cette page est en cours de construction et sera disponible prochainement.  
En attendant, voici quelques conseils afin de faire votre propre configuration WinRM.

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

Autant que possible, la configuration devra être déployée par GPO ( *Global Policy Object* ), sinon par script à usage unique.

Voici les étapes auxquelles un déploiement par GPO est possible :

- Activer le démarrage de WinRM.
- **Installer la langue Anglaise** ( Etats-Unis ).
- **Créer un utilisateur de domaine**, et l'ajouter dans des groupes locaux nécessaires.
- **Configurer la langue** du nouvel utilisateur de supervision.
- Configurer WinRM pour l'**authentification Basic ou Negotiate**, puis HTTP.
- Configurer l'utilisateur de supervision pour récupérer **les informations de W32Time, le service NTP de Windows**.

Ensuite, il sera nécessaire d'appliquer les configurations suivantes avec un script à utilisation unique.

- Configurer l'utilisateur de supervision pour exécuter des **commandes WinRM**.
- Configurer l'utilisateur de supervision pour récupérer **les informations WMI/CIM root\cimv2**.
- Configurer l'utilisateur de supervision pour récupérer **les informations WMI/CIM root\standardcimv2**.

## Configuration des permissions

Permissions WinRM

**Télécharger le script ICI**

[AddSecurityPrincipalonDefaultWinRMSDDL.ps1](#)

Autorisation aux objets WMI/CIM

**Télécharger le script ICI**

[Set-WMINameSpaceSecurity.ps1](#)