Modèles d'hôtes du pack windows-by-WinRM__shinken

Sommaire

Contexte

Afin de superviser une machine Windows, le pack windows-by-WinRM__shinken propose les modèles d'hôte suivants :

- **windows-by-WinRM** permet la supervision d'un hôte Windows pour une vérification des fonctions principales (*CPU, disques, RAM, interfaces réseau ...*).
- **windows-by-WinRM__advanced** qui permet une supervision plus avancée de l'hôte (*Statistiques d'utilisation…*).
- **windows-by-WinRM__extra** permet une supervision plus personnalisée de l'hôte (*Surveillance de processus, surveillance de fichiers*).

Afin de s'adapter aux besoins précis, il est possible de **directement modifier les modèles suivants** :

- **windows-by-WinRM**
- **windows-by-WinRM__advanced**
- **windows-by-WinRM__extra**

Ceux-ci héritent des modèles suivants :

- **windows-by-WinRM__shinken**
- **windows-by-WinRM__advanced__shinken**
- **windows-by-WinRM__extra__shinken**

Ils contiennent toute la logique du pack.

- Ces modèles internes (*finissant par la particule « __**shinken**__ »*) **ne doivent pas être modifiés**.
  - Les modifications risquent d'être écrasées lors de prochaines mises à jour du pack.

Liste des modèles d'hôte

Nom	Lien
`windows-by-WinRM`	Modèle windows-by-WinRM
`windows-by-WinRM__advanced`	Modèle windows-by-WinRM__advanced
`windows-by-WinRM__extra`	Modèle windows-by-WinRM__extra

Modes d'authentification

Le pack **windows-by-WinRM__shinken** offre les modes d'authentifications suivants :

- **ntlm**
- **basic**

Le mode d'authentification peut être changé en modifiant la donnée "**WINDOWS_BY_WINRM__AUTHMETHOD**", accroché sur les modèles d'hôtes.

NTLM

NTLM est le mode d'authentification de Windows par défaut pour les ordinateurs configurés en Groupe de Travail (lorsqu'ils ne sont pas configurés en domaine).

NTLM nécessite un **nom d'utilisateur** et un **mot de passe**. Il est activé par défaut sur les serveurs Windows.

Deux versions de NTLM existent :

- NTLMv1 : déprécié par Microsoft depuis 2010.
- NTLMv2 : Installé et configuré par défaut sur Windows, il est largement utilisé. Déprécié depuis 2024.

Toutes les versions de NTLM sont désormais dépréciés depuis juin 2024 : https://learn.microsoft.com/en-us/windows/whats-new/deprecated-features.

Le protocole NTLM utilisé chiffre ses échanges.

Les principales fragilités de NTLM sont :

- Pas d'authentification mutuelle. Les "attaques par relais" "Man-in-the-Middle" sont possibles.
- Les **hashs** échangés utilisés comme moyen d'authentification sont fragiles.

Ces problèmes sont réglés par l'utilisation de HTTPS, et d'une vérification stricte des certificats.

Basic

L'authentification **basic** utilise un nom d'utilisateur et un mot de passe. Ces derniers sont envoyés en clair sur le réseau, l'ensemble des échanges ne sont pas chiffrés.

Ce protocole n'offre pas de réelle sécurité sans être couplé à **HTTPS**.

Kerberos (*non disponible*)

Kerberos est le mode d'authentification de Windows par défaut pour les ordinateurs configurés en domaine ou Active Directory (lorsqu'ils ne sont pas configurés en groupe de travail).

L'authentification **Kerberos** nécessite une connexion à l'hôte supervisé en utilisant :

- un **nom DNS**,
- un **domaine Active Directory** (Windows),
- un **nom d'utilisateur**,
- et un **mot de passe**.

Ce protocole est recommandé et utilisé par défaut sur Windows depuis W*indows 2000* sur les postes au sein d'un **domaine Active Directory**.

Kerberos offre une **communication chiffrée** basée sur des **tickets d'authentification temporaires** émis par le **contrôleur de domaine**.

C'est la méthode d'authentification recommandée, car la plus sécurisée.

> Kerberos n'est pas implémenté dans la sonde pour le moment.

Résumé

Méthode	Authentification Mutuelle	Confidentialité	Intégrité	Implémenté dans la sonde
Basic				
NTLM				
Kerberos				

Sécurité supplémentaire

HTTPS (*non disponible*)

Le protocole HTTPS peut être utilisé via WinRM. Il permet de rajouter la sécurité nécessaire à l'authentification **basic** et **NTLM**.

> Le protocole HTTPS n'est, pour le moment, pas implémenté dans la sonde.
>
> En attendant, il est recommandé d'utiliser **ntlm**.