shinken-protected-fields-keyfile-export

Sommaire

Description
Options

Contexte

Afin de superviser une machine Windows, le pack windows-by-WinRM 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__extra** qui permet une supervision plus personnalisée de l'hôte (*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__extra**

Ceux-ci héritent des modèles suivants :

- **windows-by-WinRM__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 pour windows-by-WinRM__shinken

Nom	Lien
`windows-by-WinRM`	NEW-PAGE - SPAC-27 - Modèle windows-by-WinRM
`windows-by-WinRM__extra`	NEW-PAGE - SPAC-27 - Modèle windows-by-WinRM__extra

Modes d'authentification

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

- **negotiate**

- **basic**
- **ntlm-over-ip**

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

negotiate

negotiate est un protocole de négociation d'authentification. Il va permettre au poller et à la machine supervisée de choisir le mode d'authentification le plus sécurisé disponible.
En premier lieu **Kerberos** va être priorisé, car il est plus sécurisé, puis si cela échoue, **NTLM** sera utilisé.

NTLM

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-feature

NTLM repose sur un **échange d'authentification chiffré.** Le reste des données échangés ne sont pas chiffrés.

NTLM n'offre pas d'authentification mutuelle afin d'éviter les attaques "Man-in-the-Middle"

> L'utilisation de NTLM nécessite le paquet gssntlmssp sur le Poller.
>
> La connexion NTLM **échoue sous CentOs 7**.

Kerberos

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*.

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.

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.

Afin de protéger ces échanges en clair sur le réseau, il est possible d'utiliser *HTTPS* pour chiffrer la communication.

ntlm-over-ip

Cette méthode d'authentification le mode "**negotiate**", mais force l'utilisation de l'authentification par **NTLM**.

Pour forcer le protocole **NTLM**, la sonde va résoudre le nom de l'hôte en adresse IP, puis essayer de s'authentifier. Comme **Kerberos** ne peut pas être choisi comme méthode d'authentification lorsque la communication se passe par ip, alors **NTLM** est forcé.

Ce mode n'est pas conseillé en production, mais peut être utile pour déboguer l'authentification

Résumé

Méthode	Authentification Mutuelle	Confidentialité	Intégrité	Implémenté dans la sonde
Basic				
NTLM (via negotiate)		(Uniquement l'authentification est chiffrée. Les données échangées par les sondes sont envoyées en clair sur le réseau)	Optionelle	
ntlm-over-ip		(Uniquement l'authentification est chiffrée. Les données échangées par les sondes sont envoyées en clair sur le réseau)	Optionelle	
Kerberos (via negotiate)				
Basic + HTTPS				
NTLM (negotiate) + HTTPS				
Kerberos + HTTPS				

Sécurité supplémentaire

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

Le protocole HTTPS n'est pas implémenté dans la sonde. Il le sera prochainement.

En attendant, il est recommandé d'utiliser **negotiate**.