

Mise en place du Pack iis

Sommaire

[Procédure de mise en place du pack](#)
Installation des sondes du pack

[Import des modifications suite à une mise à jour de Shinken](#)

[Fonctionnement WMI sur poste client ou serveur Windows](#)
Windows Management Instrumentation (infrastructure de gestion Windows)
WMI Avancé - gestion de la sécurité
Déléguer des droits d'accès minimum à un utilisateur ou un groupe sur les services Windows

Étape 1 : Trouver le SID de l'utilisateur
Étape 2 : Accorder à votre utilisateur les droits d'interroger le service 'Scmanager'
Étape 3 : Déterminer les services non superviser
Étape 4 : Accorder à votre utilisateur les droits d'interroger le statut d'un service
Interpreter le Security Descriptor Language (SDDL)

[Résolutions des problèmes](#)
Les checks n'arrivent pas à récupérer les informations alors que l'utilisateur utilisé est Administrateur
Erreur : "Error: Can't locate perl58.dll"
Erreur : "ERROR: Login to remote object."

Contexte



Remarque

⚠ Attention, les modèles d'hôtes se différencient juste par les paramètres utiles a la connexion en SNMP que vous pouvez lui mettre, pour ce qui s'agit des checks qui leurs sont accrochés, ils sont strictement identiques

Les checks suivants sont rattachés au 3 modèles d'hôtes Modèles "**switch-SNMPv3-authPriv**", "**switch-SNMPv3-authNoPriv**" et "**switch-SNMPv3-noAuthNoPriv**" :

Le but de ces 3 modèles sont de donner une vue globale sur l'état du switch ainsi que les interfaces et leurs utilisations.

Comment appliquer les modèles à un hôte

En utilisant l'interface de Configuration

Dans l'interface de Configuration,

SCREEN

- créez ou [éditez un Hôte](#),
- et ajoutez le modèle "**switch-SNMPv3-authPriv**", "**switch-SNMPv3-authNoPriv**" ou "**switch-SNMPv3-noAuthNoPriv**" dans la propriété "**Modèles d'hôte hérités**" à l'aide du menu déroulant.

En éditant les fichiers de définition des éléments d'un collecteur d'import (cfg)

Dans un fichier de configuration,

- créez ou éditez votre définition d'hôte
- en ajoutant, dans la propriété "**use**", la valeur "**switch-SNMPv3-authPriv**", "**switch-SNMPv3-authNoPriv**" ou "**switch-SNMPv3-noAuthNoPriv**" selon les besoins.

Puis, le contenu du fichier devra alors être importé avec une source d'import de fichier de configuration (*plus d'information sur cette page: Collecteur de type (cfg-file-import) - Import depuis des fichiers au format .cfg*).

```
define host {
    host_name    Switch
    use switch-SNMPv3-
authPriv
        use switch-SNMPv3-
authNoPriv
        use switch-SNMPv3-
noAuthNoPriv
}
```

Les donnée des modèles

Configuration de la connexion sur un hôte

Parmi les 6 modèles d'hôtes disponibles, vous retrouverez dans le nom de chacun de ces modèles, un des 3 noms suivants : **noAuthNoPriv**, **autNoPr** **iv** ou **authPriv**.

Ceci correspond au mode d'authentification que vous allez choisir pour la connexion SNMPv3

noAuthNoPriv

Ce mode d'authentification revient au mode que l'on retrouve dans la version 1 et 2 de SNMP.

Les modèles d'hôtes qui utilisent cette authentification sont : **switch-SNMPv3-noAuthNoPriv** et **switch-SNMPv3-noAuthNoPriv-detailed**

Les champs à remplir sont donc les suivants :

	Description	Valeur par défaut	Unités
SWITCH_LOGIN	Login SNMP v3 <ul style="list-style-type: none">EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login/mot de passe	shinken	--
SWITCH_TIMEOUT	Cette variable permet au check de s'arrêter après un certain temps si une tâche ne s'est pas terminée. Cela permet d'éviter que le programme ne s'exécute indéfiniment et de prévenir des problèmes de performances. Le temps est en secondes.	60	secondes

Vue depuis l'interface de configuration:

? Unknown Attachment

authNoPriv

Ce mode d'authentification est le mode intermédiaire au niveau de l'authentification. Il utilise :

- un login,
- un mot de passe
- et un protocole d'authentification. => PASSPHRASE?

Les modèles d'hôtes qui utilisent cette authentification sont :

- switch-SNMPv3-authNoPriv**
- et **switch-SNMPv3-authNoPriv-detailed**

Les champs à remplir sont donc les suivants :

	Description	Valeur par défaut	Unités
SWITCH_LOGIN	Login SNMP v3 <ul style="list-style-type: none">EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login/mot de passe	shinken	--
SWITCH_TIMEOUT	Cette variable permet au check de s'arrêter après un certain temps si une tâche ne s'est pas terminée. Cela permet d'éviter que le programme ne s'exécute indéfiniment et de prévenir des problèmes de performances. Le temps est en secondes.	60	secondes
SWITCH_PROTOCOL_AUTH	Protocol d'authentification SNMPv3 <ul style="list-style-type: none">Ce protocole n'est pas obligatoire mais conseillé pour une meilleur sécurisation de la connexion.Deux protocoles sont possibles (MD5 ou SHA)	sha	--
SWITCH_PASSPHRASE_AUTH	Mot de passe d'authentification SNMPv3 <ul style="list-style-type: none">Le mot de passe garantit l'intégrité des données et permet d'authentifier l'origine des données	shinkenpassword	--

Vue depuis l'interface de configuration :

? Unknown Attachment

authPriv

Ce mode d'authentification est le mode le plus complet de la connexion SNMPv3. Il utilise :

- un login,
- un mot de passe **chiffré**
- et **XXXX**.

Les modèles d'hôtes qui utilisent cette authentification sont :

- **switch-SNMPv3-authPriv**
- et **switch-SNMPv3-authPriv-detailed**

Les champs à remplir sont donc les suivants :

	Description	Valeur par défaut	Unités
SWITCH_LOGIN	Login SNMP v3 <ul style="list-style-type: none"> • EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login/mot de passe 	shinken	--
SWITCH_TIME OUT	Cette variable permet au check de s'arrêter après un certain temps si une tâche ne s'est pas terminée. Cela permet d'éviter que le programme ne s'exécute indéfiniment et de prévenir des problèmes de performances. Le temps est en secondes.	60	secondes
SWITCH_PROTOCOL_AUTH	Protocol d'authentification SNMPv3 <ul style="list-style-type: none"> • Ce protocole n'est pas obligatoire mais conseillé pour une meilleur sécurisation de la connexion. • Deux protocoles sont possibles (MD5 ou SHA) 	sha	--
SWITCH_PASSWORD	Mot de passe d'authentification SNMPv3 <ul style="list-style-type: none"> • Le mot de passe garantit l'intégrité des données et permet d'authentifier l'origine des données 	shinkenpassword	--
SWITCH_PROTOCOL_PRIV	Protocol de confidentialité SNMP v3 <ul style="list-style-type: none"> • Ce protocole n'est pas non plus obligatoire, mais tout comme le protocole d'authentification, il permet une sécurité supplémentaire pour la communication via SNMP • Deux protocoles sont possibles (AES ou DES) 	aes	
SWITCH_PASSWORD_PRIV	Mot de passe de confidentialité SNMP v3 <ul style="list-style-type: none"> • Le mot de passe de confidentialité assure le chiffrement et le déchiffrement des données. 	shinkenpasswordkey	--

Vue depuis l'interface de configuration :

? Unknown Attachment