

Pack cisco-WIFI-by-SNMP__shinken - V01.00.00



Note : Si vous êtes intéressé par ce pack, veuillez nous [contacter](#) pour son téléchargement. Nous vous accompagnerons lors de l'installation de ce pack sur votre plateforme.

Sommaire

[Contexte](#)
[Comment utiliser son pack ?](#)
 [Mise en place](#)
 [Utilisation](#)
 [Choisir les modèles d'hôtes](#)
 [Liste des modèles à utiliser dans le pack](#)
[Personnaliser son pack](#)
[Version des scripts livrés](#)

Contexte

Le pack **cisco-WIFI-by-SNMP__shinken** permet de superviser les contrôleurs Cisco WLAN ainsi que les points d'accès qui leur sont rattachés. Les vérifications sont effectuées grâce au protocole SNMP, via des appels actifs exécutés depuis les pollers de Shinken.

- Le pack vous permet de vérifier :
 - l'utilisation (*Cpu*, *Memory*) des ressources du contrôleur.
 - l'état matériel du contrôleur (*Hardware Health*).
 - l'état d'un point d'accès (*Access Point Status*).
 - les informations de clients connectés pour un point d'accès donné (*Client Connected*).
- Les commandes de vérifications exécutées depuis les serveurs Shinken utilisent une sonde **PYTHON** présente dans le répertoire des sondes Shinken `/var/lib/shinken-user/libexec/shinken-additional-packs/cisco-WIFI-by-SNMP__shinken/` (ou `$GLOBAL_cisco-WIFI-by-SNMP_SHINKEN_PLUGINS`) depuis l'interface de configuration), après la mise en place du pack.

Le pack se compose de deux grandes familles de modèles d'hôtes :

- Les modèles "AP", pour superviser un point d'accès Cisco à travers son contrôleur :
 - cisco-WIFI-by-SNMPv1v2__Access-Point** qui permet d'obtenir l'état du point d'accès et les informations de clients connectés en SNMP v1 ou v2.
 - cisco-WIFI-by-SNMPv3__Access-Point__**(`noAuthNoPriv` / `authNoPriv` / `authPriv`) qui permet d'obtenir l'état du point d'accès et les informations de clients connectés en SNMP v3.
- Les modèles "Controller", pour superviser le contrôleur Cisco WLAN :
 - cisco-WIFI-by-SNMPv1v2__Controller** qui permet la supervision des ressources et de l'état matériel du contrôleur en SNMP v1 ou v2 (*Cpu*, *Memory*, *Hardware Health*).
 - cisco-WIFI-by-SNMPv3__Controller__**(`noAuthNoPriv` / `authNoPriv` / `authPriv`) qui permet la supervision des ressources et de l'état matériel du contrôleur en SNMP v3 (*Cpu*, *Memory*, *Hardware Health*).

Ce pack est importé et mis à jour par la source " **shinken-additional-packs-import** ".

Voici un aperçu du contenu du pack :

Pack cisco-WIFI-by-SNMP__shinken

V01.00.00

Modèles d'hôtes

cisco-WIFI-by-SNMPv1v2__Controller

cisco-WIFI-by-SNMPv1v2__Access-Point

cisco-WIFI-by-SNMPv3__Controller__noAuthNoPriv

cisco-WIFI-by-SNMPv3__Access-Point__noAuthNoPriv

cisco-WIFI-by-SNMPv3__Controller__authNoPriv

cisco-WIFI-by-SNMPv3__Access-Point__authNoPriv

cisco-WIFI-by-SNMPv3__Controller__authPriv

cisco-WIFI-by-SNMPv3__Access-Point__authPriv

Checks appliqués aux modèles d'hôtes

Cpu by SNMPv1v2

Hardware Health by SNMPv1v2

Memory by SNMPv1v2

Access Point Status by SNMPv1v2

Connected Clients by SNMPv1v2

Cpu by SNMPv3

Hardware Health by SNMPv3

Memory by SNMPv3

Access Point Status by SNMPv3

Connected Clients by SNMPv3

Cpu by SNMPv3

Hardware Health by SNMPv3

Memory by SNMPv3

Access Point Status by SNMPv3

Connected Clients by SNMPv3

Cpu by SNMPv3

Hardware Health by SNMPv3

Memory by SNMPv3

Access Point Status by SNMPv3

Connected Clients by SNMPv3

Comment utiliser son pack ?

Mise en place

Pour utiliser les packs externes Shinken, il faut commencer par les installer sur son infrastructure Shinken. Cette action permet :

- D'installer sur les serveurs les sondes ([le code informatique](#)) nécessaires aux vérifications.
- De faire apparaître sur l'interface de configuration les nouveaux modèles.
- De préparer l'équipement à superviser ([contrôleur Cisco WLAN et points d'accès associés](#)) pour accepter les requêtes de supervision.

Une page dédiée explique comment mettre en place le pack cisco-WIFI-by-SNMP ([Page Mise en place du Pack cisco-WIFI-by-SNMP__shinken](#)).

Utilisation

Choisir les modèles d'hôtes

Une fois le pack installé, il suffit d'appliquer les modèles nouvellement importés sur les hôtes à superviser :

- En utilisant l'interface de configuration : Créez ou éditez un Hôte, et ajoutez un des modèles ; "**cisco-WIFI-by-SNMPv3__Controller__authPriv**" par exemple ; grâce au menu déroulant ([voir la page Éditer un Hôte](#)).
- En éditant les fichiers de définition d'élément ([.cfg](#)) :
 - Dans un fichier de configuration, créez ou éditez votre définition d'hôte en ajoutant, dans la propriété "**use**", la valeur "**cisco-WIFI-by-SNMPv3__Controller__authPriv**".
 - Le fichier de configuration devra alors être importé avec une source ([voir la page Collecteur de type \(cfg-file-import \) - Import depuis des fichiers au format .cfg](#)).

Liste des modèles à utiliser dans le pack

Nom	Lien
cisco-WIFI-by-SNMPv1v2__Access-Point	Modèle cisco-WIFI-by-SNMPv1v2__Access-Point
cisco-WIFI-by-SNMPv1v2__Controller	Modèle cisco-WIFI-by-SNMPv1v2__Controller
cisco-WIFI-by-SNMPv3__Access-Point__noAuthNoPriv cisco-WIFI-by-SNMPv3__Access-Point__authNoPriv cisco-WIFI-by-SNMPv3__Access-Point__authPriv	Modèles cisco-WIFI-by-SNMPv3__Access-Point__(noAuthNoPriv / authNoPriv / authPriv)
cisco-WIFI-by-SNMPv3__Controller__noAuthNoPriv cisco-WIFI-by-SNMPv3__Controller__authNoPriv cisco-WIFI-by-SNMPv3__Controller__authPriv	Modèles cisco-WIFI-by-SNMPv3__Controller__(noAuthNoPriv / authNoPriv / authPriv)

Personnaliser son pack

Il est possible de modifier certains éléments ([commandes, checks ou modèles d'hôtes](#))

- voir la page [Les bonnes pratiques d'utilisation d'un pack livré par Shinken](#) .

Version des scripts livrés

Nom	Version	Description
check-cisco-wlc.py	01.00.00	Script principal utilisé pour vérifier l'état des contrôleurs Cisco WLAN et des points d'accès associés. Écrit en Python, il utilise un "virtual env" livré par Shinken pour fonctionner (Aucune dépendance à installer).