

Modèles d'hôtes pour SNMPv3 du pack cisco-WIFI-by-SNMP__shinken

Sommaire

- Contexte
- Liste des modèles d'hôte pour SNMPv3
- Les différents modes de connexions SNMPv3
 - noAuthNoPriv
 - authNoPriv
 - authPriv
- Pour résumer

Contexte

Pour superviser les contrôleurs Cisco WLAN et les points d'accès via le protocole SNMPv3, le pack cisco-WIFI-by-SNMP vous propose les modèles d'hôtes :

- cisco-WIFI-by-SNMPv3__Controller__(noAuthNoPriv / authNoPriv / authPriv)** qui permet la supervision des ressources et de l'état matériel du contrôleur (*Cpu, Memory, Hardware Health*). L'unique différence entre ces trois modèles est la configuration de la connexion SNMPv3.
- 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 (*Access Point Status, Client Connected*). L'unique différence entre ces trois modèles est la configuration de la connexion SNMPv3.



Les [Modèles d'hôtes pour SNMPv1 et v2](#) contiennent des checks identiques, mis à part un mode de connexion moins sécurisé.

Liste des modèles d'hôte pour SNMPv3

Nom	Lien
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)
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)



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

- **cisco-WIFI-by-SNMPv3__Controller__(noAuthNoPriv / authNoPriv / authPriv)**
- **cisco-WIFI-by-SNMPv3__Access-Point__(noAuthNoPriv / authNoPriv / authPriv)**

Ceux-ci héritent des modèles suivants :

- **cisco-WIFI-by-SNMPv3__Controller__(noAuthNoPriv / authNoPriv / authPriv)__shinken**
- **cisco-WIFI-by-SNMPv3__Access-Point__(noAuthNoPriv / authNoPriv / authPriv)__shinken**

Ils contiennent toute la logique du pack.

- Vous ne devez **pas modifier ces modèles internes**, (finissant par la particule '**__shinken**') cela risque d'écraser vos modifications lors des mises à jour du pack.



Si vous avez besoin d'aide au fonctionnement des différents modèles, consultez la page [Mise en place du Pack cisco-WIFI-by-SNMP__shinken](#)

Les différents modes de connexions SNMPv3

noAuthNoPriv

Dans ce mode, il n'y a ni authentification ni chiffrement. Les requêtes SNMPv3 **ne sont pas sécurisées**, car aucune vérification d'identité ou de confidentialité des données n'est effectuée.

authNoPriv

Ce mode offre l'**authentification** des messages SNMPv3 sans chiffrement. L'authentification assure que les messages proviennent d'une source légitime, mais les données échangées ne sont pas chiffrées. Il y a donc une intégrité des données, mais elles peuvent être lues en transit.

authPriv

C'est le mode le plus sécurisé. Il comprend à la fois l'**authentification** et le **chiffrement** des messages SNMPv3. L'authentification garantit l'identité des parties impliquées, tandis que le chiffrement assure la confidentialité des données en les rendant illisibles pour toute personne non autorisée.

Pour résumer

SNMPv3 propose différents **modes de connexion** pour gérer les appareils réseau.

- Ces modes incluent l'**authentification**, qui vérifie l'identité de l'utilisateur, et le **chiffrement**, qui protège les données échangées.
- Shinken met à disposition pour les supervisions d'un contrôleur Cisco WLAN ou d'un point d'accès Cisco en SNMPv3, **3 modèles d'hôtes par famille**.
- Ils sont reconnaissables à leur nom de modèle d'hôte, avec une de ces trois particules dans leur nom (**authPriv**, **authNoPriv**, **noAuthNoPriv**).

Voici les **différences** entre ces 3 modes de connexion :

Mode de connexion	Authentification	Chiffrement	Intégrité des données
noAuthNoPriv	Non	Non	Non
authNoPriv	Oui	Non	Oui
authPriv	Oui	Oui	Oui