Modèles Switch-SNMPv3-(noAuthNoPriv / authNoPriv / authPriv)-detailed

Sommaire

Contexte

Les modèles modèles **Switch-SNMPv3-authPriv-detailed, Switch-SNMPv3-authNoPriv-detailed et Switch-SNMPv3-noAuthNoPriv-detailed** permettent d'avoir un point de vue plus détaillé sur **chaque interface** du switch, et donner des informations plus précises comme la mémoire RAM disponible et l'état du CPU.

> Si le besoin de modifier certains éléments (*commandes, checks ou modèles d'hôtes*) se présente, il faut lire la page Les bonnes pratiques d'utilisation d'un pack livré par Shinken).

Les différents modes de connexions

> Quel que soit le mode de connexion choisi, les checks retourneront tous les mêmes informations.

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 certaine 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 switch en SNMPv3, **3 modèles d'hôtes**.
  - Ils sont reconnaissables à leur nom de modèles d'hôtes, avec une de ces trois particules dans leur nom (**authPriv, authNoPriv, noAuthNoPriv**).

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

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

Sommaire des checks

Nom	Description
`Hardware Health Switch SNMPv3`	Il vérifie le bon fonctionnement physique du matériel de l'appareil (*alimentation, ventilateurs, températures, disques…*). (*voir la page Hardware Health Switch SNMPv3 (modèle Switch-SNMPv3-detailed)*)
`Cpu Switch SNMPv3`	Il récupère et affiche les informations concernant l'utilisation du/des processeur(s) du switch. (*voir la page Cpu Switch SNMPv3*)
`Memory Switch SNMPv3`	Il récupère et affiche les informations sur l'utilisation mémoire du switch. (*voir la page Memory Switch SNMPv3*)
KEY : Errors Switch SNMPv3 *(**exemple : KEY = Vlan201, Vlan202*** => *Vlan201: Errors Switch SNMPv3* => *Vlan202: Errors Switch SNMPv3)*	Il récupère et affiche le taux moyen d'erreurs en entrée et en sortie des interfaces. (*voir la page KEY Errors Switch SNMPv3*)
KEY : Status Switch SNMPv1v2 *(**exemple : KEY = Vlan201, Vlan202*** => *Vlan201: Status Switch SNMPv3* => *Vlan202: Status Switch SNMPv3)*	Il récupère et affiche les informations concernant le statut des interfaces réseaux de votre switch. (*voir la page KEY Status Switch SNMPv3*)
KEY : Usage Switch SNMPv1v2 *(**exemple : KEY = Vlan201, Vlan202*** => *Vlan201: Usage Switch SNMPv3* => *Vlan202: Usage Switch SNMPv3)*	Il récupère et affiche les informations sur le volume d'utilisation de toutes les interfaces réseaux de votre switch. (*voir la page KEY Usage Switch SNMPv3*)

Les données

Les données communes

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description

SNMP_LOGIN	l'Hôte *(Onglet Données)*	--	shinken	**shinken**	Un nom d'utilisateur SNMP v3 défini sur votre switch : • Un nom unique qui identifie l'utilisateur SNMPv3
SNMP_CONTEXT	l'Hôte *(Onglet Données)*	--	public	**public**	Le contexte SNMPv3 permet d'identifier et d'isoler un espace de gestion spécifique sur un agent réseau SNMPv3. Il est utilisé pour définir un domaine de gestion distinct au sein d'un même appareil réseau, permettant ainsi de segmenter et d'organiser les données SNMPv3.
SWITCH_TIMEOUT	l'Hôte *(Onglet Données)*	secondes	60	**60**	Variable permettant au check de s'arrêter après un certain temps si une tâche ne s'est pas terminée. • Permet d'éviter que le programme ne s'exécute indéfiniment et de prévenir des problèmes de performances. *(La valeur doit être supérieure à 3)*
SWITCH_PORT	l'Hôte *(Onglet Données)*	--	161	**161**	Variable correspondant au port SNMP sur lequel le démon SNMP de votre équipement écoute. *(par défaut 161)*
SWITCH_WORKING_FOLDER	l'Hôte *(Onglet Données)*	--	/var/tmp/check_nwc_health	**/var/tmp/check_nwc_health**	Dossier dans lequel la sonde stockera ses fichiers de travail

Mode de connexion noAuthNoPriv

Pas de données communes supplémentaires pour ce mode de connexion

Mode de connexion authNoPriv

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
SWITCH_PROTOCOL_AUTH	l'Hôte *(Onglet Données)*	--	MD5	**MD5**	Protocole utilisé pour vérifier l'authenticité des messages SNMPv3
SWITCH_PASSPHRASE_AUTH	l'Hôte *(Onglet Données)*	--	shinkenpassword	**shinkenpassword**	Chaîne secrète utilisée pour vérifier l'authenticité des messages SNMPv3.

Mode de connexion authPriv

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description	
SWITCH_PROTOCOL_AUTH	l'Hôte *(Onglet Données)*	--	MD5	**MD5**	Protocole utilisé pour vérifier l'authenticité des messages SNMPv3	
SWITCH_PASSPHRASE_AUTH	l'Hôte *(Onglet Données)*	--	shinkenpassword	**shinkenpassword**	Chaîne secrète utilisée pour vérifier l'authenticité des messages SNMPv3.	

SWITCH_PROTOCOL_PRIV	l'Hôte *(Onglet Données)*	--	DES	**DES**	Protocole utilisé pour chiffrer les données SNMPv3	
SWITCH_PASSPHRASE_PRIV	l'Hôte *(Onglet Données)*	--	shinkencryptionkey	**shinkencryptionkey**	Chaîne secrète utilisée pour chiffrer et déchiffrer les données SNMPv3.	

Les données spécifiques

Pour le check "Cpu Switch SNMPv3"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
SWITCH_CPU_LOAD_CRIT	l'Hôte *(Onglet Données)*	Pourcentage	90	**90**	Valeur de charge à partir de laquelle le check passe en CRITIQUE.
SWITCH_CPU_LOAD_WARN	l'Hôte *(Onglet Données)*	Pourcentage	80	**80**	Valeur de charge à partir de laquelle le check passe en AVERTISSEMENT.

Pour le check "Memory Switch SNMPv3"

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description
SWITCH_MEMORY_USAGE_CRIT	l'Hôte *(Onglet Données)*	Pourcentage	90	**90**	Valeur de charge à partir de laquelle le check passe en CRITIQUE.
SWITCH_MEMORY_USAGE_WARN	l'Hôte *(Onglet Données)*	Pourcentage	80	**80**	Valeur de charge à partir de laquelle le check passe en AVERTISSEMENT.

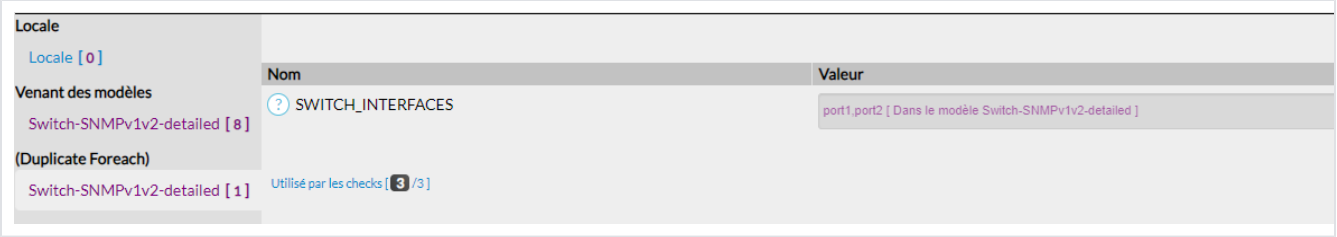
Les données DFE (Duplicate Foreach)

Nom	Modifiable sur	Unités	Défaut	Valeur par défaut à l'installation de Shinken	Description
SWITCH_INTERFACES	l'Hôte *(Onglet Données)*	---	port1, port2	**port1,port2**	Nom de ou des interfaces (*séparés par une virgule*), exemple "Vlan01,Vlan02,Vlan03". Check(s) impacté(s) : • KEY Errors Switch SNMPv3. • KEY Status Switch SNMPv3. • KEY Usage Switch SNMPv3.

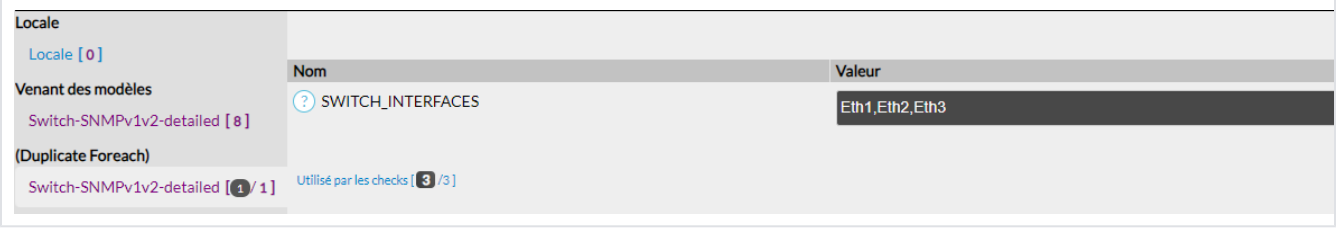
Utilisation

Il vous faudra saisir les noms des interfaces à surveiller :

- Dans l'exemple ci-dessous, le modèle liste **par défaut** les interfaces appelées **port1** et **port2**.



- Changer cette liste avec les noms qui concernent votre équipement :
  - Par exemple Eth1, Eth2, Eth3, pour avoir les checks surveillant ces interfaces.



Pour cette donnée,

- La **virgule** sert de séparateur.Comment appliquer un modèle d'hôt
- Vous pouvez mettre n'importe quelle chaîne de caractères.
  - Si vous voulez surveiller les interfaces réseaux non continues, comme les Eth1, Eth2, Eth3 et Eth9, Eth10, il vous suffit d'en faire la liste :

```
Eth1,Eth2,Eth3,Eth9,Eth10
```

Astuce

Si vous voulez générer une liste de 256 ports de la forme Eth0,Eth1, Eth2, ... Eth255, le faire à la main serait très fastidieux!

Nous avons donné la possibilité de générer **AUTOMATIQUEMENT** les nombres :

- La syntaxe **[nombre1-nombre2]** permet de générer plusieurs valeurs
- donc pour avoir notre liste, saisissez **Eth[0-255]**

Syntaxe	Résultats	Commentaire
Eth[5-9]	Eth5,Eth6,Eth7,Eth8,Eth9	Pour une liste d'interfaces continues
Eth[5-9], Eth [60-65]	Eth5,Eth6,Eth7,Eth8,Eth9,Eth60,Eth61,Eth62,Eth63,Eth64, Eth65	Pour faire des sauts entre plusieurs listes d'interfaces continues
Eth[2-3][0-5]	Eth20,Eth21,Eth22,Eth23,Eth24,Eth25,Eth30,Eth31,Eth32, Eth33,Eth34,Eth35	Pour faire un saut régulier entre des listes d'interfaces

La génération de la liste des valeurs souhaitées se fera par l'Arbiter après la mise en production, elle sera visible uniquement dans l'interface de visualisation, du coté de l'interface de production la syntaxe du DFE ne seras pas interprétée.

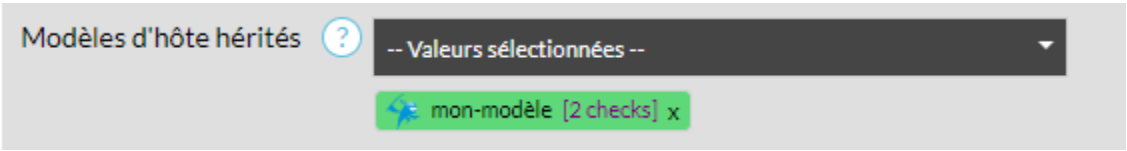
Comment appliquer un modèle d'hôte à un hôte

Application du modèle via l'interface de Configuration

Dans l'interface de Configuration :

- créer ou éditer un hôte (*voir la page Éditer un Hôte*),

- ajouter le modèle "**mon-modèle**" (*selon vos besoins*) dans la propriété "**Modèles d'hôte hérités**" à l'aide du menu déroulant.



Application du modèle via un collecteur d'import de fichiers au format .cfg

Dans votre fichier de définition de vos éléments à importer via votre collecteur :

- créer ou éditer la définition de votre hôte,
- ajouter la valeur **mon-modèle** (*selon vos besoins*), dans la propriété "**use"**,
- importer le contenu du fichier via un collecteur de type "cfg-file-import" (*voir la page Collecteur de type (cfg-file-import) - Import depuis des fichiers au format .cfg*).

```
define host {
    host_name   mon_hôte
    use         mon-modèle
}
```