Widget "Tous les checks"

Contexte

Remarque

⚠ Attention, les modèles d'hôtes se différencient juste par les paramêtres 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

Pour utiliser la connexion SNMPv3, le pack switch vous offre 6 modèles d'hôtes.

Les 6 modèles d'hôtes qui vont premettre de faire une connexion en SNMPv3, peuvent être divisés en 2 catégories :

- Les modèles d'hôtes qui offrent une vue gloable sur les interfaces du switch (expliqué dans la partie gauche du tableau ci-dessous), soit : *switch-SNMPv3-authPriv, switch-SNMPv3-authNoPriv et switch-SNMPv3-noAuthNoPriv*
- Les modèles d'hôtes qui offrent une vue spécifique sur chaques interfaces du switch (expliqué dans la partie droite du tableau ci-dessous), soit : *switch-SNMPv3-authPriv-detailed, switch-SNMPv3-authNoPriv-detailed et switch-SNMPv3-noAuthNoPriv-detailed*

Différence entre les modèles simple et detailed (exemple: switch-SNMPv3-authPriv, switch-SNMPv3-authPriv-detailed)

switch-SNMPv3-authPriv, switch-SNMPv3-authNoPriv, switch-SNMPv3-noAuthNoPriv	**switch-SNMPv3-authPriv-detailed, switch-SNMPv3-authNoPriv-detailed, switch-SNMPv3-noAuthNoPriv-detailed**
• Ces modèles offrent une vue d'ensemble pour chaque check sur l'état général de vos interfaces • Mise a part la mise en place du protocol SNMP, il ne nécéssite aucune configuration • Ces modèles sont donc conseillés si vous voulez une vue sur l'ensemble de vos interfaces en un seul résultat, mais attention, si un problème est rencontré même sur une seule des interfaces, alors le résultat indiquant l'erreur risque d'être noyé par la masse d'informations renvoyées par le check.De même, si un second problème venait à apparaître, il en serait alors, encore plus difficilement repérable.	• Ces modèles vous offrent une vue éclatée, c'est a dire un résultat interface par interface pour chaque check que vous allez effectuer • En plus de configurer SNMP, il sera nécessaire de configurer le nom de toutes les interfaces dans l'interface de configuration Shinken • Ces modèles sont conseillés si vous vous voulez voir une description interface par interface des différents checks proposé, cela vous demande une configuration, mais si un problème vient à apparaître, il vous indiquera alors l'interface qui pose problème.

Les différences entre les méthodes d'authentifications

Parmis les 6 modèles d'hôtes disponibles, vous retrouverez dans le nom de chacun de ces modèles, une de ces itérations : noAuthNoPriv, autNoPriv ou authPriv.

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

Paramêtres et explications

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 a remplir sont donc les suivants :

	Description	Valeur par défaut
SWITCH_LOGIN	Login SNMP v3 • EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login/mot de passe	shinken

authNoPriv

Ce mode d'authenfication est le mode intermédiaire au niveau de l'authentification. Il utilise un login, un mot de passe et une protocole d'authentification.

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

Les champs a remplir sont donc les suivants :

	Description	Valeur par défaut
SWITCH_LOGIN	Login SNMP v3 • EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login /mot de passe	shinken
SWITCH_PROTOCOL_AUTH	Protocol d'authentification SNMPv3 • Ce protocol n'est pas obligatoire mais conseillé pour une meilleur sécurisation de la connexion. • Deux protocol sont possibles ici, **MD5** ou **SHA**	sha
SWITCH_PASSPHRASE_AUTH	Mot de passe d'authentification SNMPv3 • Le mot de passe garantit l'intégrité des données et permet de'authentifier l'origine des données	shinkenpassword

authPriv

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

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

Les champs a remplir sont donc les suivants :

	Description	Valeur par défaut
SWITCH_LOGIN	Login SNMP v3 • EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login/mot de passe	shinken

SWITCH_PROTOCOL_AUTH	Protocol d'authentification SNMP v3 • Ce protocol n'est pas obligatoire mais conseillé pour une meilleur sécurisation de la connexion. • Deux protocol sont possibles ici, **MD5** ou **SHA**	sha
SWITCH_PASSPHRASE_AUTH	Mot de passe d'authentification SNMP v3 • Le mot de passe garantit l'intégrité des données et permet de'authentifier l'origine des données	shinkenpassword
SWITCH_PROTOCOL_PRIV	Protocol de confidentialité SNMP v3 • Ce protocol n'est pas non plus obligatoire, mais tout comme le protocol d'authentification, il permet une sécurité suppleméntaire pour la communication via SNMP • Deux protocoles sont possibles ici, **AES** ou **DES**	aes
SWITCH_PASSPHRASE_PRIV	Mot de passe de confidentialité SNMP v3 • Le mot de passe de confidentialité assure le chiffrement et le déchiffrement des données.	shinkencryptionkey

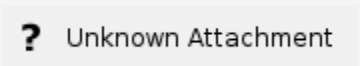
Paramètre supplémentaires pour les modèles finissant par -detailed

Pour les modèles suivant : "switch-SNMPv3-authPriv-detailed"," switch-SNMPv3-authNoPriv-detailed" et "switch-SNMPv3-noAuthNoPriv-detailed"

- Il sera nécéssaire de remplir une donnée supplémentaire, SWITCH_INTERACES.

Pour la donnée en Duplicate Foreach, il vous faudra rentré le nom des interfaces qui vont être surveillées (*SWITCH_INTERFACES*) :

- 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 surveillantes ces interfaces.

Pour cette donnée,

- La **Virgule** sert de séparateur
- Vous pouvez mettre n'importe quel chaine de caractère.
  - Si vous voulez surveiller l'interfaces non continue, comme les Eth1, Eth2, Eth 3 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 port de la forme Eth0,Eth1, Eth2, ... Eth255, le faire à la main sera trés fastidieux!

Nous avons donnez la possiblité de générer **AUTOMATIQUEMENT** les nombres

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

Synthaxe	Résultats	Commentaire
Eth[5-9]	Eth5,Eth6,Eth7,Eth8,Eth9	Pour une liste d'interfaces continue
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

Test de connexion pour s'assurer de la configuration SNMPv3

Test de connexion

```
[root@shinken-poller ~]# snmpwalk -v3 -l SecurityLevel -u LOGIN -a AUTH -A AUTHPASSWORD -x PRIV -X
PRIVPASSWORD IP-SWITCH
```

Il vous faudra alors remplacer :

1. **SecurityLevel** par : **noAuthNoPriv** ou **authNoPriv** ou **authPriv** suivant la configuration de votre connexion SNMPv3.
2. **LOGIN** par le login utilisé sur le switch.
3. **AUTH** l'algorithm d'authenfication que vous avez choisi pour la connexion (**md5** ou **sha).**
4. **AUTHPASSWORD** par le mot de passe que vous avez choisi pour l'authentification SNMPv3.
5. **PRIV** par le protocole de confidentialité que vous avez choisi pour la connexion SNMPv3 (**aes** ou **des).**
6. **PRIVPASSWORD** par le mot de passe de confidentialité que vous avez choisi pour la connexion SNMPv3.
7. **IP-SWITCH** par l'adresse IP de votre switch.

Une liste de valeur doit défiler à l'écran pour valider la bonne connexion.

```
$ snmpwalk -v3 -l authPriv -u newUser -a MD5 -A abc12345 -x DES -X abc12345 192.168.1.5 -v3
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software

IOS (tm) 7200 Software (C7200-IS-M), Version 12.3(21b), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2007 by cisco Systems, Inc.

Compiled Sat 21-Jul-07 16:57 by ccai
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.223
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3597) 0:00:35.97
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: Xiamen-R
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 6
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 5
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
...
```

Version des scripts livrés

check_nwc_health : 10.3.0.2