Guide d'Administration

Contexte

Le pack Switch vous offre deux manières de vous connecter en SNMP.

La version 1/2c qui correspond aux modèles d'hôtes suivant : *switch et switch-detailed*

On a ensuite 6 modèles d'hôtes que l'on peux divisé en 2 catégories et qui vont premettre de faire une connexion en Sersion 3 :

- 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 (switch, switch_snmp_v3) et (switch-detailed, switch_snmp_v3-detailed)

switch | switch_snmp_v3	switch-detailed | switch_snmp_v3-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

SNMPv1/2c

Une seule méthode pour s'authentifier est possible

En effet, en SNMPv1/2c le seul moyen sécuritaire qui est proposé est l'utilisation d'un nom de communauté qui servira de mot de passe pour les utilisateurs voulant récupérer les informations du matériel ciblé

SNMPv3

noAuthNoPriv

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

Ici, le seul champ a remplir est SWITCH_LOGIN.

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

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 champs a remplir sont donc : SWITCH_LOGIN, SWITCH_PASSPHRASE_AUTH et SWITCH_PROTOCOL_AUTH

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

authPriv

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

Les champs a remplir sont donc : SWITCH_LOGIN, SWITCH_PASSPHRASE_AUTH, SWITCH_PROTOCOL_AUTH, SWITCH_PASSPHRASE_PRIV et SWITCH_PROTOCOL_PRIV

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

Test de connexion pour s'assurer de la configuration SNMP

Les différents tests

Vous pouvez tester la bonne configuration du service SNMP de votre switch depuis votre serveur Poller en fonction du SNMP utilisé

SNMP V2

```
[root@shinken-poller ~]# snmpwalk -v2c -c COMMUNAUTE IP-SWITCH
```

En replaçant COMMUNAUTE et IP-SWITCH par ceux de votre switch.

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

```
$ snmpwalk -v2c -c public 192.168.1.4
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System SoftwareIOS (tm) MSFC Software (C6MSFC-
JS-M), Version 12.0(7)XE1, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)TAC:Home:SW:IOS:Specials for infoCopyright
(c) 1986-2000 by cisco Systems, Inc.Compiled Thu 03-Feb-00 23:
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.258
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (22061) 0:03:40.61
SNMPv2-MIB::sysContact.0 = STRING: admin
SNMPv2-MIB::sysName.0 = STRING: CISCOROUTER
SNMPv2-MIB::sysLocation.0 = STRING: server-room
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 13
IF-MIB::ifIndex.2 = INTEGER: 2
...
```

SNMP V3

```
[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
...
```

PASSS

SNMP v3

Dans chaque hôte héritant du modèle d'hôte **"switch_SNMP_v3" ou "switch_SNMP_v3-detailed"**, vous aurez plusieurs données a modifier ou no
suivant la configuration SNMP choisi :

	Description	Valeur par défaut	Valeur par défaut à l'installation de shinken

SWITCH_LOGIN	Login SNMP v3 • EN SNMP v3, la communauté est un équivalent du nom d'utilisateur dans une doublet login /mot de passe		
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**		
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		
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**		
SWITCH_PROTOCOL_PRIV	Mot de passe de confidentialité SNMP v3 • Le mot de passe de confidentialité assure le chiffrement et le déchiffrement des données.		

Version des scripts livrés

check_nwc_health : 10.3.0.2