Collecteur de type discovery-import (Scan NMAP)

Sommaire

Procédure de mise en place du pack

Installation des sondes du pack

Les sondes du pack (*et leurs dépendances*) sont installées et mises à jour automatiquement par Shinken si votre source "**cfg-file-shinken**" est activée.

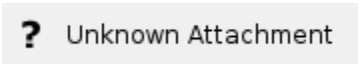
Cas particuliers : Plusieurs Pollers dans un même royaume

La sonde *check_nwc_health* utilisée par le pack Switch-SNMP écrit des fichiers temporaires locaux à l'endroit d'exécution de la sonde. Donc si cette sonde est exécutée sur un Poller puis un autre, elle n'aura pas les valeurs de la précédente exécution.

Ainsi, si vous avez plusieurs Pollers dans un même royaume, vous devrez mettre en place un dossier partagé accessible par tous vos Pollers afin de garder de la cohérence dans les résultats retournés par la sonde.

⚠ Pour votre dossier partagé, ne pas utiliser de partage Windows (*samba*), car la sonde étant lancée avec les droits du démon Poller (*shink en*) elle aura des problèmes d'accès/écriture au répertoire.

Une fois que vous avez créé ce dossier partagé, il faudra modifier la donnée "SWITCH_WORKING_FOLDER" (*dans l'interface de configuration*) de l'hôte avec le chemin absolu du dossier partagé :



Import des modifications suite à une mise à jour de Shinken

Suite à une mise à jour de Shinken, et si le pack Switch a été modifié, la source "cfg-file-shinken" sera réimportée (*si active*) :

- Des différences vous seront proposées pour mettre à jour les éléments du pack (*modèles d'hôtes, checks, commandes, etc...*).
- Nous vous conseillons d'accepter les nouveaux éléments et les différences de cette source afin de profiter des dernières mises à jour.

Modifier vos seuils

Tous les checks retournant des erreurs ou l'utilisation d'interfaces dans le pack Switch-SNMP possèdent la donnée CUSTOM_THRESHOLD.
Cette donnée donne à un utilisateur la possibilité de changer les seuils par défaut définis par la sonde, ainsi que certains seuils spécifiques à une interface.

Modifier les seuils pour toutes les interfaces en même temps

Par défaut, la sonde nous donne les seuils suivants pour tous les checks du pack Switch-SNMP qui interrogent les erreurs d'une interface.

? Unknown Attachment

En surchargeant la donnée CUSTOM_THRESHOLD sur le check par :

```
--warning 60 --critical 70
```

On obtient les nouveaux seuils suivants :

? Unknown Attachment

Modifier les seuils pour une ou plusieurs interfaces

Il est aussi possible de vouloir mettre des seuils différents suivant l'interface que vous allez utiliser.
Par exemple, sur les checks interrogeant l'utilisation des interfaces, nous obtenons les seuils suivants :

? Unknown Attachment

On voudra donc modifier les seuils pour Null0 et Loopback0 mais ne pas toucher à ceux de Vlan201.
Il faut donc utiliser les arguments suivants :

```
--warningx Null0_usage_in=50 --warningx Loopback0_usage_in=60 --criticalx Null0_usage_out=95
```

On obtient nos nouveaux seuils :

? Unknown Attachment

Vérification de la compatibilité SNMP avec le switch à superviser

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

Tester la configuration SNMP v1 ou v2

Remplacer dans la commande ci-dessous :

- VERSION par la version SNMP utilisée (*ici 1 ou 2c*)
- COMMUNAUTE par la communauté paramétrée sur votre switch,
- IP-SWITCH par l'adresse IP de votre switch.

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

Exemple de résultat

Une liste de valeurs doit défiler à l'écran pour valider la bonne connexion (*l'exemple ci-dessous était dans le cadre d'une connexion SNMPv2*).

```
$ snmpwalk -v2c -c public 1.2.3.4
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
...
```

Tester la configuration SNMPv3

Dans le cas de SNMPv3, la liste des arguments de la commande est plus exhaustive, mais tous ne sont pas forcément nécessaires suivant le mode de connexion configuré.

Remplacer ou enlever :

- *IP-SWITCH* par l'adresse IP de votre switch
- *USER-NAME* par le nom d'utilisateur
- *CONTEXT* par le contexte SNMP (*optionnel*),
- *LEVEL* par le niveau de sécurité configuré pour la connexion SNMPv3 (*noAuthNoPriv | authNoPriv | authPriv*),
- *AUTH_PROTOCOL* par le protocole d'authentification utilisé (*à utiliser dans le cas du niveau authNoPriv et authPriv*) ,
- *AUTH_PASSPHRASE* par le mot de passe lié au protocole d'authentification (*à utiliser dans le cas du niveau authNoPriv et authPriv*),
- *PRIV_PROTOCOL* par le protocole de confidentialité utilisé pour la connexion SNMPv3 (*à utiliser dans le cas du niveau authPriv*),
- *PRIV_PASSPHRASE* par le mot de passe lié au protocole de confidentialité (*à utiliser dans le cas du niveau authPriv*),
- *SECU_ENGINE-ID* par l'ID de sécurité (*optionnel*),
- *CONTEXT_ENGINE-ID* par l'ID du contexte (*optionnel*),

```
[root@shinken-poller ~]# snmpwalk -v3 IP-SWITCH -u USER-NAME -n CONTEXT -l LEVEL -a AUTH_PROTOCOL -A
AUTH_PASSPHRASE -x PRIV_PROTOCOL
-X PRIV_PASSPHRASE -e SECU_ENGINE-ID -E CONTEXT_ENGINE-ID
```

Exemple de résultat

Une liste de valeurs doit défiler à l'écran pour valider la bonne connexion (*l'exemple ci-dessous était dans le cadre d'une connexion SNMPv3*).

```
$ snmpwalk -v3 -l authPriv 1.2.3.4 -u MyUser -a MD5 -A Password1 -x DES -X Password2
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: (19974) 0:03:19.74
SNMPv2-MIB::sysContact.0 = STRING: admin
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
...
```