Pack SNMP (linux_by_snmp, windows_by_snmp)

Note : Si vous êtes intéressé par ce pack, veuillez nous contacter pour son téléchargement. Nous vous accompagnerons lors de l'installation de ce pack sur votre plateforme.

Sommaire

- Contexte
- Sommaire des checks
  - Modèle linux_by_snmp
  - Modèle windows_by_snmp
- Les modèles d'hôtes et leurs données héritées
- Comment utiliser le pack snmp_checks
  - En utilisant l'interface de Configuration
  - En éditant les fichiers de configuration
- Configuration de la connexion SNMP
  - Côté client (machine ou serveur supervisé)
    - Linux
      - Serveur en SNMPv3
    - Windows
      - Serveur en SNMPv3
  - Côté serveur Poller
- Problèmes connus
  - Check "Disks SNMP" CRITICAL supérieur à 100% sur une partition ou un point de montage d'une capacité supérieur à 2To
- Version des scripts livrés

Contexte

Lorsque vous installez Shinken Enterprise, un certain nombre de modèles et de commandes sont inclus dans votre configuration.

Le pack "snmp_checks", comme son nom l'indique, permet de superviser des hôtes sur lesquels est installé un système d'exploitation basé sur Linux ou Windows (*serveur ou client*) via le **protocole SNMP**.

Il contient 9 commandes, 9 modèles de checks dédiés à 2 modèles d'hôte spécifiques (nommés "**linux_by_snmp**" et "**windows_by_snmp**").

Toutes les commandes de ce pack se basent sur des scripts présents dans le répertoire des scripts shinken **/var/lib/shinken/libexec** (ou **$PLUGINSDIR$** depuis l'interface de configuration).

Le protocole SNMP (*Simple Network Management Protocol*) est utilisé par chacun des scripts du pack. Les scripts communiqueront donc avec votre machine via le port 161 et la communauté SNMP spécifiée.

Nous allons ici détailler ces checks associés au modèle de ce pack.

Sommaire des checks

2 modèles d'hôtes sont inclus à ce pack, le modèle **linux_by_snmp** (pour les OS Linux) et le modèle **windows_by_snmp** (pour les OS Windows).

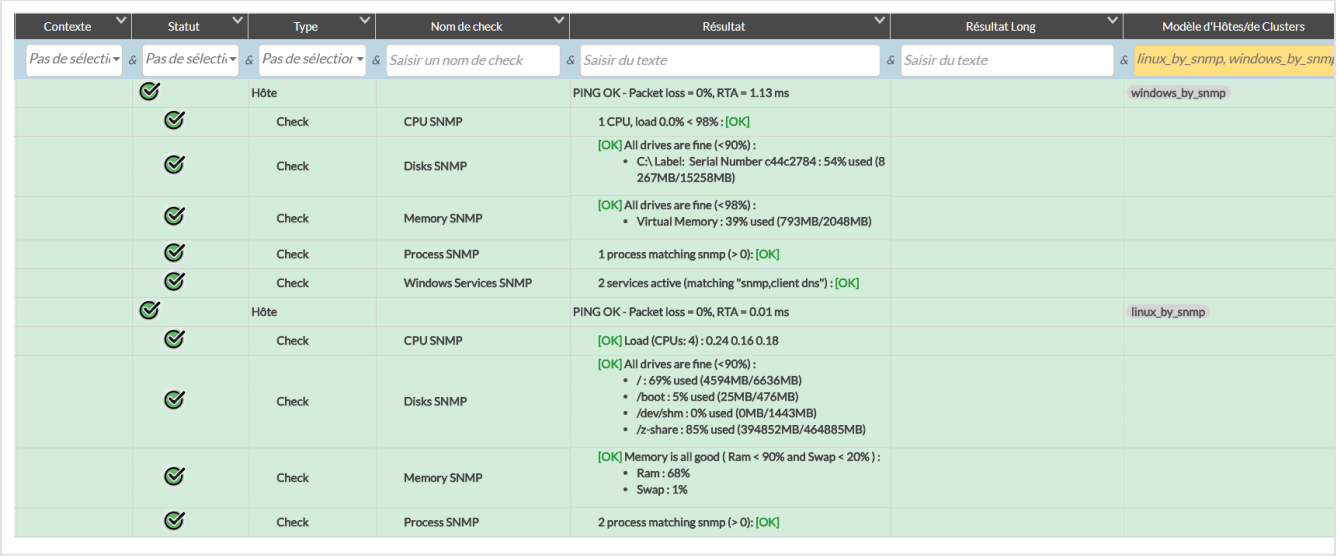
Modèle linux_by_snmp

Check Name	Description
CPU SNMP (linux)	Récupère et vérifie le Load Average du CPU
Disks SNMP (linux)	Récupère et vérifie les informations de taille des disques
Memory SNMP (linux)	Récupère et vérifie les informations concernant la RAM
Process SNMP (linux)	Récupère et vérifie les informations concernant les processus du système

Modèle windows_by_snmp

Check Name	Description
CPU SNMP (windows)	Récupère et vérifie le pourcentage de CPU utilisé
Disks SNMP (windows)	Récupère et vérifie les informations de taille des disques
Memory SNMP (windows)	Récupère et vérifie les informations concernant la RAM
Process SNMP (windows)	Récupère et vérifie les informations concernant les processus du système
Windows Services SNMP (windows)	Récupère et vérifie les informations concernant les services Windows du système

Voici par exemple la supervision de deux hôtes, un windows et un linux avec les checks du pack "snmp_checks" :



Contexte	Statut	Type	Nom de check	Résultat	Résultat Long	Modèle d'Hôtes/de Clusters
Pas de sélecti	Pas de sélecti	Pas de sélectior	Saisir un nom de check	Saisir du texte	Saisir du texte	linux_by_snmp, windows_by_snmp
		Hôte		PING OK - Packet loss = 0%, RTA = 1.13 ms		windows_by_snmp
		Check	CPU SNMP	1 CPU, load 0.0% < 98% : [OK]		
		Check	Disks SNMP	[OK] All drives are fine (<90%) : • C:\ Label: Serial Number c44c2784 : 54% used (8 267MB/15258MB)		
		Check	Memory SNMP	[OK] All drives are fine (<98%) : • Virtual Memory : 39% used (793MB/2048MB)		
		Check	Process SNMP	1 process matching snmp (> 0): [OK]		
		Check	Windows Services SNMP	2 services active (matching "snmp,client dns") : [OK]		
		Hôte		PING OK - Packet loss = 0%, RTA = 0.01 ms		linux_by_snmp
		Check	CPU SNMP	[OK] Load (CPUs: 4) : 0.24 0.16 0.18		
		Check	Disks SNMP	[OK] All drives are fine (<90%) : • / : 69% used (4594MB/6636MB) • /boot : 5% used (25MB/476MB) • /dev/shm : 0% used (0MB/1443MB) • /z-share : 85% used (394852MB/464885MB)		
		Check	Memory SNMP	[OK] Memory is all good (Ram < 90% and Swap < 20%) : • Ram : 68% • Swap : 1%		
		Check	Process SNMP	2 process matching snmp (> 0): [OK]		

Les modèles d'hôtes et leurs données héritées

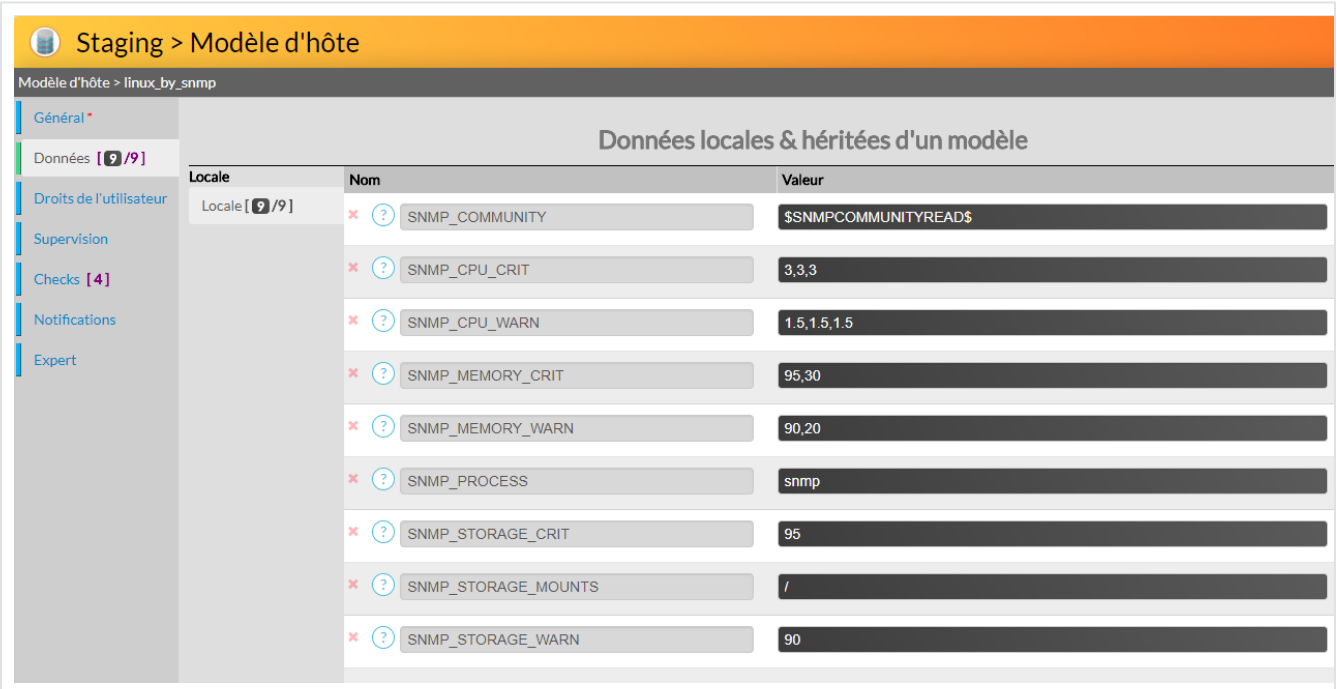
Les modèles d'hôtes **windows_by_snmp** et **linux_by_snmp**, sur lesquels sont accrochés les différents checks dédiés, contiennent des données (locales) qui seront utilisés par les checks. Ces données seront invoquées par les checks et commandes via **$_HOST** suivi du nom de la variable.

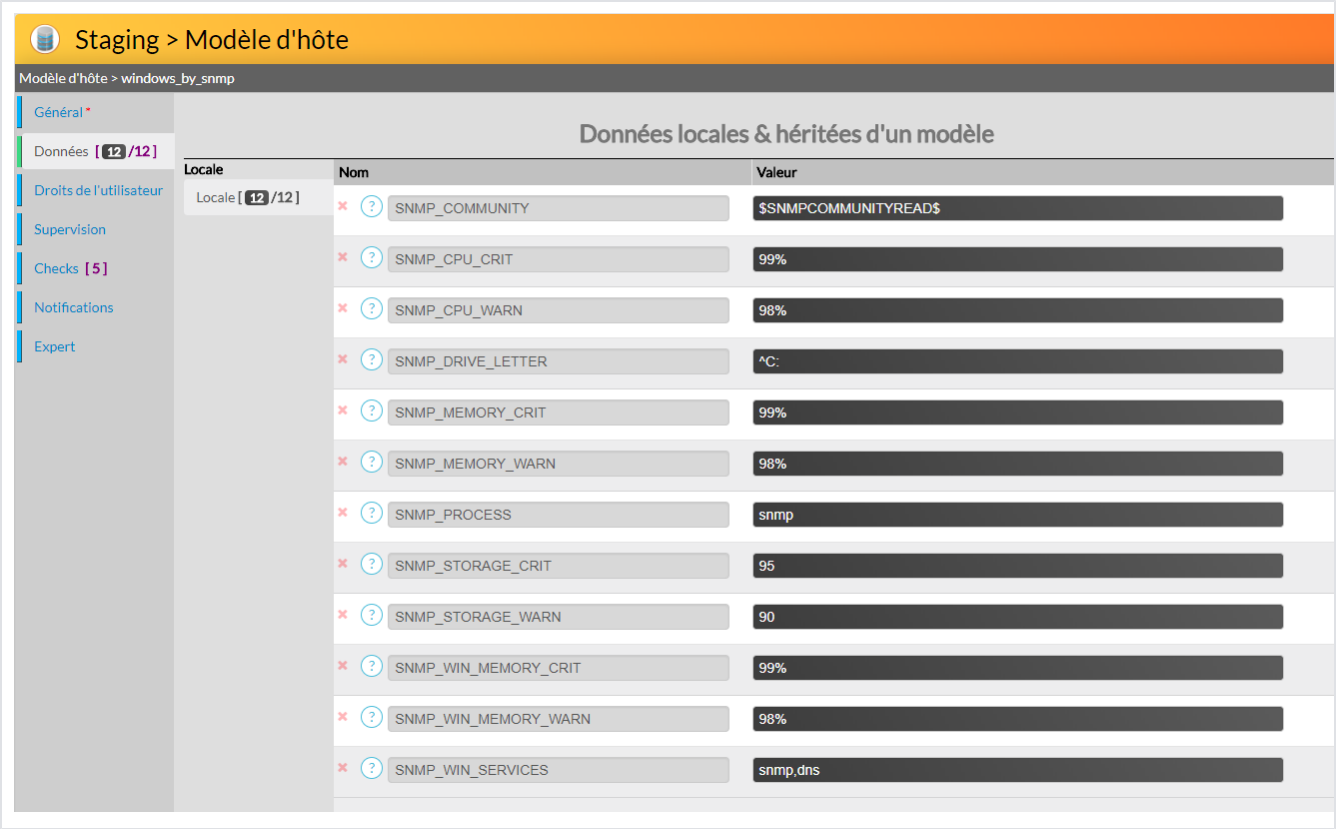
Exemple : **$_HOSTSNMP_PROCESS$** utilisera la donnée nommée **SNMP_PROCESS** (quelle soit locale ou héritée d'un modèle).

Pour un hôte qui hérite par exemple du modèle windows_by_snmp ou linux_by_snmp de notre pack, ces données seront donc héritées également, mais elles pourront aussi être surchargées directement sur l'hôte (attention aux conflits de nom des données).

Si vous souhaitez modifier de manière globale ces données, ou en rajouter, faites le directement sur le modèle voulu, ceci s'appliquera alors à tous vos hôtes utilisant ce modèle.

Pour plus d'information, veuillez consulter la page sur les Les Variables (Remplacement dynamique de contenu - Anciennement les Macros).





Pour la bonne connexion, le nom de communauté est requis. Par défaut, celle-ci se trouve dans le fichier snmp.cfg dans /etc/shinken/resource.d et elle est à définie à *public* :

```
$ cat /etc/shinken/resource.d/snmp.cfg

#-- Discovery
# default snmp community
$SNMPCOMMUNITYREAD$=public
```

Vous pouvez donc changer la communauté par défaut via ce fichier, mais vous pouvez aussi bien entendu surcharger la valeur directement sur le modèle, ou encore directement sur votre hôte supervisé (*donnée* ***SNMP_COMMUNITY***)

Comment utiliser le pack snmp_checks

Le pack **snmp_checks** peut être utilisé en appliquant le modèle souhaité à un hôte. Il existe deux manières de procéder :

En utilisant l'interface de Configuration

Dans l'interface de Configuration, créez ou éditer un hôte (*voir la page* Éditer un Hôte), et ajoutez le modèle **windows_by_snmp** ou **linux_by_snmp** grâce au menu déroulant.

En éditant les fichiers de configuration

Dans un fichier de configuration, créez ou éditez votre définition d'hôte en ajoutant, dans le propriété "**use",** la valeur "**windows_by_snmp"** ou **"linux_by_snmp"** selon les besoins.

Le fichier de configuration devra alors être importé avec une source (*voir la page* Collecteur de type (cfg-file-import) - Import depuis des fichiers au format .cfg).

Configuration de la connexion SNMP

Pour l'exécution correcte des commandes, vous aurez besoin du service SNMP sur l'hôte supervisé.

Côté client (machine ou serveur supervisé)

Linux

Sur votre serveur supervisé avec l'OS Linux, il vous faut installer les paquets **net-snmp** et **net-snmp-utils** :

```
yum -y install net-snmp net-snmp-utils
```

Ensuite, par précaution, faîtes une copie puis éditez le fichier de configuration de snmpd :

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak
vim /etc/snmp/snmpd.conf
```

La ligne suivante permet de changer la communauté *public* vers une communauté propre à votre réseau et plus ou moins complexe (*remplacez "public" par la chaîne de caractères que vous souhaitez*):

```
####
# First, map the community name "public" into a "security name"

#       sec.name  source          community
com2sec notConfigUser  default       public
```

Par défaut, le fichier de configuration associe ensuite (*étape 3 dans le fichier*) le nom de sécurité (*"notConfigUser"*) a une vue d'accès restreintes à certains OID (*"systemview"*).
Pour un accès sur l'ensemble des OIDs du système, utilisez une nouvelle vue, par exemple "*all*":

```
####
# Third, create a view for us to let the group have rights to:
# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
#view    systemview    included   .1.3.6.1.2.1.1
#view    systemview    included   .1.3.6.1.2.1.25.1.1
view    all    included   .1
```

Et par conséquent, remplacez la vue "*systemview*" par "*all*" dans la dernière étape de configuration du fichier :

```
#       group          context sec.model sec.level prefix read   write  notif
access  notConfigGroup ""      any       noauth    exact  all none none
```

Vous pouvez maintenant démarrer le démon SNMPD :

```
service snmpd start
```

Pensez à redémarrer le service snmpd à chaque modification du fichier de configuration snmpd.conf.

Pour un démarrage du service snmpd à chaque démarrage de votre machine, utilisez la commande :

```
chkconfig snmpd on
```

Vous pouvez tester votre service snmpd avec la commande snmpwalk (*changez la communauté si besoin*) :

```
snmpwalk -v 1 -c public localhost
```

Serveur en SNMPv3

Le pack incluant le SNMP V3 nécessite la mise en place d'un utilisateur qui sera utilisé pour se connecter sur les serveurs distants supervisés.

Voici un exemple d'installation et configuration d'un serveur linux distant (*Redhat*) qui sera interroger par le pack en SNMPv3.

```
# Rajout de l'utilisateur shinken
service snmpd stop
net-snmp-create-v3-user -ro -A shinkenpassword -a SHA -X shinkenencryptionkey -x AES shinken
service snmpd start

# Test de connexion en local
snmpwalk -u shinken -A shinkenpassword -a SHA -X shinkenencryptionkey -x AES -l authPriv 127.0.0.1 -v3
```

A noter qu'ici nous avons défini:

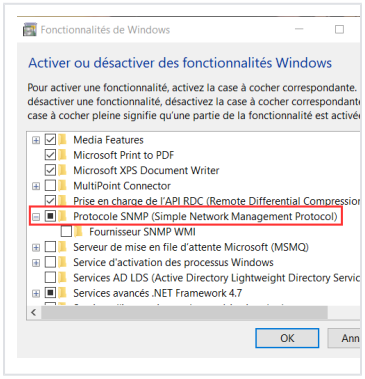
- **shinken**: nom de l'utilisateur côté serveur SNMPv3
- **shinkenpassword**: mot de passe de l'utilisateur. Attention: il ne peux pas être plus petit que 8 caractères.
- **shinkenencryptionkey**: clé de chiffrement pour cet utilisateur
- **AES**: protocole de chiffrement de l'utilisateur
- **SHA**: méthode de hashage des informations de l'utilisateur

Ces **paramètres seront utilisés dans les modèles de supervisions** pour interroger les équipements supervisés.

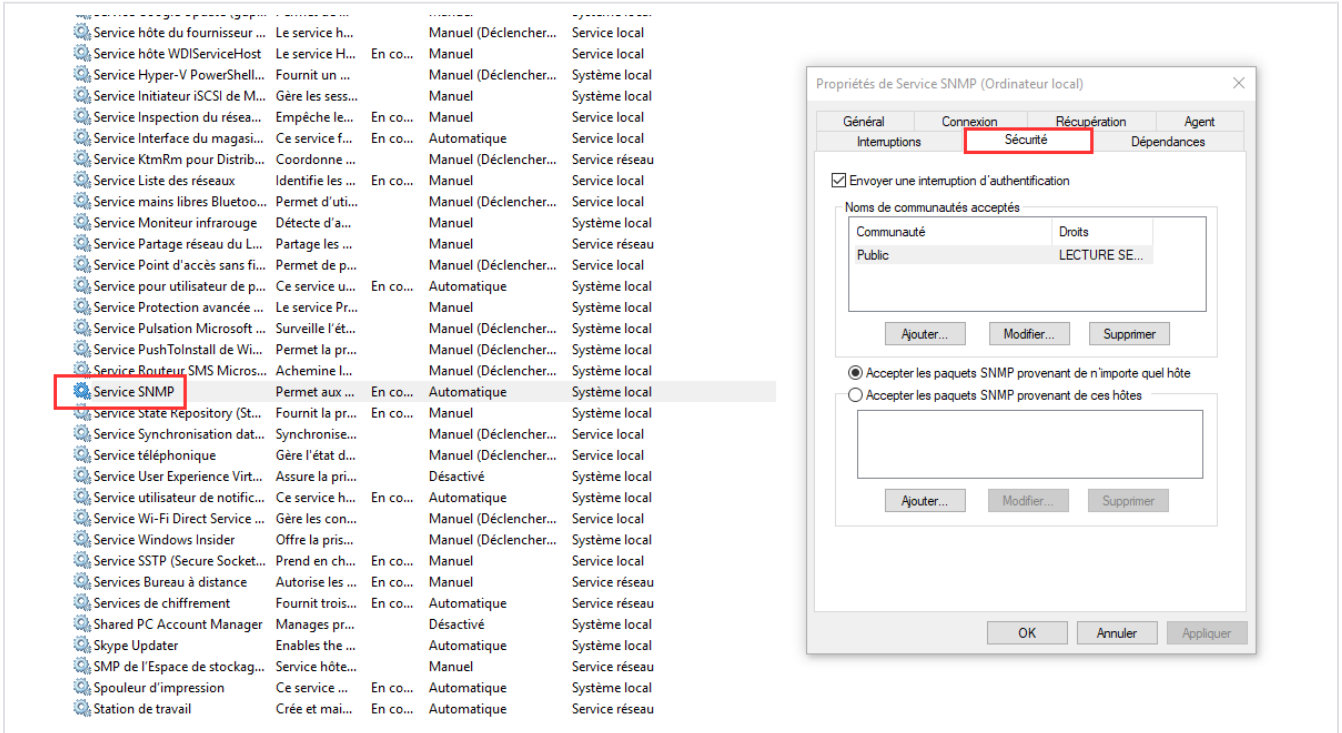
Windows

Sur le système d'exploitation Windows, il vous faut activer la fonctionnalité SNMP :

Suivant la version de Windows, l'activation se fait depuis les "ajouts/suppressions de composants Windows", depuis le "gestionnaire de fonctionnalités Windows", ou encore depuis "la page des rôles et fonctionnalités de serveur Windows".



Une fois l'installation terminée, il vous suffit de paramétrer votre service SNMP depuis la MMC des services Windows (*Démarrer - Exécuter : services.msc*) et ouvrez le Service SNMP:



Vous pouvez alors paramétrer votre Communauté, ainsi que les autorisations (*vous pouvez n'autoriser les requêtes SNMP qu'en provenance de certaines IP*). Vous pouvez ici mettre uniquement les adresses IP de vos Pollers Shinken.

⚠ Si vous ne voyez pas l'onglet Sécurité, veuillez redémarrer votre console MMC.

Serveur en SNMPv3

Windows n'inclus **PAS SNMP v3**, seulement v1 et v2.

C'est assumé par Microsoft qui a mis en deprecated SNMP depuis windows 2012: https://learn.microsoft.com/en-us/answers/questions/622162/how-to-configure-snmp-v3-on-windows-server-2016.html

Il est possible de trouver des agents spécifiques qui l'implémentent, mais ils ne sont pas natifs Microsoft, et nous n'avons pas d'expérience particulière avec eux.

Côté serveur Poller

Les scripts sont exécutés par le ou les serveurs Poller.

- Les commandes sont basées sur des scripts PERL.
- Pour information, les librairies suivantes sont nécessaires:
  - **Déjà installé** par l'installeur de Shinken :
    - Perl
    - net-snmp-utils
    - net-snmp-libs
  - Nécessaire pour SNMP V3 :
    - perl-Crypt-Rijndael (*que vous devez rajouter sur votre OS*)

Problèmes connus

Check "Disks SNMP" CRITICAL supérieur à 100% sur une partition ou un point de montage d'une capacité supérieur à 2To

Une partition ou un point de montage d'une capacité supérieur à 2To peux entrainer une erreur d'affichage dont le seuil d'alerte peux dépasser les 100% d'occupations.

Exécution sur le poller (production) [*poller-master-2*] :

Statut	Résultat	Exécuté dans un Shell	Temps d'exécution
Critical	**Résultat :** CRITICAL : (>99%) /data/fic/plan-interactif/data: 337%used(3541335MB/1050494MB) **Métriques :**	false	0.277

Métrique	Valeur	Seuil d'avertissement	Seuil critique
/cluster	18738MB	98649	99655
/var	12162MB	14691	14841
/dev/shm	58MB	15726	15886
/var/log	727MB	9752	9852
/tmp	85MB	4813	4863
/appli	8957MB	47288	47770
/boot	39MB	956	966
/home	15339MB	19630	19830
/data/fic/plan-interactif/data	3541335MB	1029484	1039989
/usr	1730MB	9752	9852
/data	9712MB	197430	199444
/	4228MB	9752	9852

Métriques brutes :

'/cluster'=18738MB;98649;99655;0;100662 '/var'=12162MB;14691;14841;0;14991 '/dev/shm'=58MB;15726;15886;0;16046 '/var/log'=727MB;9752;9852;0;9951 '/tmp'=85MB;4813;4863;0;4912 '/appli'=8957MB;47288;47770;0;48253 '/boot'=39MB;956;966;0;976 '/home'=15339MB;19630;19830;0;20031 '/data/fic/plan-interactif/data'=3541335MB;1029484;1039989;0;1050494 '/usr'=1730MB;9752;9852;0;9951 '/data'=9712MB;197430;199444;0;201459 '/'=4228MB;9752;9852;0;9951

Pour corriger ce problème il faut éditer le fichier "/etc/snmp/snmpd.conf" du serveur ou se trouve le disque ou le point de montage en question et ajouter le paramètre suivant :

```
realStorageUnits 0
```

Redémarrer le serveur SNMP :

```
systemctl restart snmpd
```

Explication :

realStorageUnits contrôle la façon dont l'agent SNMP rapporte les OIDs hrStorageAllocationUnits, hrStorageSize et hrStorageUsed dans hrStorageTable. Lorsque cette option est définie sur '0', l'agent recalcule ces valeurs pour les grands disques de stockage avec de petites unités d'allocation, de sorte que hrStorageAllocationUnits x hrStorageSize donne la taille réelle du stockage.

Version des scripts livrés

Tous les scripts présents dans ce pack fonctionnent avec les versions 1, 2c et 3 de SNMP.

Nom du script	Version
check_snmp_boostedge.pl	2.1.0
check_snmp_cpfw.pl	2.1.0
check_snmp_css_main.pl	2.1.0
check_snmp_css.pl	2.1.0
check_snmp_env.pl	2.1.0
check_snmp_int.pl	2.1.0
check_snmp_linkproof_nhr.pl	2.1.0
check_snmp_load.pl	2.1.0
check_snmp_mem.pl	2.1.0
check_snmp_nsbox.pl	2.1.0
check_snmp_process.pl	2.1.0
check_snmp_storage.pl	2.1.0
check_snmp_vrrp.pl	2.1.0
check_snmp_win.pl	2.1.0