Annexe 1 Surveiller un équipement réseau avec SNMP

| Sommaire : |
|---|
| I - Simple Network Management Protocol : SNMP1 |
| II - Le manager SNMP sous Linux2 |
| III - Surveiller un équipement CISCO avec SNMP3 |
| III.1. Installation et configuration de l'agent SNMP sur un routeur CISCO |
| III.2. Supervision du routeur CISCO3 |
| IV - Surveiller une machine Linux avec SNMP5 |
| IV.1. Installation et configuration de l'agent SNMP sur une machine Linux |
| IV.2. Supervision de la machine Linux5 |
| V - Surveiller une machine Windows avec SNMP6 |
| V.1. Installation et configuration de l'agent SNMP sur une machine Windows6 |
| V.2. Supervision de la machine Windows8 |
| |

I - Simple Network Management Protocol : SNMP

SNMP (Simple Network Management Protocol) est un protocole qui permet aux administrateurs réseaux de gérer les équipements et de diagnostiquer les problèmes.

Un périphérique réseau (routeur, switch, pare-feu, ...) exécute un **agent SNMP** qui est en fait un processus **serveur** qui répond aux requêtes du réseau. L'interrogation d'un **agent** par le **manager SNMP** (ou **client SNMP**) se fait en lui envoyant des messages sur le port **UDP 161**. L'agent envoie des alertes au **manager** sur le port **UDP 162**.



L'agent SNMP fournit des données qui sont organisées de manière hiérarchique et représenté par un OID (Object IDentifier) : Un OID est une paire clé-valeur unique. Les OID SNMP peuvent être lus ou écrits. Les OID sont numériques, par exemple : 1.1.3.6.1.2.1.1.1.0.

Notons qu'il est rare d'écrire des informations sur un périphérique **SNMP**. **SNMP** est surtout utilisé par de nombreuses applications de management pour contrôler l'état des périphériques réseaux. Un système d'authentification basique existe dans **SNMP**, il permet au manager d'envoyer un **community name** (qui est en fait un mot de passe en clair) pour autoriser la lecture ou l'écriture des **OID**. La plupart des périphériques utilisent le **community name** non sécurisé « **public** ».

Les **OID** (**O**bject **ID**entifier) sont organisées de manière hiérarchique dans une **MIB** (**M**anagement Information **B**ase) :



SNMP peut être utilisé de deux manières distinctes : le **polling** et les **traps**.

- Le polling consiste simplement à envoyer une requête à intervalles réguliers pour obtenir une valeur particulière. Cette technique est appelée « vérification active ». Si la requête échoue, il est possible qu'il y ait un problème avec le périphérique. Cependant, vu que le SNMP s'appuie sur UDP, il est conseillé de réitérer la requête pour confirmer le problème (surtout dans le cas d'une vérification au travers d'Internet).
- Les traps consistent à faire de la vérification passive, l'agent SNMP contacte un autre agent SNMP en cas de problème. C'est-à-dire que l'on peut configurer un périphérique réseau (comme un routeur) pour qu'il envoie un trap SNMP lors de certains événements. Par exemple, le routeur peut envoyer un trap lorsqu'il détecte que la ligne est coupée (down). Quand un événement trap apparait, l'agent sur le périphérique va envoyer le trap vers une destination pré-configurée communément appelé trap host. Le trap host possède son propre agent SNMP qui va accepter et traiter les traps lorsqu'ils arrivent. Le traitement des traps est effectué par des trap handlers. Le handler peut faire ce qui est approprié pour répondre au trap, comme envoyer un courriel d'alerte.

Il existe actuellement 3 versions différentes du protocole **SNMP**. La coexistence des trois versions est détaillée dans la **RFC 3584** :

SNMP v1 (RFC 1155, 1157 et 1212). SNMP v2c (RFC 1901 à 1908). SNMP v3 (RFC 3411 à 3418).

II - Le manager SNMP sous Linux

Pour installer le manager SNMP sous Debian, il faut installer Net-SNMP à l'aide de la commande : apt install snmp.

Sous Linux, l'application Net-SNMP fournit des commandes en lignes pour consulter ou administrer des agents SNMP :

- snmpget permet d'obtenir une ou plusieurs données ;
- snmpset permet de définir une ou plusieurs données ;
- snmpwalk permet de parcourir les données disponibles ;
- **snmptranslate** permet de traduire les noms de la MIB en OID.

Exemples :

snmpget -v1 localhost -c public .iso.3.6.1.2.1.1.3.0 iso.3.6.1.2.1.1.3.0 = Timeticks: (367418) 1:01:14.18

snmpwalk -v2c -c public localhost .iso.3.6.1.2.1.1.3.0 iso.3.6.1.2.1.1.3.0 = Timeticks: (372828) 1:02:08.28

III - Surveiller un équipement CISCO avec SNMP

III.1. Installation et configuration de l'agent SNMP sur un routeur CISCO

Il faut se connecter au routeur et passer en mode de configuration. Pour des raisons de sécurités, il est préférable de **désactiver** la communauté **public** et d'**activer** la communauté **privé** :

configure terminal no snmp-server community public ro snmp-server community private ro

On peut ensuite si on le désire activer les **traps SNMP** que l'on veut récupérer. On peut lister les **traps SNMP** que le routeur **Cisco** peut activer grâce à la commande :

snmp-server enable traps ?

Pour plus d'indications sur l'utilité de chacune de ces **traps SNMP**, on peut se référer au **site de Cisco** : <u>http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_18.html</u>

Enfin on active chaque traps SNMP grâce à la commande :

snmp-server enable traps <type> (exemple snmp-server enable traps snmp)

On doit maintenant définir **l'adresse de destination**, ainsi que la **communauté** pour l'envoi des **traps SNMP**. Si l'on veut superviser le routeur **Cisco** depuis la machine **192.168.1.47**, il faut taper cette ligne :

snmp-server host 192.168.1.47 private

et depuis toutes les machines du réseau 192.168.1.0/24 : snmp-server host 192.168.1.0 private

III.2. Supervision du routeur CISCO

Depuis la machine Linux **192.168.1.47**, on peut maintenant visualiser la **MIB** du routeur d'adresse **192.169.0.100** avec la commande :

snmpwalk -v1 -c private 192.169.0.100 ou **snmpwalk -v2c -c private 192.169.0.100**

Si on veut visualiser un **OID** particulier :

snmpwalk -v2c -c private 192.169.0.100 <OID>

Par exemple, pour récupérer la version de l'IOS Cisco du routeur, il faut lire l'OID .1.3.6.1.2.1.1.1.0 :

#snmpwalk -v2c -c private 192.169.0.100 .1.3.6.1.2.1.1.1.0

Couches Hautes - TP5-1 - Annexe 1 « Surveiller un équipement réseau avec SNMP »

iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C2600 Software (C2600-IPBASEK9-M), Version 12.4(15)T3, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Thu 24-Jan-08 14:23 by prod_rel_team"

Par exemple, pour obtenir " **l'uptime** ", le temps depuis lequel le système est en service, il faut lire l'**OID 1.3.6.1.2.1.1.3.0** :

#snmpwalk -v2c -c private 192.169.0.100 1.3.6.1.2.1.1.3.0
iso.3.6.1.2.1.1.3.0 = Timeticks: (372828) 1:02:08.28

Si on veut connaître l'utilisation du CPU en % :

| Cisco IOS Software releases later to 12.0(3)T and prior to 12.2(3.5) |
|--|
| CISCO-PROCESS-MIB |
| cpmCPUTotal5min (.1.3.6.1.4.1.9.9.109.1.1.1.1.5) |
| cpmCPUTotal1min (.1.3.6.1.4.1.9.9.109.1.1.1.1.4) |
| cpmCPUTotal5sec (.1.3.6.1.4.1.9.9.109.1.1.1.1.3) |

Si on veut connaître l'utilisation du CPU en % durant la dernière minute (cpmCPUTotal1min), il faut lire l'OID .1.3.6.1.4.1.9.9.109.1.1.1.1.4 :

snmpwalk -v2c -c private 192.169.0.100 .1.3.6.1.4.1.9.9.109.1.1.1.1.4 iso.3.6.1.4.1.9.9.109.1.1.1.1.4.1 = Gauge32: 2

On trouve 2 %, validé par la commande show processes CPU sur le routeur :

R1#show processes CPU

CPU utilization for five seconds: 4%/0%; one minute: 2%; five minutes: 1% PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 800 0.00% 0.00% 0.00% 0 Chunk Manager 5 1 4 2 3800 0.08% 0.08% 0.08% 0 Load Meter 7366 1938 2044 0.00% 0.01% 0.00% 0 IP SNMP 11744 0.00% 0.09% 0.11% 0 Check heaps 3 11439 5595 4 17770 1513 5 10000 0.00% 0.03% 0.00% 0 Pool Manager 80 8

Si on veut connaître la mémoire utilisée, il faut lire l'OID .1.3.6.1.4.1.9.9.48.1.1.1.5.1 :

snmpwalk -v2c -c private 192.169.0.100 .1.3.6.1.4.1.9.9.48.1.1.1.5.1 iso.3.6.1.4.1.9.9.48.1.1.1.5.1 = Gauge32: 9330992

Si on veut connaître la mémoire libre, il faut lire l'OID .1.3.6.1.4.1.9.9.48.1.1.1.6.1 :

snmpwalk -v2c -c private 192.169.0.100 .1.3.6.1.4.1.9.9.48.1.1.1.6.1 iso.3.6.1.4.1.9.9.48.1.1.1.6.1 = Gauge32: 60093156

Résultats validés par la commande show processes memory sur le routeur :

| R1#show processes memory | | | | | | | |
|---|--|---|--|---|---|---|------------------|
| Proc | ess | or Pool Tota | l: 694241 | 48 Used: | 9330 | 992 Free: | 60093156 |
| I | /O I | Pool Total: | 19922944 | Used: 2 | 01144 | 0 Free: 1 | 7911504 |
| PID | TT | Y Allocated | Freed | Holding | Getbu | ifs Retbut | fs Process |
| 0 | 0 | 22536036 | 11643568 | 3 917524 | 48 | 0 0 | *Init* |
| 0 | 0 | 12052 | 214396 | 12052 | 0 | 0 *Scł | ned* |
| 0 | 0 | 1613240 | 2008452 | 106804 | 170 | 064 170 | 064 *Dead* |
| 1 | 0 | 71384 | 0 78 | 8620 | 0 | 0 Chunk | Manager |
| 2 | 0 | 252 | 252 42 | 236 | 0 | 0 Load Me | eter |
| 3 | 0 | 639452 | 637060 | 14220 | 0 | 0 IP S | NMP |
| #sn iso. iso. iso. iso. iso. iso. | mp 3.6 3.6 3.6 3.6 3.6 3.6 3.6 3.6 | walk -v2c .1.4.1.9.9. .1.4.1.9.9. .1.4.1.9.9. .1.4.1.9.9. .1.4.1.9.9. .1.4.1.9.9. .1.4.1.9.9. .1.4.1.9.9. | -c private 48.1.1.1.2 48.1.1.1.3 48.1.1.1.3 48.1.1.1.4 48.1.1.1.4 48.1.1.1.5 48.1.1.1.5 | 192.169 .1 = STR .2 = STR .1 = INT .2 = INT .1 = INT .2 = INT .1 = Gau .2 = Gau | 0.0.10 (ING: " EGER: EGER: EGER: EGER: Ige32: Ige32: | 0 .1.3.6.1. Processor I/O" 0 1 1 9330992 2011440 | 4.1.9.9.48 ." |
| iso. | 3.6 | .1.4.1.9.9. | 48.1.1.1.6 | .1 = Gau | ige32: | 60093150 | 5 |
| iso. | 3.6 | .1.4.1.9.9. | 48.1.1.1.6 | .2 = Gau | ige32: | 17911504 | 1 |
| iso. | 3.6 | .1.4.1.9.9. | 48.1.1.1.7 | '.1 = Gau | ige32: | 53445030 | 5 |

IV - Surveiller une machine Linux avec SNMP

IV.1. Installation et configuration de l'agent SNMP sur une machine Linux

Si on veut surveiller une machine **Linux** via **snmp**, il faut installer les paquets **snmp** et **snmpd** puis il faut modifier la configuration **snmp** afin de voir l'ensemble de l'arbre **snmp** en modifiant le fichier **/etc/snmp/snmpd.conf** :

Il faut commenter les lignes : **#view systemonly included .1.3.6.1.2.1.1 #view systemonly included .1.3.6.1.2.1.25.1** puis rajouter cette ligne : **view systemonly included .1**

Il faut commenter la ligne : #agentAddress udp:127.0.0.1:161

Il faut décommenter la ligne : agentAddress udp:161,udp6:[::1]:161

puis il faut relancer **snmpd** : **#service snmpd restart**

IV.2. Supervision de la machine Linux

Pour obtenir " l'uptime ", le temps depuis lequel le système est en service, il faut lire l'OID : 1.3.6.1.2.1.1.3.0

iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.sysUpTimeInstance

#snmpwalk -v2c -c public 192.168.0.100 .1.3.6.1.2.1.1.3.0 iso.3.6.1.2.1.1.3.0 = Timeticks: (372828) 1:02:08.28 Par exemple, pour récupérer la version de l'**OS** du poste Linux, il faut lire l'**OID** .1.3.6.1.2.1.1.1.0 :

#snmpwalk -v2c -c public 192.168.0.100 .1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "Linux ubuntu-NJ50-70CU 5.8.0-48-generic
#54~20.04.1-Ubuntu SMP Sat Mar 20 13:40:25 UTC 2021 x86 64"

Voici la liste des principaux OID disponibles sur une machine Linux :

Network Interface Statistics :

List NIC names: .1.3.6.1.2.1.2.2.1.2 Get Bytes IN: .1.3.6.1.2.1.2.2.1.10 Get Bytes IN for NIC 4: .1.3.6.1.2.1.2.2.1.10.4 Get Bytes OUT: .1.3.6.1.2.1.2.2.1.16 Get Bytes OUT for NIC 4: .1.3.6.1.2.1.2.2.1.16.4

Load :

1 minute Load: .1.3.6.1.4.1.2021.10.1.3.1 5 minute Load: .1.3.6.1.4.1.2021.10.1.3.2 15 minute Load: .1.3.6.1.4.1.2021.10.1.3.3

CPU times :

percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0 raw user cpu time: .1.3.6.1.4.1.2021.11.50.0 percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0 raw system cpu time: .1.3.6.1.4.1.2021.11.52.0 percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0 raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0 raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

Memory Statistics :

Total Swap Size: .1.3.6.1.4.1.2021.4.3.0 Available Swap Space: .1.3.6.1.4.1.2021.4.4.0 Total RAM in machine: .1.3.6.1.4.1.2021.4.5.0 Total RAM used: .1.3.6.1.4.1.2021.4.6.0 Total RAM Free: .1.3.6.1.4.1.2021.4.11.0 Total RAM Shared: .1.3.6.1.4.1.2021.4.13.0 Total RAM Buffered: .1.3.6.1.4.1.2021.4.13.0 Total RAM Buffered: .1.3.6.1.4.1.2021.4.14.0

Disk Statistics :

Path where the disk is mounted: .1.3.6.1.4.1.2021.9.1.2.1 Path of the device for the partition: .1.3.6.1.4.1.2021.9.1.3.1 Total size of the disk/partion (kBytes): .1.3.6.1.4.1.2021.9.1.6.1 Available space on the disk: .1.3.6.1.4.1.2021.9.1.7.1 Used space on the disk: .1.3.6.1.4.1.2021.9.1.8.1 Percentage of space used on disk: .1.3.6.1.4.1.2021.9.1.9.1 Percentage of inodes used on disk: .1.3.6.1.4.1.2021.9.1.10.1

V - Surveiller une machine Windows avec SNMP

V.1. Installation et configuration de l'agent SNMP sur une machine Windows

<u>Remarque</u>: Une fois l'**agent SNMP** installé, on trouve le descriptif de la **MIB** dans les fichiers portant l'extension **mib** du dossier **C:\Windows\System32**. Par exemple le fichier **hostmib.mib**.

Pour installer l'agent SNMP sous Windows 7, il faut depuis le menu Panneau de configuration / Programmes / Activer ou désactiver les fonctionnalités Windows cocher Protocole SNMP et Fournisseur SNMP WMI :

| 🚱 🗢 🧱 🕨 Panneau de confi | guration > Programmes > v 49 | 🛐 Fonctionnalités de Windows |
|---|---|---|
| Page d'accueil du panneau de configuration Système et sécurité Réseau et Internet Matériel et audio • Programmes Comptes et protection des utilisateurs | Programmes et fonctionnalités Désinstaller un programme Affricher les mises à jour installées Exécuter des programmes conçus pour des versions précédentes de Windows Comment installer un programme Programmes par défaut Modifier les paramètres par défaut Toujours ouvrir un type de fichier particulier avec un programme spécifique Choisrie les programmes par défaut | Activer ou désactiver des fonctionnalités Windows Pour activer une fonctionnalité, activez la case à cocher correspondante. Pour désactiver une fonctionnalité, désactivez la case à cocher correspondante. Une case à cocher pleine signifie qu'une partie de la fonctionnalité est activée. |
| Apparence et personnalisation Horloge, langue et région Options d'ergonomie | Gadgets du Bureau Ajouter des gadgets au Bureau Trouver d'autres gadgets en ligne Désinstaller un gadget Restaurer les gadgets du Bureau installés avec Windows | Service d'indexation Service d'activation des processus Windows Services d'impression et de numérisation de document OK |

Pour configurer l'agent SNMP, il faut ouvrir la fenêtre de propriétés du service SNMP depuis le menu Panneau de configuration / Système et sécurité / Outil d'administration / Services / Service SNMP. Dans l'onglet Agent, les variables SNMP de la Mib2 system peuvent être définies :

| Interruptions | Sécurité | Dép | pendances | | | Interruption | ns | Sécu | ité | Dép | endances |
|--|---|---|----------------|---|--|--|--|--|------------------------|--|-----------|
| Général 😡 Conne | xion Récu | pération | Agent | | | Général | Connex | tion | Récu | pération | Age |
| om du service : SHME om complet : Service escription : Permet Manage nemin d'accès des fichier Windows System 32 an upe de démarrage : Au btenir de l'aide pour confr at du service : Démard Démarre An | SNMP www.requêtes SNMP (' ment Protocol) d'être p exécutables : p exé tomatique aurer les options de dé | imple Netw tratées par o imarrage de dre | ork * cet * | | | Les systèmes de d'indiquer la per réseau pour cet Contact : Emplacement : Service V Physique V Internet | e gestion d'In sonne conta ordinateur. | temet peu ct, l'emplace ations I | vent dema sement du | inder au serv système et le e données et | sous-rése |
| ous pouvez spécifier les p arvice. aramètres de démarrage : | aramètres qui s'appliq | uent au dém | narrage du |] | | En savoir plu | is sur le proto | cole <u>SNM</u> | 2 | | |

Dans l'onglet Sécurité, il faut au moins déclarer l'adresse du manager et la communauté :

| Général Con Interruptions | | ion | Récup | ération | Age |
|--|--|------------|------------------------------|---|---------|
| | | Sécu | rité | Dépendance | |
| Envoyer une Noms de com | interruption munautés ac | d'authenti | fication | | |
| Communaut | té | NS | Droits | | |
| private | | | LECTI | URE SE | |
| _ | | | | ooppiinter | |
| Accepter Accepter localhost | les paquets les paquets | SNMP pro | ovenant de ovenant de | n'importe qui ces hôtes | el hôte |
| Accepter Accepter localhost 192.168.4 | les paquets les paquets 0.1 | SNMP pro | ovenant de ovenant de o | n'importe que | el hôte |
| Accepter Accepter Iocalhost 192.168.4 Ajo | les paquets les paquets 0.1 | SNMP pro | ovenant de r ovenant de r | n'importe qui ces hôtes - Supprimer | el hôte |
| Accepter Accepter Iocalhost 192,168,4 Ajo savoir plus s | les paquets les paquets 0.1 puter | SNMP pro | ier | n'importe que ces hôtes | el hôte |
| Accepter Accepter Accepter Iocalhost 192.168.4 Ajo savoir plus s | les paquets les paquets 0.1 puter | SNMP pro | ier | n'importe que ces hôtes | el hôte |

V.2. Supervision de la machine Windows

Pour obtenir " l'uptime ", il faut lire l'OID : 1.3.6.1.2.1.1.3.0 #snmpwalk -v2c -c private 192.168.40.3 .1.3.6.1.2.1.1.3.0 iso.3.6.1.2.1.1.3.0 = Timeticks: (372828) 1:02:08.28

Pour obtenir " hrSystemDate.0 " la date système, il faut lire l'OID : 1.3.6.1.2.1.25.1.2.0 #snmpwalk -v2c -c private 192.168.40.3 1.3.6.1.2.1.25.1.2.0 iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07:E5:04:05:11:2B:17:09

| Octets 1 et 2 | =>Année = 0x07E5 = | 2021 |
|---------------|---------------------|-----------|
| Octet 3 | =>Mois = 0x04 = | 4 (Avril) |
| Octet 4 | =>Jour = 0x05 = | 5 |
| Octet 5 | =>heures = 0x11 = | 17 |
| Octet 6 | =>Minutes = 0x2B = | 43 |
| Octet 7 | =>Secondes = 0x17 = | 23 |
| Octet 8 | =>Dixièmes = 0x09 = | 9 |
| | | |