SUPERVISION RÉSEAU

JOSHUA CNUDDE

SOMMAIRE

I. Brainstorming
II. Les protocole de supervision réseau
III. Introduction
IV. SNMP
V. SYSLOG

I. BRAINSTORMING

- Pourquoi les entreprises souhaitent superviser leurs réseaux ?
- Quelle/s protocole/s de supervision réseau connaissez-vous ?
- Quel/s logicielle/s de supervision réseau connaissez-vous ?

II. LES PROTOCOLES DE SUPERVISION RÉSEAU

- SNMP : SIMPLE NETWORK MANAGEMENT PROTOCOLE
- SYSLOG
- NETFLOW/SFLOW

III . SNMP : INTRODUCTION

- Besoin d'administrer les réseaux (entretien et surveillance).
- Détecter les pannes qui pourraient arriver.
- Normalisation de deux protocoles pour l'administration du réseau: SNMP et CMOT/CMIP (Common Management Information Protocol)
- Normalisé par l'IETF (« Internet Engineering Task Force ») en 1988 pour les réseaux s'appuyant sur TCP/IP.
- Devenu un standard pour l'administration des réseaux.
- Il est actuellement à la version 3.
- Objectif : communiquer, échanger des données et gérer les équipements de façon automatique et transparente.

IV. SNMP : PRÉSENTATION GÉNÉRALE

- SNMP => Créé en 1988.
  => Simple Network Management Protocol
  => Apporte des moyens simples pour superviser
- SNMP est un protocole de la couche application.
- Il utilise le concept d'application Client / Serveur :
  - Serveur => station d'administration.
  - Client => machine ou service ayant un agent de supervision.
- Avantages :
  - Simple : mise en place rapide et peu chère.
  - Stable : repose sur le principe du paradigme « aller chercher – enregistrer ».
  - Souple : on installe uniquement les commandes qui seront adaptées au réseau.
  - Performant : rapide et de petite taille.
  - Disponible : répandu sur le marché (incontournable pour les constructeurs)

IV. SNMP : 3 VERSIONS

SNMPv1

Voici les points négatifs de la version 1:

- Manque de sécurité (communauté circule en clair sur le réseau).
- Protocole inefficace (pas de transfert de masse).
- Pas de limitations sélectives d'accès à la MIB de l'agent.

Voici les points positifs de la version 1: • Standard accepté par l'ensemble des constructeurs. • Grand choix de logiciels pour la supervision

SNMPv2 (1993)

Voici les apports pour la version 2:

- Une Entité SNMP peut être à la fois agent et manager
- Primitive Inform : dialogue de manager à manager
- Primitive GetBulk : permet à une plate forme de gestion, de demander en bloc plusieurs variables consécutives dans la MIB de l'agent.
- Mécanismes de sécurité : confidentialité des messages par cryptographie en DES • Support multi-protocoles : UDP, OSI

IV. SNMP : 3 VERSIONS

SNMPv3 (1999)
Voici les apports pour la version 3 :
Le renforcement de la sécurité est basé sur:

- L'authentification : Elle a pour but de garantir l'authenticité de l'émetteur et du récepteur. L'authentification utilise MD5 ou SHA afin de crypter les données d'authentification.
- Le chiffrement : Il est réalisé à l'aide de l'algorithme DES (Data Encryption Standard). Cela empêche quiconque de lire les informations contenues dans un paquet SNMPv3 (totalement illisible).
- L'estampillage du temps : Empêche la réutilisation d'un paquet SNMPv3 valide déjà transmis par quelqu'un. Chaque paquet est estampillé avec une date. A la réception du paquet, on compare le temps avec celui du paquet et si la différence est supérieure à 150 secondes le paquet n'est pas traité.

IV. SNMP - COMMUNAUTÉS

- Elle réunit la machine de gestion ainsi que les équipements administrés. ■
- Une communauté SNMP se définit comme une relation entre un agent SNMP et un ensemble de stations d'administration => Authentification => Contrôle d'accès
  Authentification : La station de gestion envoie avec le message un mot de passe correspondant à la communauté, cela permet au récepteur de vérifier l'authenticité.
  Politique d'accès: Organisation des MIB par « communautés », on met la communauté « public » pour les équipements accessibles par toutes les stations de gestion et on met en « private » pour restreindre l'accès à certaines.

IV. SNMP : 3 VERSIONS

SNMP SECURITY MODEL PER LEVEL

Version	Level	Authentication	Encryption	Process
V1	noAuthNoPriv	Community String	No	Uses a community string match for authentication
V2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication
V3	noAuthNoPriv	Username	No	Uses a username match for authentication
V3	authNoPriv	MD5 or SHA	No	Authenticates based on HMAC-MD5 or HMAC-SHA
V3	authPriv	MD5 or SHA	DES	Same as previous plus 56-bit DES encryption

Based on Chart from http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

IV. SNMP : 3 VERSIONS

Feature	SNMPv1	SNMPv2c	SNMPv3
Get	Yes	Yes	Yes
GetNext	Yes	Yes	Yes
Set	Yes	Yes	Yes
GetBulk	No	Yes	Yes
Trap	Yes	Yes	Yes
Inform	No	Yes	Yes
Community strings	Yes	Yes	No
User based secuirty	No	No	Yes
Message authentication	No	No	Yes
Message encryption	No	No	Yes

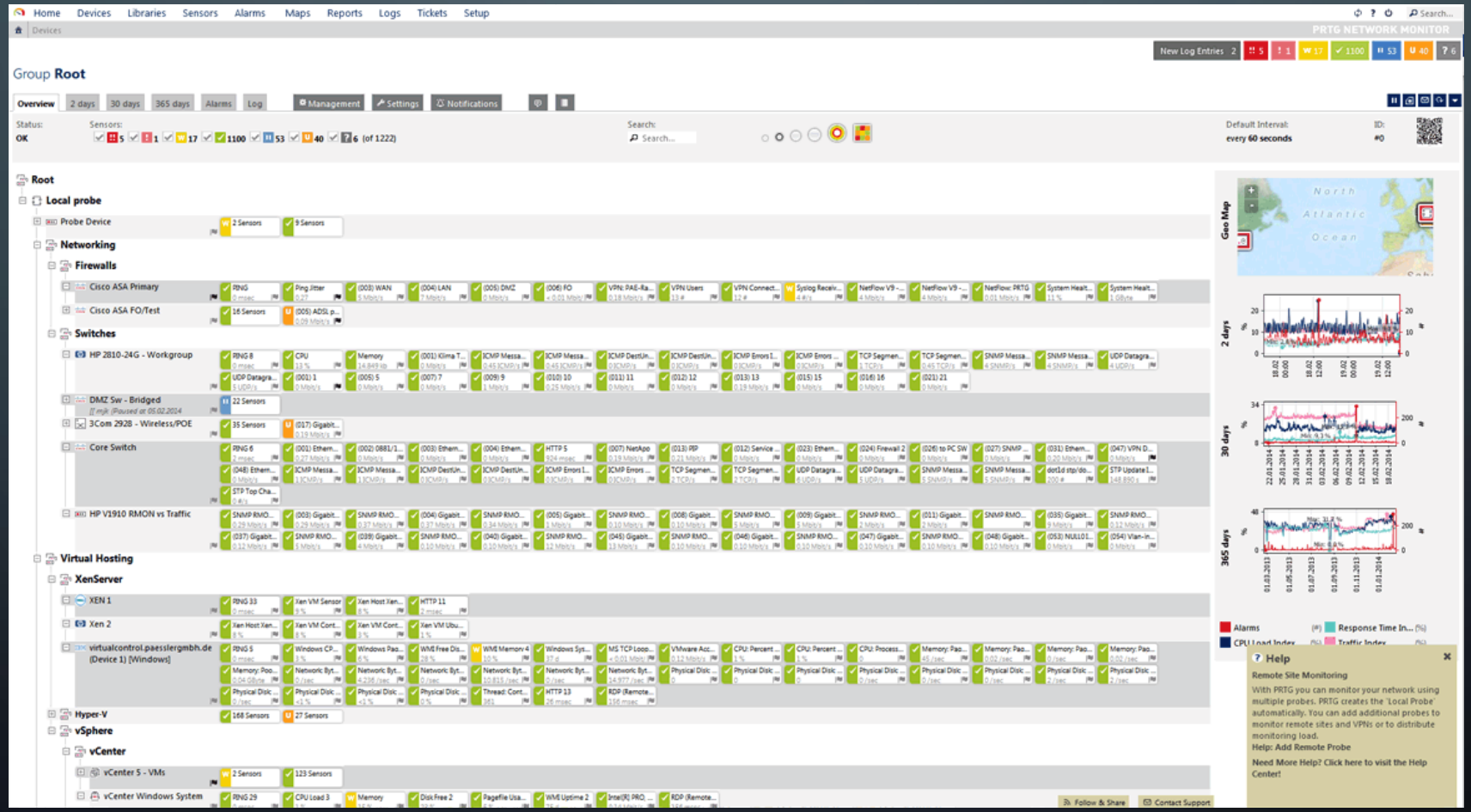
IV. SNMP : LES LOGICIELS

Les plus utilisées :

- PRTG
- ICINGA 2
- ZABBIX
- Observium/LibreNMS

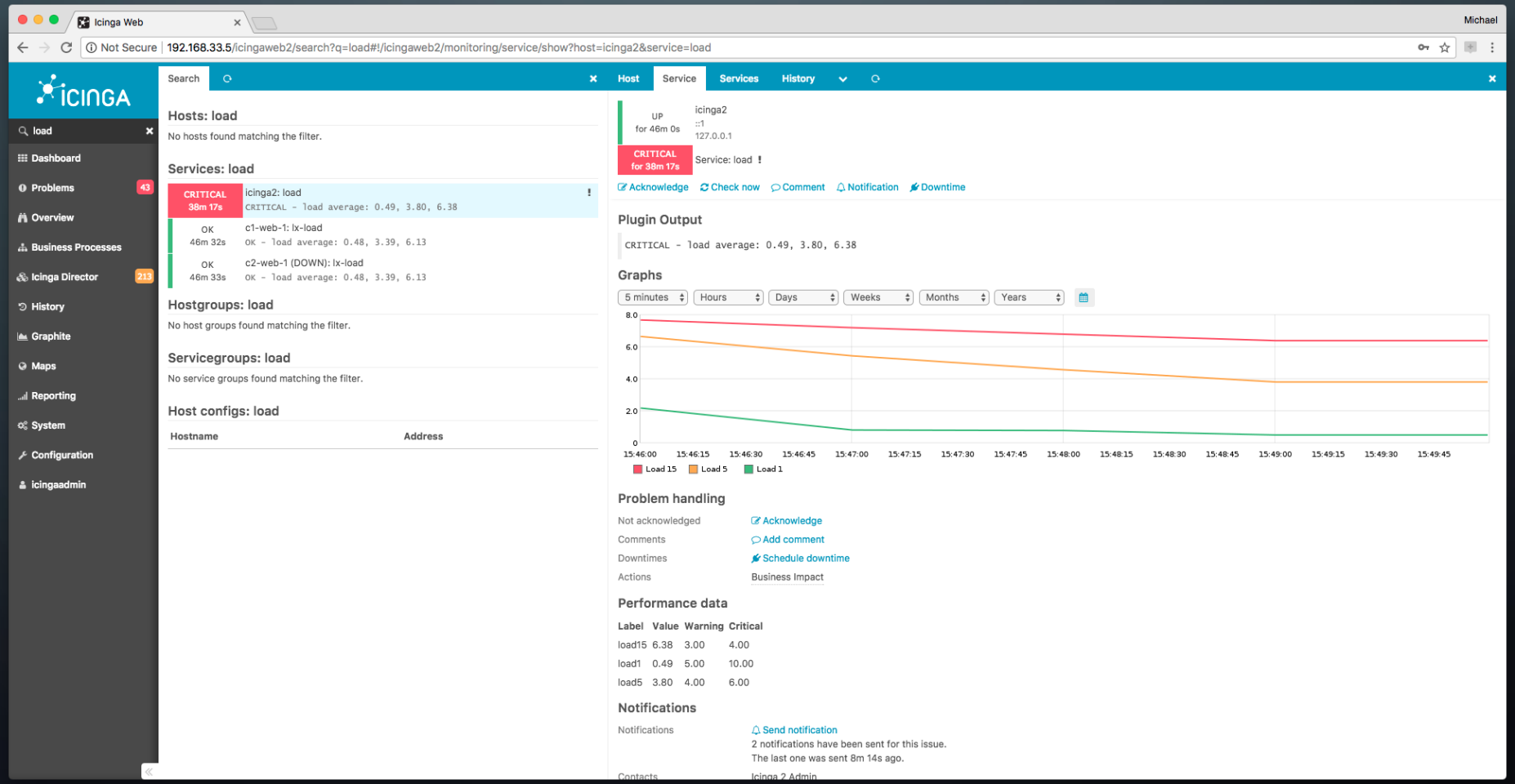
IV. SNMP : LES LOGICIELS

- PRTG :



IV. SNMP : LES LOGICIELS

- ICINGA 2 :



IV. SNMP : LES LOGICIELS

- ZABBIX:

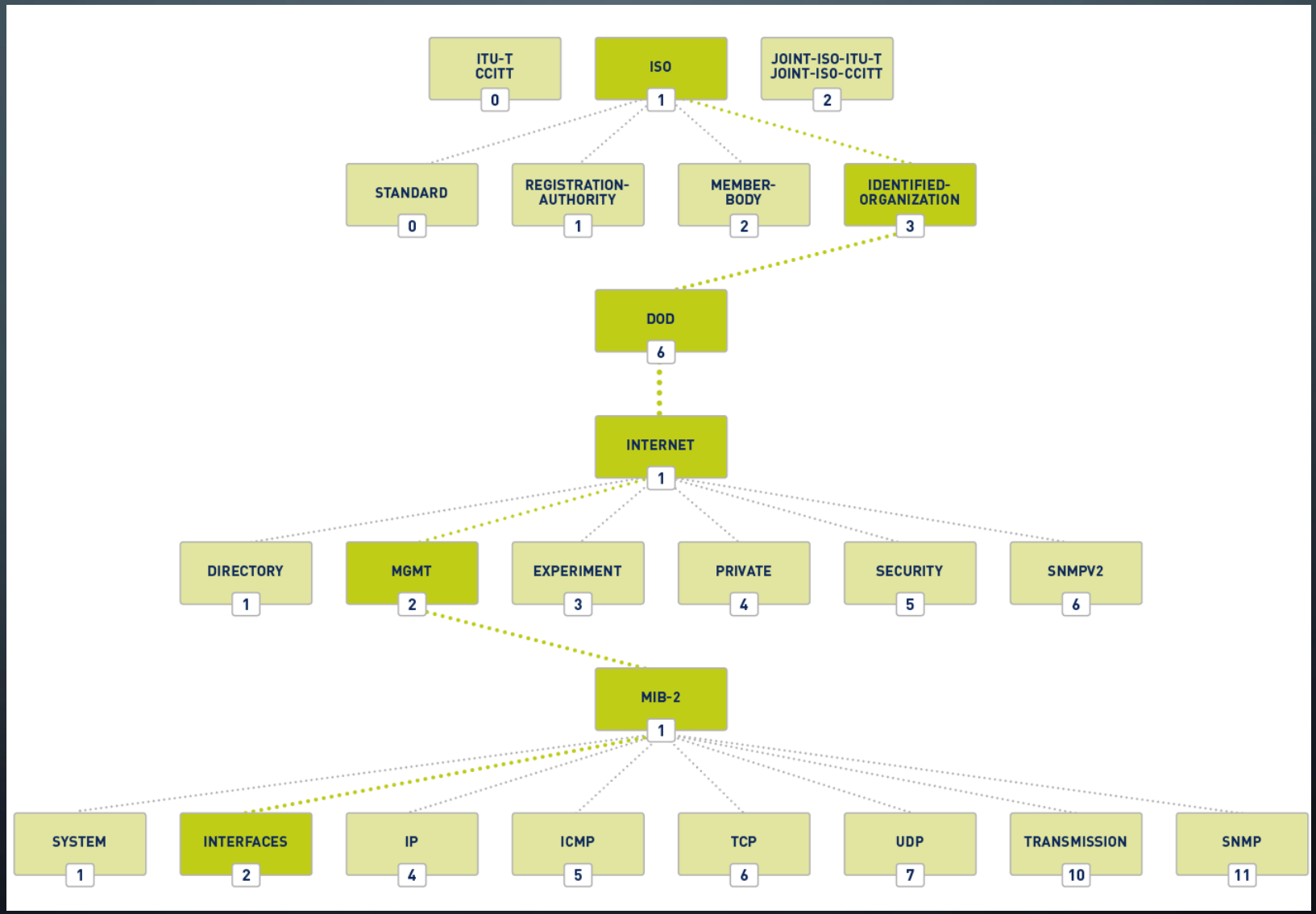
IV. SNMP : LES LOGICIELS

- OBSERVIUM :

IV. SNMP : MIB

- La MIB est une base de données gérée par un agent SNMP regroupant les objets gérés en respectant les règles SMI (Structure of Management Information). La SMI est la définition de la structure de la MIB, cela montre comment elles sont connectées ensemble pour former un arbre. Elle possède une structure d'arbre similaire à celui employé dans le DNS (Domain Name System). On retrouve une racine non nommée à partir de laquelle on référence de façon absolue un objet par son OID (nœud de l'arbre).

IV. SNMP : MIB


ITU-T
CCITT
0
ISO
1
JOINT-ISO-ITU-T
JOINT-ISO-CCITT
2
STANDARD
0
REGISTRATION-
AUTHORITY
1
MEMBER-
BODY
2
IDENTIFIED-
ORGANIZATION
3
DOD
6
INTERNET
1
DIRECTORY
1
MGMT
2
EXPERIMENT
3
PRIVATE
4
SECURITY
5
SNMPV2
6
MIB-2
1
SYSTEM
1
INTERFACES
2
IP
4
ICMP
5
TCP
6
UDP
7
TRANSMISSION
10
SNMP
11

IV. SNMP : MIB

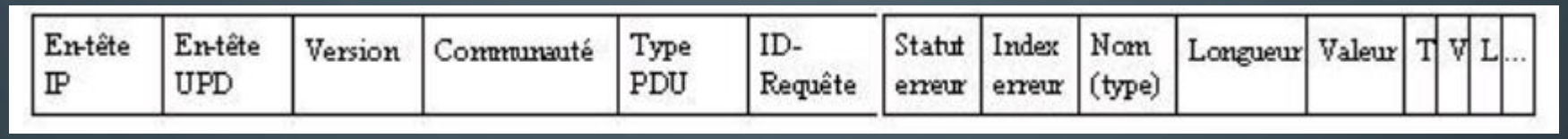
- Les variables des MIB sont classées en groupes
- Voici les MIB les plus utilisées :
  - System ➔ MIB descriptive de l'environnement.
  - Interfaces ➔ Attachements réseaux (MTU, Speed, Status…).
  - Dot1dbridge ➔ Equipements de routage (port STP, port forwarding, routage…).
  - Host ➔ pour voir les OS (Disque dur, RAM…).

IV. SNMP : MIB

- SNMP – MIB Où trouver les MIB correspondantes aux équipements ?
- Sites spécialisés :
  - http://www.plixer.com
  - http://www.oidview.com/
- Demande aux constructeurs. Logiciel freeware : Getif (compatible SNMPv1 seulement), SNMPUtil (ligne de commande), SNMP tester (GUI pour SNMPUtil), MIB Browser de iReasoning

IV. SNMP : STRUCTURE

- SNMPv1/2c



- **Version**: Le manager et l'agent doivent envoyer la même version.
- **Communauté**: Sert d'identification => mot de passe de validation d'une requête SNMP par l'agent.
- **Type PDU:** 0 => GetRequest 1 => GetNextRequest 2 => GetResponse 3 => SetRequest .
- **ID de requête :** Champ servant à coordonner la requête du manager et la réponse de l'agent.
- **Index d'erreur :** Identifie les entrées avec la liste des variables qui ont causé l'erreur.
- **Obj/Val** : Association du nom de la variable à transmettre avec sa valeur.

IV. SNMP : STRUCTURE

- Qu'est ce qu'un Trap ?
  - Une alerte est envoyée quand un événement non attendu se produit sur l'agent. L'agent informe la station de supervision de ce problème via un Trap.

  - Quelques événements peuvent êtres configurés pour signaler un Trap, comme un défaut de câble réseau, un disque dur défaillant, un problème d'alimentation…

IV. SNMP : STRUCTURE

- Qu'est ce qu'un Trap ?
  - Une alerte est envoyée quand un événement non attendu se produit sur l'agent. L'agent informe la station de supervision de ce problème via un Trap.

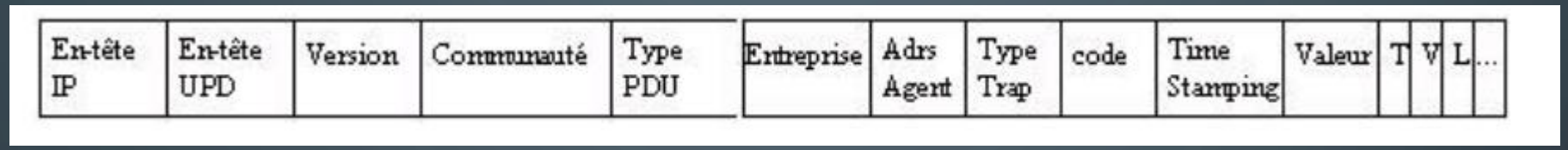
  - Quelques événements peuvent êtres configurés pour signaler un Trap, comme un défaut de câble réseau, un disque dur défaillant, un problème d'alimentation…

IV. SNMP : STRUCTURE

- Exemple de Trap SNMP :
  - Link Down, Link Up : lorsqu'un accès réseau cesse ou commence à fonctionner
  - Cold, Warm : selon le type de réinitialisation
  - Authentification : lorsqu'un agent SNMP reçoit une requête dont le nom de communauté ne correspond pas au sien
  - Loss of BGP: lorsqu'un agent SNMP ne peut plus communiquer avec son voisinage BGP (no BGP neighbor)

IV. SNMP : STRUCTURE

- Format de Trap snmp



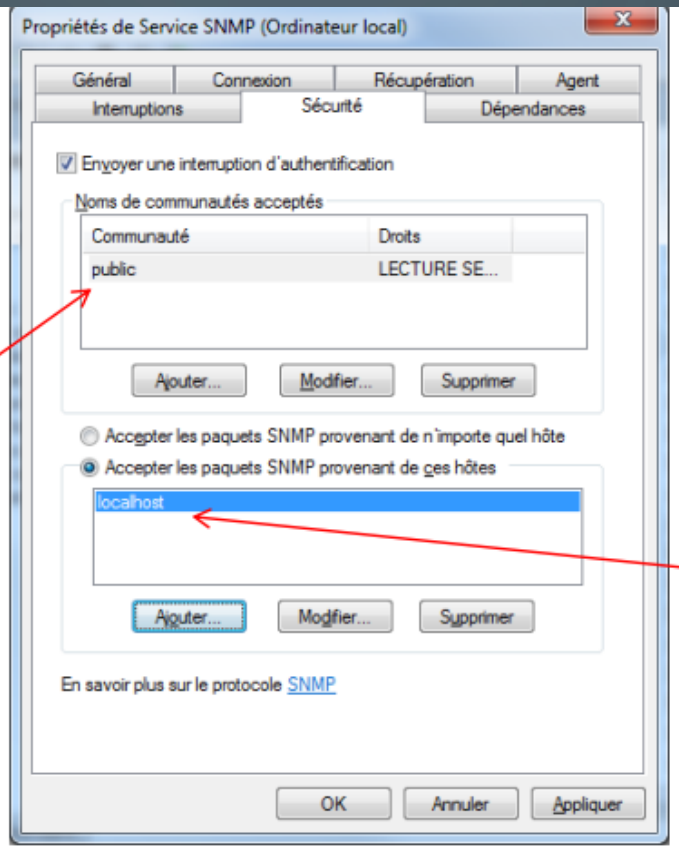
- **Communauté:** Sert d'identification.
- **Type PDU:** 4 => Trap
- **Entreprise :** Identifie l'entreprise de management qui a défini la Trap.
- **Adresse Agent:** Adresse IP de l'agent.
- **Type Générique:** Décrit quel type de problème est survenu. (7 valeurs sont possibles).
- **Type Spécifique:** Est utilisé afin d'identifier une TRAP spécifique à une entreprise.
- **Timestamp:** Contient la valeur de l'objet sysUptime représentant le temps écoulé depuis la dernière initialisation.
- **Obj/Val :** Association du nom de la variable à transmettre avec sa valeur.

IV. SNMP : MISE EN PLACE

- Mise en place du service SNMP sous Windows :

⇒ **Service SNMP**

⇒ **« Sécurité »**



Nom de la communauté

Adresse IP de la machine de gestion

IV. SNMP : MISE EN PLACE

- Mise en place du service SNMP sous Linux:
- => exemple pour la communauté « test » :

```
debian:~# apt-get install snmpd
```
→ Installation des paquets

```
debian:/# nano /etc/snmp/snmpd.conf
```
→ Edition du fichier de configuration

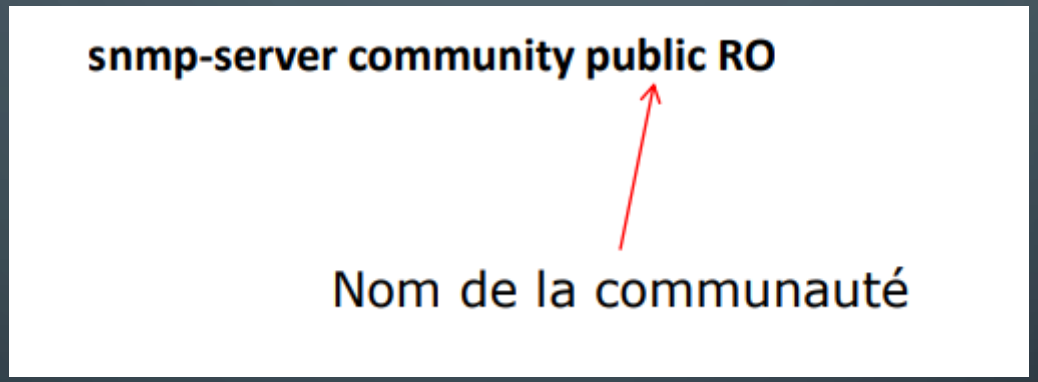
```
#          sec.name  source          community
com2sec paranoid  default         public
#com2sec readonly  default          public
#com2sec readwrite default         private
```
→ Fichier de base

```
#          sec.name  source          community
#com2sec paranoid  default          public
com2sec readonly  default         test
#com2sec readwrite default         private
```
→ Pour notre exemple

```
debian:/# /etc/init.d/snmpd restart
Restarting network management services: snmpd.
```
→ Redémarrage du service

IV. SNMP : MISE EN PLACE

- Mise en place du service SNMP sous CISCO:
- => exemple pour la communauté « public » :



- Activer les traps SNMP sur un équipement Cisco:

Activation =>	**snmp-server enable traps** « type de traps »
Export =>	**snmp-server host** « IP » **version** « *1,2c ou 3* » « *communauté* »

IV. SNMP : COMMANDES UTILES

- SNMPGET et SNMPTRANSLATE

- **SNMPGET** => permet d'obtenir une information sur un objet de la MIB d'un agent SNMP distant .

Exemple:

```
debian:/etc/snmp# snmpget -v 1 -c test localhost .1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (284989) 0:47:29.89
```

- **SNMPTRANSLATE** => permet de convertir un objet d'une MIB représenté sous sa forme décimale OID en sa forme symbolique

```
debian:/etc/snmp# snmptranslate .1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance
```

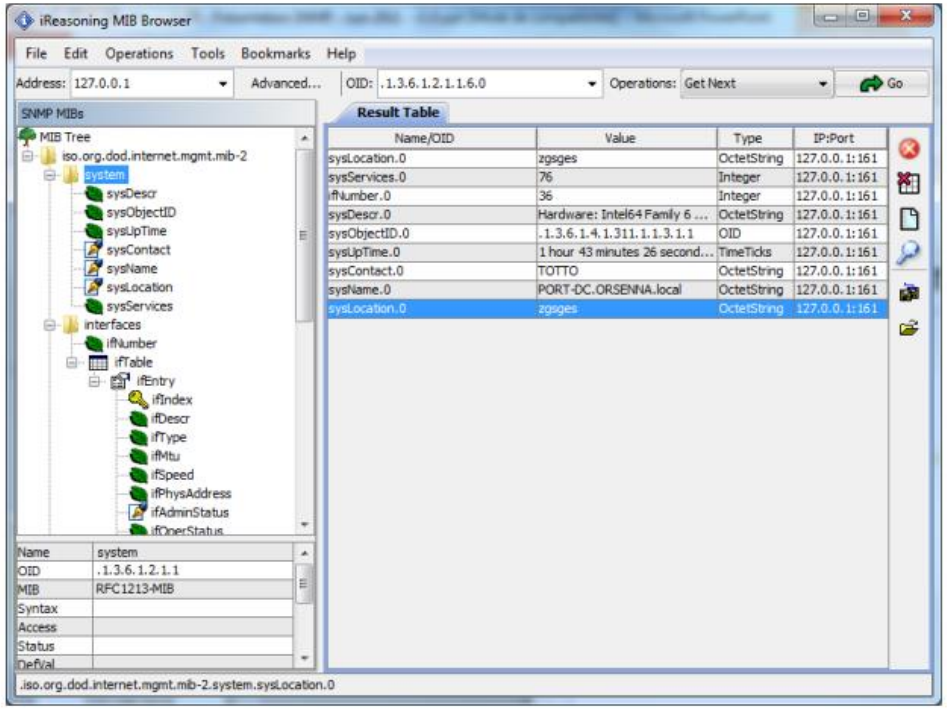
```
debian:/etc/snmp# snmptranslate -Tp -IR
```
→ Affichage de l'arbre complet (1)

```
debian:/etc/snmp# snmptranslate -Tp -IR system
```
→ Affichage de l'arbre à partir de la branche system (2)

IV. SNMP : COMMANDES UTILES

- **Windows**

MIB Browser Gratuit:



DOWNLOAD:
http://www.ireasoning.com/downloadmibbrowserfree.php

IV. SYSLOG: PRÉSENTATION

- Protocole simple utilisé dans le monde de Linux.
- Il permet de centraliser les journaux d'évènements.
- Il permet aussi de transporter les messages de journalisation générés vers un serveur Syslog.
- Il décharge les programmeurs de la gestion des journaux.
- Il permet à l'administrateur de contrôler l'ensemble des journaux avec un fichier unique.
- Il permet de gérer les entrées de journaux en fonction de leur type et de leur niveau d'urgence.
- De base sous Linux, les log sont situés dans /var/log

V. SYSLOG: PRÉSENTATION

- Il se compose d'une partie cliente (émet les informations) et d'une partie serveur (collecte les informations et créer les journaux).
- Le transfert utilise le port 514 en UDP.
- Syslogd est un deamon chargé de gérer les journaux d'une machine.
- Syslog est couramment utilisé pour centraliser tous les journaux d'un parc informatique. • Il existe un Syslog pour Windows => ntsylog.
- On peut gérer les journaux d'hôtes distants => utilisation de la commande –r de syslogd

V. SYSLOG - FORMAT

- Un journal comporte dans l'ordre les informations suivantes :
  - La date à laquelle a été émis le log.
  - Le nom de l'équipement ayant généré le log.
  - Une information sur le processus qui a déclenché cette émission.
  - Le niveau de gravité.
  - Un identifiant du processus.
  - Un corps de message.

Certaines des informations sont optionnelles – Exemple :

```
Mar 23 11:39:58 debian nrpe[3443]: Connection from 192.168.3.101 port 53000
```

V. SYSLOG - FORMAT

- Voici les différents types de fonctionnalités :

Identifiant	Origine	Identifiant	Origine
0	kernel messages	1	user-level messages
2	mail system	3	system daemons
4	security/authorization messages (note 1)	5	messages generated internally by syslogd
6	line printer subsystem	7	network news subsystem
8	UUCP subsystem	9	clock daemon (note 2)
10	security/authorization messages (note 1)	11	FTP daemon
12	NTP subsystem	13	log audit (note 1)
14	log alert (note 1)	15	clock daemon (note 2)
16	local use 0 (local0)	17	local use 1 (local1)
18	local use 2 (local2)	19	local use 3 (local3)
20	local use 4 (local4)	21	local use 5 (local5)
22	local use 6 (local6)	23	local use 7 (local7)

Auth => Sécurité relatifs à la sécurité du système d'authentification.
Kern => Message générés par le noyau (envoyé par klogd).
Local => Services définis localement par l'administrateur
Ipr => Impression
Mail => Message provenant du système de mail.
User => Message en provenance des utilisateurs.

V. SYSLOG - FORMAT

- Voici les différents niveaux de gravité:
  - 0 Emerg (emergency) => Système inutilisable
  - 1 Alert => Une intervention immédiate est nécessaire
  - 2 Crit (critical) => Erreur critique pour le système
  - 3 Err (error) => Erreur de fonctionnement
  - 4 Warning => Avertissement
  - 5 Notice => Événement normal méritant d'être signalé
  - 6 Info (informational) => pour information seulement
  - 7 Debug => Message de mise au point
  - 8 none => Ignorer ce message

V. SYSLOG - FORMAT

- Voici les différents niveaux de gravité:
  - 0 Emerg (emergency) => Système inutilisable
  - 1 Alert => Une intervention immédiate est nécessaire
  - 2 Crit (critical) => Erreur critique pour le système
  - 3 Err (error) => Erreur de fonctionnement
  - 4 Warning => Avertissement
  - 5 Notice => Événement normal méritant d'être signalé
  - 6 Info (informational) => pour information seulement
  - 7 Debug => Message de mise au point
  - 8 none => Ignorer ce message

V. SYSLOG - FORMAT

- Comment connaitre la priorité ?
- Elle est définie par sa fonctionnalité ainsi que par sa gravité
- Il faut multiplié par 8 la fonctionnalité et y ajouter la gravité.
  - Exemple : local5 avec un warning

(21 * 8) + 4 = 172

Une priorité importante ne sera pas traité ou acheminé plus rapidement qu'un message de moindre priorité.

V. SYSLOG – SECURITÉ

- Syslog est-il sécurisé ?
  - Pas d'authentification .
  - Pas de chiffrement des informations.
  - Facile à abuser, à inonder avec de fausses alertes…
  - Les informations circulent en clair sur le réseau (risque de sniffer).
  - Risque de spoofing (envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet).
  - Utilise le mode UDP => ne garantie pas que le paquet arrive à destination.

V. SYSLOG – GESTION DES JOURNAUX

- Les journaux sont des fichiers dans lesquels l'information s'accumule. Ils peuvent devenir très gros et totalement inexploitables, il faut donc les gérer.
- Nous avons donc 2 contraintes pour cette gestion des journaux :
  - Taille: supprimer les informations quand la taille devient trop importante.
  - Durée: Ne garder les informations qu'un temps minimal pour permettre de les analyser.
- Possibilité d'utiliser une politique s'appuyant sur des rotations à intervalles régulier avec une conservation des fichiers un temps donné.
- Il faut aussi créer une alerte si d'un seul coup les fichiers syslog augmentent => problème ou attaque…
- Actuellement des outils comme logrotate ou newsyslog permettre de gérer la rotation des journaux

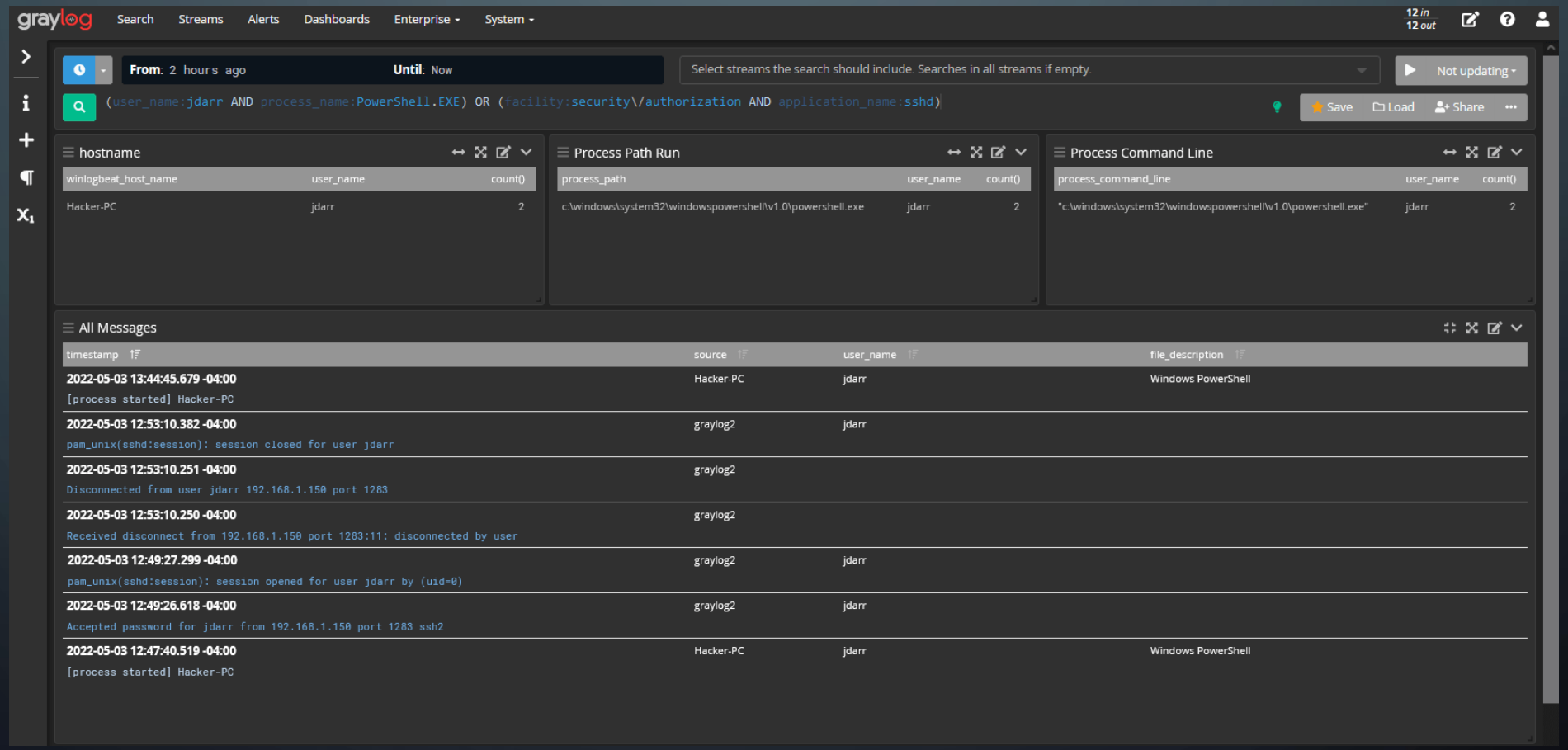
V. SYSLOG – GESTION DES JOURNAUX

- Les journaux sont des fichiers dans lesquels l'information s'accumule. Ils peuvent devenir très gros et totalement inexploitables, il faut donc les gérer.
- Nous avons donc 2 contraintes pour cette gestion des journaux :
  - Taille: supprimer les informations quand la taille devient trop importante.
  - Durée: Ne garder les informations qu'un temps minimal pour permettre de les analyser.
- Possibilité d'utiliser une politique s'appuyant sur des rotations à intervalles régulier avec une conservation des fichiers un temps donné.
- Il faut aussi créer une alerte si d'un seul coup les fichiers syslog augmentent => problème ou attaque…
- Actuellement des outils comme logrotate ou newsyslog permettre de gérer la rotation des journaux

V. SYSLOG – GESTION DES JOURNAUX

- Les journaux sont des fichiers dans lesquels l'information s'accumule. Ils peuvent devenir très gros et totalement inexploitables, il faut donc les gérer.
- Nous avons donc 2 contraintes pour cette gestion des journaux :
  - Taille: supprimer les informations quand la taille devient trop importante.
  - Durée: Ne garder les informations qu'un temps minimal pour permettre de les analyser.
- Possibilité d'utiliser une politique s'appuyant sur des rotations à intervalles régulier avec une conservation des fichiers un temps donné.
- Il faut aussi créer une alerte si d'un seul coup les fichiers syslog augmentent => problème ou attaque…
- Actuellement des outils comme logrotate ou newsyslog permettre de gérer la rotation des journaux

V. SYSLOG – LOGICIELS



V. SYSLOG – LOGICIELS