General info

Syslog et Netflow sont des outils utiles pour l'admin réseau qui lui permettent de gérer, d'afficher une collection d'événements associés à des dispositifs réseau.

Syslog

Est un outil rudimentaire pour collecter et afficher les messages qui apparaissent sur la console d'un routeur ou d'un switch.

Netflow

Permet de collecter des données opérationnelles de réseaux IP.
Loguer qui utilise les ressources et pour quoi.
Facturation en contion de l'utilisation.
Allocation des ressoureces de manière plus efficaces.
Dispose d'options sophistiquées d'analyse pour le flot de données.
Données récoltées:

- Ip src/dst
- port src/dst
- type proto niv.3
- type service
- interface d'entée logique

SNMP

port : 161, 162 (UDP)
niveau d'activité:

- inactif,(aucun monitoring, ignore alarmes)
- reactif,(aucun monitoring, réagit en cas de problème)
- interactif,(monitoring, dépannage interactif)
- proactif,(monitoring,process de restauration automatique)

communautés: **read-only** (lecture, consultation), **read-write** (modification, activer/desactiver, changer des configs), **TRAP** (alertes des clients)

- MIB (SMIv1)

- **Nom:** OID, définit de manière unique un objet
- **Type et syntaxe:** représentation des données échangées entre le manager et le client. indépendant des machines.
- **codage:** une instance d'un objet est codé dans une chaine d'octets avec BER.

- IANA : gère les nom des individus entreprises -> IOD numbers

opérations SNMP

- **get**
- getnext
  part de root et avance à l'objet suivant de l'arbre (par la droite)
- getbulk (SNMPv2,SNMPv3)
- **set**
- getresponse
- **trap**
  msg d'un agent -> manager(pad de ACK)
  exemple: interface desctivé/réactivé, ventilation en panne, ...
- notification (SNMPv2,SNMPv3)
- inform (SNMPv2,SNMPv3)
- report (SNMPv2,SNMPv3)

- SNMPv3

version originale défaut: sécu -> unique protection: un mot de passe (community)
Amélioration de v3, la sécu
Abandon de la notion d'agents et de managers -> entités SNMP.
-SNMPv3 engin: Dispatcher, processing des messages, **Securité(DES->3DES->AES), authentifiaction(MD5, SHA)**

- ***snmpwalk*** **/** ***snmpget***: walk permet de recevoir plusieurs valeurs de la MIB.

- NET-SNMP

outil gratuit
commandes -> type : snmpset / snmpget / snmpwalk

niveaux d'alertes

pooling interne: vérif de l'état en interne
pooling externe: utilise de la bande passante, préférer le pooling interne

Trapes

Notification envoyée par un agent SNMP à une station de management en utilisant UDP.
Manière pour un agent d'envoyer des notifications de manière asynchrone sur les conditions de réseau.
Les trapes qu'un agent peut générer sont définies dans la MIB.
Configuration du NMS en réponse aux différentes trapes (ignorer, script)
port UDP 162
Définis de 0 à 6 (coldStart(0): reboot,warmstart(1) variables are not reset, linkUp(3)/linkDown(2): chg interface state,authenticationFailure(4), egpNeighborLoss(5): neibor gone down, enterprisepecifig(6): trape générique)

Log Management

types de message: Info / Debug / Erreur / Alertes
utilité des logs: gestion / détection / troubleshooting / investigation / audit
process des logs :

1. Raw Log Data
2. Filter
   prlème, car pas de standard entre les différents acteurs (Cisco,..)
3. Normalization
   prendre les messages de log et les arranger dans un format commun
4. Corrélation
   En fonction des logs de plusieurs équipements on peut détecter une corrélation d'événements.
5. Action
   - To Analysts
   - Alerts
   - Email
   - Long-Term Storage

Correlation de vulnérabilité:

Scanners de vuln, permettent de trouver les systèmes qui sont vulnérables à certains types d'attaques.
info des scannes: vuln host / vuln ports / what to do
Combinaison des analyses de menaces avec des données réèles pour éviter les faux positifs.

analyse statistique

analys fréquencielle / Baseline / Machine learning / combinaison avec règles de corrélation

Acronymes

MIB : Management Information Base
SMI : Structure of Management Information -> SMIv2
NMS : Network Managment Station
OID : Object Identifier
TCO : Total Cost of Ownerships
BER : Basic Encoding Rules
IANA: Internet Assigned Numbers Authority
USM : User-Based Security Model
VACAM: View Access Control Model

1,

1. **"le Network managment" :**
   fait référence aux activités, methods, procédures et outils qui se rapportent aux opérations, administration, maintenance et provisionnement d'un sysème connecté.
2. **analogies entre un patient en soin intensif et la management d'un réseau :**
   on peut monitorer un patient comme on gère un réseau, lever des excéption en cas de crise cardiaque ou distribuer des médicaments automatiquement.
3. **aspect dans lesquels une analogies au management réseau s'applique:**
   Monitoring, planning et controle sont impliqués dans beaucoup d'aspect.(trains, mission spaciales, centrale électriques.
4. **Comment le network management peut aider un dep IT à économiser:**
   Localiser plus facilement des pannes réseaux, moins de temps pour les résoudres et la répartition des techniciens est plus efficaces. Automatisation des tâches répétitives pour soulager le personnel.
5. **Comment le network management peut acroitre le revenu d'un service provider :**
   Mettre en place des services pour plus de clients rapidement signifie plus d'entrée plus vite. / Offrire de nouveau services de communication incombe à plus d'entrées qui serait pas possible sans des capacités de management correspondant.
6. **network management perspectives en entreprise ou pour service provider :**
   service provider : Network management est un point de valeur compétitive. Donc gros investissement sur la partie support infra. En entreprise, cette partie est sous évalués.
7. **five nines, temps de disponibilité de 99,999%, si un erreur cause l'arret du système durant 5 min, calculer la temps en mois :**
   le temps de disponibilité tombe de 99,999 à 99,9% (30x24x60x60=2'592'000 sec en 1 mois) 99,999 = 2'5910987 seconde, avec 5 min en moins = 2'591'687 donc 99,988%
8. **En quoi le network management d'une entreprise diffère de celle d'un service provider :**
   le service provider cherche a avoir le réseau le plus compétitif possible sur le marché, invéstisse dans le support des infras, et custom développement, une entreprise va prendre en considération les couts.
9. **sydrome de la chaise pivotante :**
   problème de manque d'intégration entre les app de gestion obligeant les opérateurs réseau à utiliser plusieurs termianux à la fois et a pivoter la chaise.
10. **Pourquoi les app de net man sont sous la form de systèmes distribués :**
    Management applications are inherently of a distributed nature because they involve communication among multiple systems (management systems and network equipment). In addition, distributed systems help to address scaling requirements that might require the capability to add hardware to increase horsepower, resilience requirements that might require support for failovers between systems in case individual systems fail, and requirements to support follow-the-sun operations across geographically diverse regions.

1,

- **la gestion réseau considère seulement les technos de management réseau :**
  Non, aussi l'organisation, les procédure et les facteurs humains
- **comment tracer la résolution d'un problème dans un réseau :**
  avec un système de ticket contenant les informations pertinentes et les étapes de leur résolution, permet d'éviter les infos redondantes, notifie les adminitrateurs, checker les status.
- **Quels outils utiliser pour un admin réseau :**
  feuilles excel pour les graph de performance, feuille et stilo pour tracer les numéro de téléphone, et des outils de management réseau.

3,

- **donner les deux context ou le terme agent est utilisé :**
  1. le role d'agent, role de gérer un élément du réseau. 2. composant logiciel d'un réseau implémentant une gestion d'interface et de communication entre élément réseau.
- **comparez le paradigme de manager/agent et client/server :**
  dans les deux cas, la communication entre les role est asymétrique, entre manager et client on les deux l'initiative et envoient des demande au système, Agent et serveur sont les deux subordonné aux demandes reçue. La différence est que le manager gère plusieurs agent mais un agent est gérer par un seul ou peu de manager, alors que le serveur sert beaucoup de client.
- qu'est ce qu'une MIB :
  c'est un base d'information représentant une abstraction d'élément réseau pour le management, fournit par agent sytème.
- **différence entre MIB et base de donnée :**
  la MBI représente une vue des ressources réelles, pas un set de données nécéssitant d'etre géré de l'extérieur.
- **le traffic de gestion est différent des autre traffic, dans ce cas les network equipement sont la destination ou l'origine du traffic, donnez un exemple de traffic ou le network equipement ne fait que de switcher et rooter mais participe activement :**
  les netowrk equipement peuvent controler et signaler le trafic comme par exemple le traffic provenant des protocol de routing.
- **quelle est la raison la plus important pour utiliser une gestion réseau dédiée au lieu d'une partagle :**
  Pour des questions de fiabilité, dans le cas d'erreur réseau ou de congestion, il est important de communiquer avec des élément réseau pour le diagnostique et corriger les erreurs, sans le management dédié cela serait compliqué. Cela permet aussi d'éviter les interférence avec d'autre traffic réseau.
- **QUel autre terme est utilisé pour parler de management système :**
  Operational support système (OSS)
-

6, management conversation

1. **Nomer 4 catégores d'information de management et dire ce qui les distingues :**
   - State information reflects the current state of physical and logical resources. It is used mainly for monitoring. It tends to be dynamic in nature and subject to constant change, and it cannot be modified by management applications.
   - Physical configuration information is static in nature, changing rarely, if at all; it cannot be modified by management applications.
   - Logical configuration information concerns parameter settings that are subject to modification by network administrators and management applications. It provides the management "knobs" for the managed device.
   - Historical information contains periodic past snapshots of state information, as well as logs of events that have occurred in the past. It is less common than other categories of management information and is often retrieved in bulk from the device.
2. **De quel manière une MIB diffère d'une base de donnée :**
   C'est une vue abstraite d'un système réèle actif, non un set d'information qui est toqué quelque part dans un système de fichier. La MIB est optimizée pour les tâches de management.- for example, omitting general-purpose database capabilities such as joins— and has a smaller footprint. L'objet managé contenu dans une MIB tend à être plus heterogene qu'une information contenue dans une base de donnée de management system.
3. **2 paradimgs sous-jacent au langage de definition MIB :**
   - Orienté Table
   - Orienté Objet
4. **Un objet MIB pour lequel il fait sens d'avoir un accès maximum de "write only :**
   Un objet content des informations sensible tel que des mots de passe.
5. **Nom du langage pour la definition de l'information de management utilisé avec SNMP:**
   SMI, Structure of Management Information -> SMIv2
6. **Dans SMI, différence entre un OID désignant :**
   - **un objet** : OID qui férère un objet est globalement unique.
   - **l'instance d'un objet** : est unique seulement dans le MIB qui le contient.
7. **Pourquoi les objet SNMP MIB ne sont pas considérés objets dans un sens "object-oriented" :**
   They lack features that are commonly associated with object orientation. One such feature is inheritance (the capability to derive specializations from existing object class definitions). Other object-oriented features that SNMP MIB objects lack but that were not mentioned in the chapter include polymorphism (the capability for instances of a subclass to be treated as if they are instances of a superclass) and the inclusion of methods as part of the object class definition, commonly associated with the property of encapsulation. SNMP MIB objects are essentially simply MIB variables.
8. **Les SNMP MIBs utilisent une nomenclature hiérarchic très similaire à la structure de beaucoup de système opérationels utilisent pour nomer une strucutre de fichiers. Dans quel sens l'arbre d'identifcation d'objects de SNMP MIB est différent d'un système de nomenclature d'un système de fichier.**
   The naming tree in a file system represents a containment hierarchy between the objects. If you delete an object that contains other objects—that is, that are in a subtree underneath the object—those other objects will be deleted as well. The object identifier tree of SNMP MIBs, on the other hand, does not reflect a hierarchy between objects. Instead, it reflects the structure of the underlying MIB definition, or the way in which the definitions of the object types are grouped that are instantiated by objects in the MIB. The objects in the MIB themselves are flat; every one of them is a leaf node in the MIB object identifier tree.
9. **A quoi fait référence la granularité d'un model :**
   It refers to the degree to which management information is aggregated and lumped together (coarse granularity), or to which every individual real resource is separately accounted for (fine granularity). Generally, a coarse-grained model is more efficient but offers less detailed control capabilities than a fine-grained model.