

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 ressourceces de manière plus efficaces.

Dispose d'options sophistiquées d'analyse pour le flot de données.

Données récoltées:

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

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 engine: Dispatcher, processing des messages, **Sécurité(DES->3DES->AES), authentification(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
5. Action

En fonction des logs de plusieurs équipements on peut détecter une corrélation d'événements.

- 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 réelles pour éviter les faux positifs.

analyse statistique

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

Acronymes

MIB : Management Information Base

SMI : Structure of Management Information -> SMIV2

NMS : Network Management 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

TMN : Telecommunications Management Network, standards définissant un réseau utilisé pour la gestion d'autres réseaux

1,

1. **"le Network management" :**
fait référence aux activités, méthodes, procédures et outils qui se rapportent aux opérations, administration, maintenance et provisionnement d'un système connecté.
2. **analogies entre un patient en soin intensif et la gestion d'un réseau :**
on peut monitorer un patient comme on gère un réseau, lever des exceptions en cas de crise cardiaque ou distribuer des médicaments automatiquement.
3. **aspect dans lesquels une analogie au management réseau s'applique:**
Monitoring, planning et contrôle sont impliqués dans beaucoup d'aspects (trains, mission spatiales, 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 résoudre et la répartition des techniciens est plus efficace. Automatisation des tâches répétitives pour soulager le personnel.
5. **Comment le network management peut accroître le revenu d'un service provider :**
Mettre en place des services pour plus de clients rapidement signifie plus d'entrée plus vite. / Offrir de nouveaux services de communication incombe à plus d'entrées qui seraient 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 évaluée.
7. **five nines, temps de disponibilité de 99,999%, si une erreur cause l'arrêt du système durant 5 min, calculer la temps en mois :**
le temps de disponibilité tombe de 99,999 à 99,9% ($30 \times 24 \times 60 \times 60 = 2'592'000$ sec en 1 mois) $99,999 = 2'591'0987$ 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 à avoir le réseau le plus compétitif possible sur le marché, investisse dans le support des infra, et custom développement, une entreprise va prendre en considération les coûts.
9. **syndrome de la chaise pivotante :**
problème de manque d'intégration entre les appl de gestion obligeant les opérateurs réseau à utiliser plusieurs terminaux à la fois et à pivoter la chaise.

10. **Pourquoi les appl de net man sont sous la forme 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.

2,

- **la gestion réseau considère seulement les technos de management réseau :**
Non, aussi l'organisation, les procédures 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 administrateurs, checker les status.
- **Quels outils utiliser pour un admin réseau :**
feuilles excel pour les graph de performance, feuille et stilo pour tracer les numéros de téléphone, et des outils de management réseau.

3,

- **donner les deux contextes où le terme agent est utilisé :**
1. le rôle d'agent, rôle 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 rôles est asymétrique, entre manager et client on les deux l'initiative et envoient des demandes au système, Agent et serveur sont les deux subordonnés aux demandes reçues. La différence est que le manager gère plusieurs agents mais un agent est géré par un seul ou peu de managers, alors que le serveur sert beaucoup de clients.
- **qu'est-ce qu'une MIB :**
c'est une base d'information représentant une abstraction d'élément réseau pour le management, fournit par agent système.
- **différence entre MIB et base de données :**
la MIB représente une vue des ressources réelles, pas un set de données nécessitant d'être géré de l'extérieur.
- **le trafic de gestion est différent des autres trafics, dans ce cas les network equipment sont la destination ou l'origine du trafic, donnez un exemple de trafic où le network equipment ne fait que de switcher et router mais participe activement :**
les network equipment peuvent contrôler et signaler le trafic comme par exemple le trafic provenant des protocoles de routing.
- **quelle est la raison la plus importante pour utiliser une gestion réseau dédiée au lieu d'un partage :**
Pour des questions de fiabilité, dans le cas d'erreur réseau ou de congestion, il est important de communiquer avec des éléments réseau pour le diagnostic et corriger les erreurs, sans le management dédié cela serait compliqué. Cela permet aussi d'éviter les interférences avec d'autres trafics réseau.
- **Quel autre terme est utilisé pour parler de management système :**
Operational support système (OSS)

4,

- **Quels sont les aspects de gestion de l'interopérabilité :**
la communication, les fonctions et les informations.
- **Pourquoi un protocole entre managers et agents est-il nécessaire et pas seulement un connectivité:**
La connectivité leurs permettrait de s'entendre mais pas forcément ce comprendre. le protocole de gestion va permettre de définir les syntaxe et les règles de communication.
- **Pourquoi il est important pour l'interopérabilité qu'un manager comprenne les fonction provenant d'un agent :**
si il n'y a pas de compréhension entre eux, le manager pourrait de pas comprendre les code de retour et les effets d'un opération. Pas exemple si un manager envoie un groupe de commande et que l'agent les effectue pas de manière transactionnelles.
- **Utilité des normes de gestion dans le cas ou on gère plusieurs périphériques et fournisseurs :**
Car si on a pas de norme nous devrions définir des script pour toutes les différentes interfaces au lieu d'une.
- **nommer les 3 phases du cycle de vie de la gestion réseau :**
planification réseau, déploiement réseau, opération réseau.
- **Un upgrade peut causer des soucis de disponibilité dans un réseau, citez trois exemples :**
déconnection et reconnection d'un cable physique, charger une nouvelle image logiciel (OS) nécessitant un reboot. Effectuer des mise à jour réinitialisant les configurations déjà faites.

6, management conversation

1. **Nommer 4 catégories d'information de management et dire ce qui les distingues :**

- **State information :** reflète l'état courant de ressources physique ou logiques. Utilisé dans le monitoring, dynamique et souvent modifié par les applications de management.
- **Physical configuration information :** statique par nature, change rarement et ne peut pas être modifié par les applications de management.
- **Logical configuration information :** concerne la configuration des paramètre qui peut être modifié par les administrateurs réseau ou les application de management
- **Historical information :** contient des snapshots periodiques de l'état des informations, logs des événements passés, le plus commun.

2. **De quel manière une MIB diffère d'une base de donnée :**

C'est une vue abstraite d'un système réel actif, non un set d'information qui est stocké quelque part dans un système de fichier. La MIB est optimisée 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 hétérogène qu'une information contenue dans une base de données de management system.

3. **2 paradigmes sous-jacent au langage de définition MIB :**

- Orienté Table
- Orienté Objet

4. **Un objet MIB pour lequel il fait sens d'avoir un accès maximum de "write only" :**
Un objet contient des informations sensibles tel que des mots de passe.

5. **Nom du langage pour la définition 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 définit un objet est globalement unique.
- **l'instance d'un objet :** est unique seulement dans la MIB qui le contient.

7. **Pourquoi les objets SNMP MIB ne sont pas considérés objets dans un sens "object-oriented" :**

Il manque de fonctionnalités généralement associées à l'orienté objet tel que l'héritage, ou le polymorphisme ainsi que la définition des méthodes dans les classes qui sont au final essentiellement fait de variables MIB.

8. **Les SNMP MIBs utilisent une nomenclature hiérarchique très similaire à la structure de beaucoup de systèmes opérationnels utilisés pour nommer une structure de fichiers. Dans quel sens l'arbre d'identification d'objets de SNMP MIB est différent d'un système de nomenclature d'un système de fichier.**

Dans le cas d'une arborescence d'un système de fichier, si on supprime un objet contenant d'autres objets ces derniers seront aussi supprimés. Dans le cas d'une arborescence MIB SNMP, ça ne reflète pas une hiérarchie entre objets mais la structure de la définition de base MIB, les objets dans la MIB sont donc plats et chacun est un nœud.

9. **A quoi fait référence la granularité d'un modèle :**

cela se réfère au degré auquel les informations de gestion sont regroupées (granularité forte) ou chaque ressource individuelle (granularité faible). En général la granularité forte offre de meilleures performances mais moins de capacité de contrôle.