Licence Professionnelle SEICOM
Module M3-7
« Administration des SI »

Pierrick Tasse – Damien VERON
IUT Nantes, GEII

Présentation technique

Sommaire

- Introduction
- L'approche structurée de l'administration
- La supervision
- Logiciels de supervision et métrologie
- Logiciels d'administration

Introduction

- **Introduction**
- L'approche structurée de l'administration
- La supervision
- Logiciels de supervision et métrologie
- Logiciels d'administration

Introduction

- Croissance des réseaux informatiques
  - Autrefois : concentrés sur des gros systèmes avec terminaux déportées
  - Maintenant : éclatés sur différents environnements
- La tendance va à regrouper des systèmes autrefois indépendants :
  - Téléphonie sur IP et Interphonie sur IP
  - Vidéo sur IP (caméras, télévision)
  - SCSI over Ethernet (iSCSI), Fiber Channel over Ethernet (FCoE)
- Dépendance des entreprises vis-à-vis de leur SI et plus particulièrement dudit réseau.
  - Besoin de contrôler l'état et la qualité

Introduction

- La donnée subit souvent un traitement particulier : sauvegarde, archivage, haute-disponibilité (matérielle, logicielle)
  - Le rôle des équipes informatiques est de contrôler le bon fonctionnement de ces systèmes qui hébergent les données.
- Le réseau (infrastructure de transit des données entre les équipements serveurs et les postes de travail) ne subit pas toujours les mêmes attentions, voir est négligé. Pourtant, il est au cœur des enjeux de :
  - Performance
  - Disponibilité
  - Intégrité

Introduction

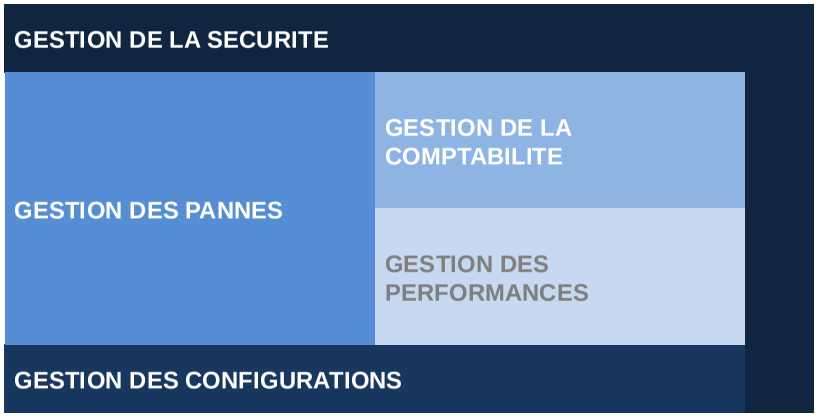
- L'administration : c'est l'ensemble des moyens mis en œuvre pour garantir l'efficacité du système et sa disponibilité, pour assurer la surveillance des coûts et la planification des évolutions.
- L'administration d'un réseau suppose l'existence d'une base d'informations décrivant l'ensemble des objets administrés.

L'approche structurée de l'administration

- Introduction
- **L'approche structurée de l'administration**
- La supervision
- Logiciels de supervision et métrologie
- Logiciels d'administration

L'approche structurée de l'administration

- L'ISO (Organisation internationale de normalisation) distingue cinq domaines de l'administration réseau :



L'approche structurée de l'administration

- Gestion des configurations
  - Définition : recueillir, définir et suivre les configurations des équipements.
  - Exemples :
    - Inventaire du parc (manuel, automatique)
    - Consignation des évolutions
      - Matérielles et logicielles
      - Configurations

L'approche structurée de l'administration

- Gestion des pannes
  - Définition : identifier, isoler, corriger et enregistrer les incidents qui surviennent sur un réseau.
  - Exemples :
    - Données recueillies par un logiciel de supervision (NMS – Network Management System)
      - 1 - Requête
      - 2 - Détection d'un incident
      - 3 - Enregistrement
      - 4 - Notification
      - 5 - Correction
      - 6 - Consignation dans une base de connaissances

L'approche structurée de l'administration

- Gestion de la comptabilité
  - Définition : récupérer des statistiques d'usage pour les utilisateurs.
  - Exemples :
    - Définition des centres de coût
    - Mesure des dépenses (structure) et répartition
    - Mesure des consommations par service
    - Imputation des coûts

L'approche structurée de l'administration

- Gestion des performances
  - Définition : déterminer l'efficacité d'un système d'informations pour mieux anticiper l'avenir.
  - Exemples :
    - Données recueillies par un logiciel de supervision (NMS – Network Management System)
      - Mesures : Temps de réponse, Espace disque, Débits réseaux, CPU/RAM, etc.
      - Le stockage des données mesurées
      - Présentation des données : tableau, graphique, tendance

L'approche structurée de l'administration

- Gestion de la sécurité
  - Définition : contrôler l'accès aux ressources du système d'informations.
  - Exemples :
    - Regroupe tous les domaines de la sécurité afin d'assurer l'intégrité des informations traitées et des objets administrés :
      - Contrôle d'accès au réseau
      - Confidentialité des données
      - Intégrité des données
      - Authentification
      - Non-répudiation

La supervision

- Introduction
- L'approche structurée de l'administration
- **La supervision**
- Logiciels de supervision et métrologie
- Logiciels d'administration

Le concept de supervision réseau

- La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants.
- Ces données seront ensuite traitées et affichées afin de mettre en lumière d'éventuels problèmes.
- La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS par exemple) les administrateurs.
- Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4.

Le concept de supervision réseau

- **Supervision réseau**
  - Par le terme réseau on entend ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre que l'on va vérifier par exemple si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.
- **Supervision système**
  - La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Si l'on souhaite par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur voire analyser les fichiers de logs système.
- **Supervision applicative**
  - Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine. Cela peut être par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs. En effet rien ne garantit qu'un port X ouvert veut dire que l'application qui tourne derrière n'est pas "plantée".

Le concept de supervision réseau

- Il existe des protocoles réseaux qui permettent de récupérer des informations sur le parc informatique.
  - Supervision ICMP
  - Supervision de bas niveau (locale)
  - Supervision par centralisation des logs
  - Supervision SNMP

La supervision ICMP

- ICMP est un protocole de couche réseau (couche 3 du modèle OSI)
  - Vient palier à l'absence de message d'erreur du protocole IP (Internet Protocol).
  - Si il y a un incident de transmission les équipements intermédiaires vont utiliser ce protocole pour prévenir la machine émettrice.
  - Les paquets ICMP sont encapsulés dans des paquets IP (malgré qu'ils soient au même niveau OSI), et peuvent contenir des bouts de paquets IP pour citer celui ayant généré l'erreur.

La supervision ICMP

- Afin de catégoriser les erreurs, elles sont divisés en types eux-mêmes parfois redivisés en codes.
  - Par exemple le type 3 représente un destinataire inaccessible : Il existe 16 codes différents en fonction de la raison pour laquelle le destinataire n'est pas joignable.
- C'est un protocole très simple, qui n'a pas pour fonction directe la supervision d'un réseau mais qui est utilisé comme source d'information sur la qualité du réseau ou sur la présence d'une machine.

La supervision Bas niveau

- Accès local depuis la machine
- En quelques lignes de shell script, on peut construire un rapport d'état de la machine.
- Une entrée dans la crontab et la supervision locale peut être assurée.
- Cette méthode est à éviter autant que possible :
  - on réinvente la roue ;
  - difficulté de maintenance de scripts maison à long terme;
  - de nombreux outils "clés en main" sont disponibles !

La supervision Bas Niveau

- On vérifie la charge :
  - **`top ou htop`**
- On vérifie la mémoire
  - **`free`**
- On vérifie l'espace disque
  - **`df -ah`**
- On vérifie la connectivité réseau
  - **`ethtool ethX`**

Supervision Bas Niveau

- On teste la connectivité d'une machine :
  - **`ping firewall.seicom.fr`**
- On vérifie que le service SSH fonctionne :
  - **`nmap -p 22 firewall.seicom.fr`**
- On vérifie qu'un service SMTP fonctionne :
  - **`telnet mail.seicom.fr 25`**
- On mesure les performances réseaux entre deux équipements :
  - **`Un serveur : iperf –s`**
  - **`Un client  : iperf –c firewall.seicom.fr`**

Supervision Bas Niveau

- On vérifie l'intégrité d'un fichier après un transfert par exemple :
  - **`ls –i /root/.basrc`**
  - **`md5sum /root/.basrc`**
  - **`sha1sum /root/.basrc`**
- Plusieurs outils permettent d'automatiser le contrôle d'intégrité : Tripwire et aide qui fonctionnent serveur par serveur et osiris qui fournit une protection centralisée.

Supervision par centralisation des Logs

- Face à l'augmentation de contrôles réglementaires et des audits, les solutions de collectes et de stockage des logs sont devenus incontournables.
- Certains dysfonctionnements ne peuvent pas être diagnostiqués (et donc résolus) sans les informations de « log » fournies par les équipements concernés. La plupart des équipements réseau, système et sécurité émettent régulièrement des messages sur leur fonctionnement. La majorité sont anodins, tandis que certains peuvent être critiques.
- Plusieurs protocoles standards sont disponibles :
  - Syslog est un protocole de transmission d'événements systèmes. Il permet de centraliser les événements systèmes de chaque serveur ou équipement réseau sur une seule machine pour des fins d'analyse statistique, d'archivage ou production d'alertes.
    - Composé d'une partie cliente et d'une partie serveur. La partie cliente émet les informations sur le réseau, via le port UDP 514. La partie serveur collectent l'information et se chargent de créer les journaux.
  - Netflow/IPFIX : Collecte les informations du trafic IP

Supervision par centralisation des Logs

- Attention ! Pour centraliser efficacement des journaux systèmes, il faut une source de temps (NTP) commune;
- En général, chaque événement est accompagné de (syslog) :
  - la date a laquelle a été émis le log
  - le nom de l'équipement ayant généré le log (hostname),
  - une information sur le processus qui a déclenché cette émission
  - le niveau de gravité du log
  - un identifiant du processus ayant généré le log
  - un corps de message.

Le protocole SNMP

- SNMP (Simple Network Management Protocol) est un protocole de couche applicative qui a pour but de superviser les réseaux.
- Conçu en 1988 par l'IETF (Internet Engineering Task Force) avec pour idée directrice de créer un protocole simple qui ne vienne pas gêner le trafic du réseau qu'il supervise.
- Depuis sa création, le protocole a évolué par soucis de sécurité: La version 2 qui est pour l'instant la plus utilisée possède une notion de communauté qui est utilisée comme un mot de passe, la version 3 durcit un peu plus le protocole en y ajoutant le chiffrement.

Le protocole SNMP

- Fonctionnement :
  - Par soucis de simplicité et donc de rapidité, SNMP ne transporte que des variables et s'appuie sur le protocole UDP (User Datagram Protocol).
  - SNMP va créer un dialogue entre des agents installés sur des machines à superviser et un serveur de supervision.
- Les échanges entre agents et serveur se résument à trois opérations, les alarmes, les requêtes et les réponses :
  - Une requête est émise du serveur vers un agent via le port 161 UDP si le serveur veut demander ou imposer quelque chose à cet agent. La requête peut être de quatre types
    - **GetRequest** : Demande la valeur d'une variable à un agent
    - **GetNextRequest** : Demande la valeur suivante de la variable
    - **GetBulk** : Demande un ensemble de variables regroupées
    - **SetRequest** : Demande la modification de la valeur d'une variable sur un agent

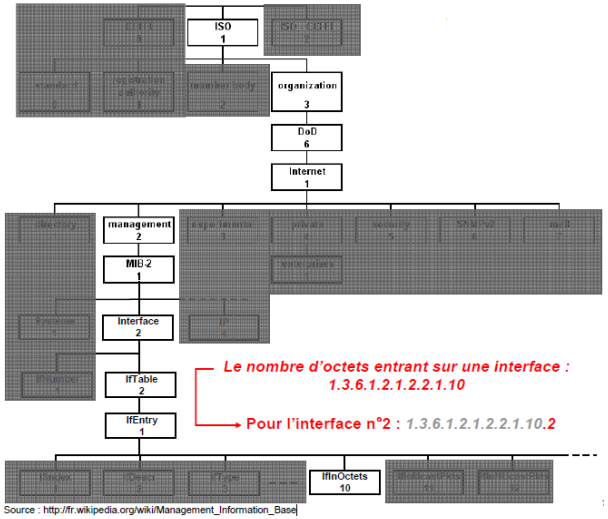
Le protocole SNMP

- L'agent va ensuite traiter cette requête et émettre une réponse via le même port. Si tout se passe bien, l'agent répond un GetResponse accompagné de la valeur demandée. Mais dans le cas contraire l'agent ajoutera un code d'erreur en réponse (par exemple No Access ou Read Only)
- Une alarme est créée par un agent en cas d'évènement et utilise un message dit de type trap ou de type inform pour prévenir le serveur. Ce message SNMP transite via le port 162 UDP. Les alarmes peuvent prendre les formes suivantes :
  - **ColdStart(0)** : Démarrage à froid du système
  - **WarmStart(1)** : Redémarrage à chaud du système
  - **LinkDown(2)** : Le lien réseau n'est plus opérationnel
  - **LinkUp(3)** : Le lien réseau est opérationnel
  - **AuthentificationFailure(4)** : Tentative d'accès à l'agent avec un mauvais nom de communauté
  - **EGPNeighboorLoss(5)** : La passerelle adjacente ne répond plus
  - **EntrepriseSpecific(6)** : Alarme propre aux constructeurs

- 4 éléments composent SNMP :
  - Un superviseur :
    - Station à l'origine de requêtes SNMP pour la collecte de données et leur mise en forme pour analyse.
  - Un élément actif :
    - Equipement du réseau comportant les informations à analyser.
  - La MIB (Management Information Base) :
    - Base d'information contenant tous les objets interrogeables (OID) de l'élément actif
  - Un agent :
    - Processus intégré aux éléments actifs en écoute et répondant au superviseur
    - Interroge les objets définis dans la MIB :
      - Nombre de paquets droppés sur une interface…
      - Etat de charge CPU…
      - Objet propriétaire, en fonction du constructeur…
    - Met à jour les informations concernant ces objets : les compteurs

- La MIB: Management Information Base
  - Base d'information permettant la gestion d'un équipement réseau
  - Structure normalisée et organisée de manière hiérarchique sous forme d'un arbre où chaque information est représentée par un objet (Object IDentifier - OID) dans une table
    - Un OID est identifié par une suite de chiffres séparés par des points :
      - Ex : ifType : type d'interface : 1.3.6.1.2.1.2.2.1.3
  - MIB-2 : sous-ensemble concernant les protocoles de l'Internet.
    - En métrologie c'est essentiellement ce sous-ensemble qui est utilisé!
    - Gestion des informations sur IPv4 et IPv6 partiellement
    - « Une MIB dans la MIB »

- L'arbre MIB

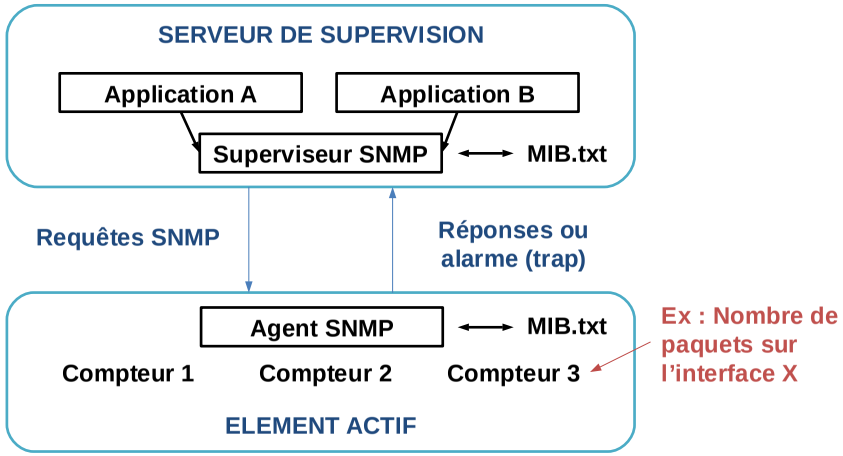


Source : http://fr.wikipedia.org/wiki/Management_Information_Base

- Utiliser la MIB
  - Sur un élément actif, la MIB standard et la MIB propriétaire sont déjà installées
  - Sur un serveur :
    - Besoin de connaître la MIB standard : installée avec NET-SNMP par exemple.
    - Besoin de connaître la(es) MIB(s) propriétaire(s) : à intégrer soi-même (à télécharger sur le site web du constructeur par exemple).
      - /usr/share/snmp/mibs/<Table_name>.txt :
        - SNMPv2-MIB.txt
        - IF-MIB.txt
        - IPV6-UDP-MIB.txt
        - TCP-MIB.txt
        - …
      - Sous forme de fichiers texte

Le protocole SNMP

- Fonctionnement

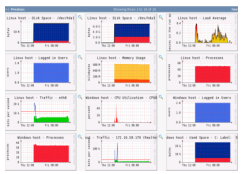


Logiciels de supervision et métrologie

- Introduction
- L'approche structurée de l'administration
- La supervision
- **Logiciels de supervision et métrologie**
- Logiciels d'administration

Logiciels de métrologie

- Ces logiciels fonctionnent tous sur le même principe :
  - collecter régulièrement les données de supervision sur les différents équipements en appelant un agent préinstallé (SNMP ou spécifique),
  - stocker ces données dans une base de données,
  - produire des représentations graphiques temporelles,
  - rassembler l'ensemble de ces informations sur un site web.
- *MRTG, MUNIN, GANGLIA, CACTI, CRICKET, TORRUS, NTOP, Monitorix*

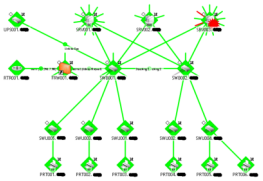


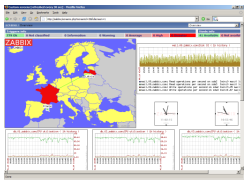
Logiciels de supervision

- Parmi les fonctions couramment proposées par les logiciels de supervision, on peut citer:
  - L'accès aux MIB des équipements supervisés
  - La visualisation de la topologie du réseau, et l'état des équipements
  - La collecte et La gestion des traps (quel action sur quel événement)
  - L'affichage et l'enregistrement de statistiques sur des objets de la MIB (charge CPU, occupation mémoire, charge d'un lien, etc.)
  - La génération automatique de rapports
  - Pour les logiciels propriétaires : la configuration d'équipements, la sauvegarde et la gestion des logiciels et configurations
- Ces logiciels permettent souvent de créer des graphiques avec les données obtenues, mais sans la flexibilité des logiciels de métrologie.

Logiciels de supervision

- Logiciels de SUPERVISION Open-Source : MONIT, XYMON / HOBBIT, NAGIOS, ZABBIX, MONALISA, OpenNMS, ZENOSS CORE
- Logiciels de SUPERVISION éditeurs : HP Open View, Castle Rock SNMPC, CA Unicenter, Microsoft SCOM, Ipswitch WhatsUp Gold, IBM Tivoli Netcool, Luteus LoriotPro





Logiciels d'administration

- Introduction
- L'approche structurée de l'administration
- La supervision
- Logiciels de supervision et métrologie
- **Logiciels d'administration**

Pour l'OS Windows

- Kiwi Cattools : sauvegarde automatique des équipements réseaux et d'autres tâches d'automatisation
- mRemote : gestion des connexions aux équipements (RDP, telnet, SSH, VNC, http, etc.)
- puTTY, WinSCP : accès SSH
- Keepass, TrueCrypt : protection des données
- Look@LAN Network Monitor : scanner réseau
- Wireshark : Analyseur réseau

Pour l'OS Linux

- Nmap : Scanner réseau
- Metasploit : Outil de détection et de tests de vulnérabilités
- Nessus : Outil de détection de vulnérabilités
- Snort : Détection et prévention des intrusions
- Wireshark : Analyseur réseau
- Cain & Abel : Outil de récupération de mots de passe pour Windows
- Kismet : outil de détection, de capture et d'analyse des réseaux wifi

Application Serveurs

- OCSi NG : Outil d'inventaire d'un parc informatique
- GLPI : Outil de gestion de parc
- Network WeatherMap : Météo d'un réseau
- Octopussy : centralisation des logs