La supervision

Un monde transverse

Présentateur

Nom — **MAILLIET François-Hugues**

Position — **Experts et architectes des solutions de traçabilité et de surveillance**

Expérience — **Experts des solutions de surveillance, d'automatisation et des processus ITIL depuis une vingtaine d'année**

Contributeur à la Cool Team

Sociétés

TOULOUSE ynov CAMPUS

Cool Monitoring Supervision en mode SaaS

LA BANQUE POSTALE

UTAK

Agenda

- Préambule
- Positionnement, définition
- Quelques déclinaisons
  - Introduction à la supervision réseau
  - Introduction à la supervision des systèmes et des infrastructures applicatives
  - Introduction au ressenti utilisateur et à l'APM

Préambule

- De quoi parlons nous ?
  - En soit, l'automatisation est applicable a beaucoup de domaine :
    - Informatique, Domestique, Chaine de montage et robotique, …
- Brouillage
  - la recherche du mot clef, de l'accroche ou encore attirer l'œil
    - pour se distinguer, chaque compétiteur a une façon de parler déformée : le jargon
      - ✓ http://jargonf.org/wiki/Accueil

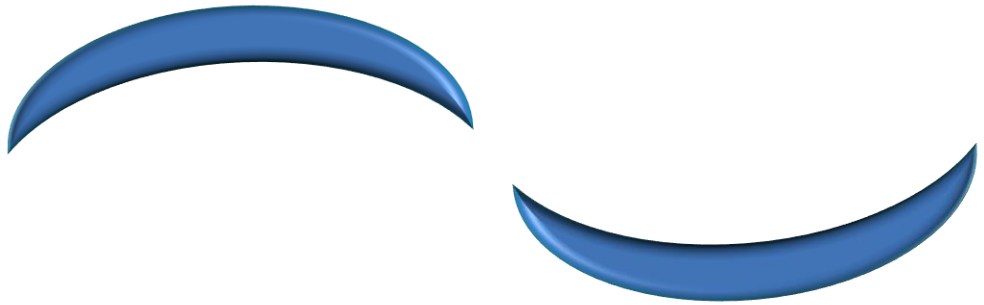
  - l'innovation
    - dans le domaine de l'informatique, ne sommes nous pas tous rentrés dans le « **cloud** » voire l'air du 2.0, oups, 3.0 ?
  - Les sigles et acronymes : KPI, VIP, SMS

Internet

- Outil extrêmement puissant, et la puissance a 2 conséquences
  - Le meilleur
  - Le pire
- Les recherches
  - Une information sur 2 est fausse ou obsolète
- Comportement
  - Ne pas prendre pour argent comptant ce que vous trouvez
  - Regarder la vétusté des informations
  - Améliorer vos critères de recherches sur la temporalité
  - Prendre le temps de lire, comprendre, analyser et tester
  - Utiliser son sens critique
  - Remonter à la source

… et de conclure le préambule

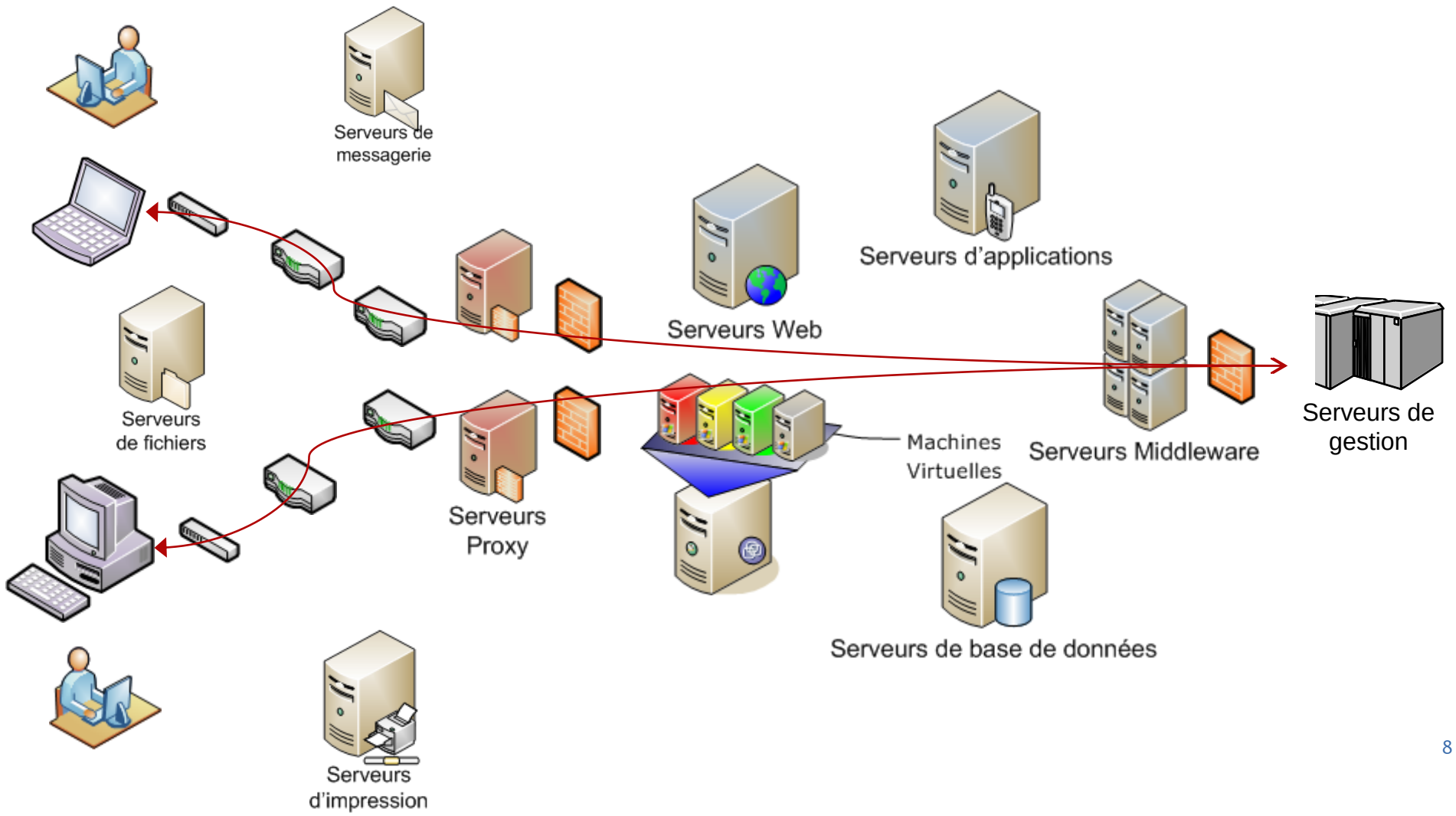
Entre ce que je pense,
ce que je veux dire,
ce que je crois dire,
ce que je dis,
ce que vous voulez entendre,
ce que vous entendez,
ce que vous croyez y comprendre,
ce que vous voulez comprendre,
et ce que vous comprenez,
Il y a au moins 9 possibilités de ne pas se comprendre…



Définitions

L’essentiel de la supervision

Le système d'informations



La supervision

- Le terme « supervision » dépend beaucoup du contexte :
  - Supervision industrielle
    - La supervision est chargée d'assurer le contrôle de l'exécution d'un plan de fabrication.
    - Elle est liée à des fonctions de surveillance du système de production.
    - Exemple :
      - ✓Surveillance d'une chaine de montage
      - ✓Surveillance d'un plan de circulation d'une ville (gestion des feux)
      - ✓Surveillance des crues (capteurs de niveaux).
  - Supervision des infrastructures informatiques

Définition

- Supervision : permet de surveiller, rapporter et alerter sur le fonctionnement du système d'informations.

- Amalgame :
  - « administration », on ne gère ni ne modifie des configurations d'équipements au travers de la supervision ;
  - « automatisation », la supervision n'est pas un gestionnaire de travaux planifiées avec dépendances.

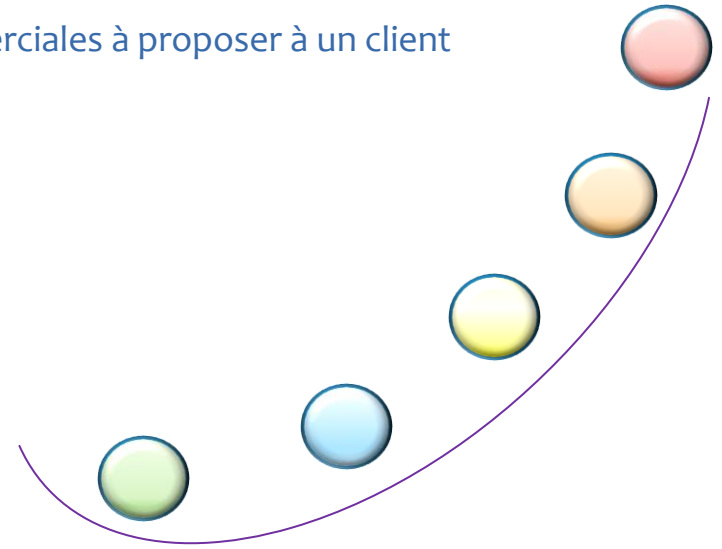
- Fonctionnements anormaux : à quoi pense-t-on ?
  1. Indisponibilité
  2. Dégradation de performance
  3. Capacité insuffisante
  4. …

Alerte

Disponibilité

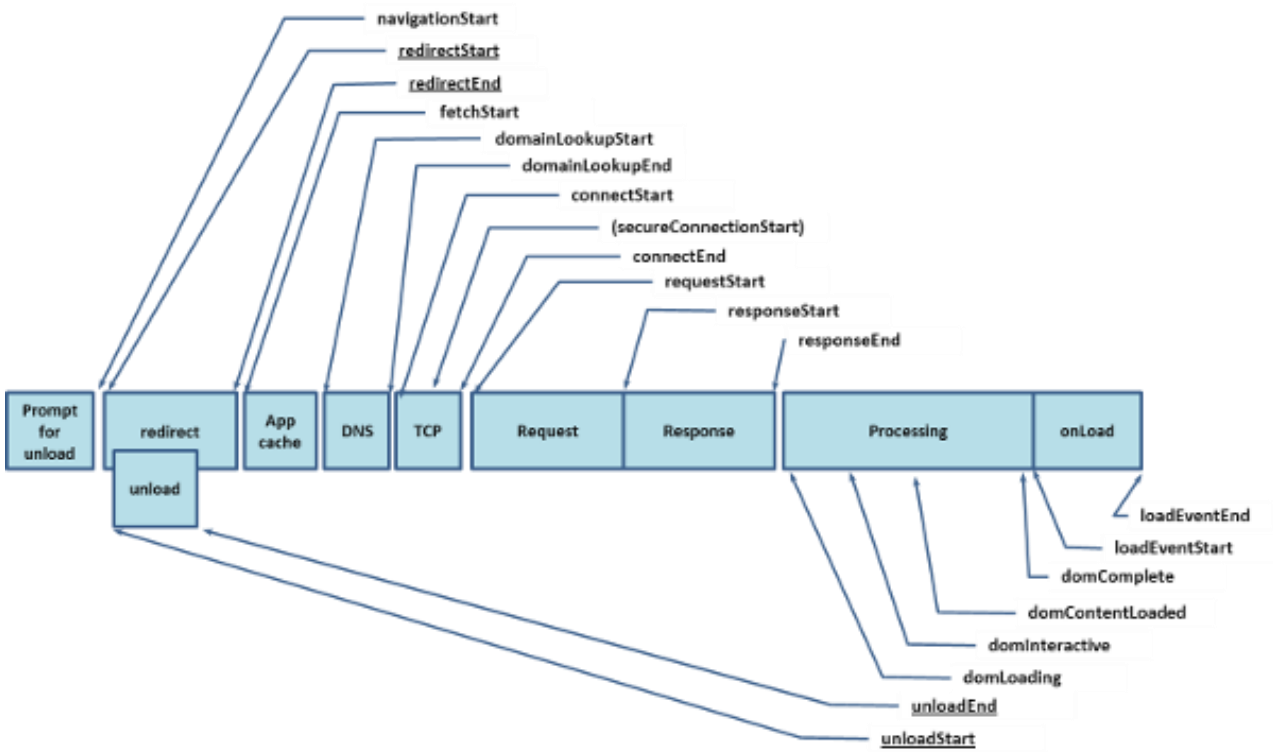
- Contrôle de disponibilité
  - D'un composant de l'infrastructure (serveur, baie, switch, routeur, borne Wifi, cluster , …)
  - D'un service rendu
    - D'infrastructure, comme l'attribution d'une adresse IP (DHCP)
    - Métier s'appuyant sur le système d'informations. Ce service rendu s'appuie sur une application « métier ». Exemples :
      - ✓ Consultation d'un dossier « patient » par un médecin
      - ✓ Consultation par un conseiller d'une liste d'actions commerciales à proposer à un client
      - ✓ Consultation des interdits bancaires

- Besoins :
  - Alerte
  - Rapport de disponibilité
  - Engagement & contrât de service (SLO/SLA)



Performance

- Service rendu
  - Avec quelle performance le service est-il rendu ?
    - Temps de réponse
      - ✓Global
      - ✓Détaillé
    - Latence



Capacité

- On prévoit :
  - Un espace disque
  - Puissance CPU
  - Une taille mémoire
  - Un débit des accès réseau
- On regarde :
  - Le taux d'occupation des espaces disque
  - Le pourcentage d'utilisation de la puissance CPU
  - Le pourcentage d'occupation de la taille mémoire
  - Le taux d'occupation de la bande passante

Définition : la métrologie

- Métrologie :
  - La métrologie est la science de la mesure au sens le plus large
- La supervision s'appuie sur la métrologie, que cela soit pour le contrôle de :
  - la disponibilité
  - la performance
  - la capacité
- Historiquement :
  - On associe souvent en informatique le terme « métrologie » au domaine « réseau », plus particulièrement pour désigner les analyseurs réseau (sniffers), mais également à la partie suivi des indicateurs dans le temps et à l'aspect restitution.

Une approche par couche

Collecte
- Gestion des prérequis
- Récupération des indicateurs

Traitement
- Normalisation, dépollution, filtrage, …
- Corrélation

Stockage
- Gestion de la rétention
- Gestion des volumes de données (fréquence)

Restitution
- Gestion des événements, notifications, …
- Rapports de suivi, tendance, capacité, …

La terminologie

- Monitoring vs supervision vs métrologie vs hypervision vs supervision unifiée
- Monitoring interne/externe
- Monitoring actif/passif
- États, métriques, événements, alertes, incidents

Autres termes

- Monitoring : anglicisme de la supervision
  - Ce dernier a souvent une connotation de « petit » outil apportant peu de valeur ou trop cantonné à un domaine ou une technique (purement réseau, uniquement SNMP par exemple)
- Hypervision
  - A pour vocation a donner une vision plus élargie du système d'informations, fédérant les silos et apportant une meilleure analyse d'impact.
- Gestion des événements (cf. planche suivante)

Approche ITIL v3

- ITIL v2 avait introduit
  - La gestion de la capacité et la gestion de la disponibilité
- ITIL v3 introduit 3 nouveaux processus dans le domaine « Service Operation »
  - La **gestion des événements**, des accès et la gestion des demandes complètent la gestion des incidents et des problèmes

Approche ITIL v3

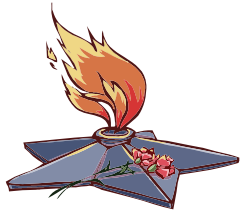
- Gestion des événements : une des sources de la gestion d'incidents
- Un événement peut conduire ou non à un incident, voire, fonction de sa récurrence, à un problème.
- Mais au fait, un événement c'est quoi ?
  - toute occurrence détectable ou discernable ayant une importance en relation avec l'infrastructure du système d'informations ou la mise à disposition d'un service

La sévérité

- « Informationnel » :
  - événement ne nécessitant aucune action (connexion ok, sauvegarde ok, job ok, ...)

- « Avertissement » :
  - événement généré lorsqu'un service ou un équipement s'approche d'un seuil d'exception, mais n'y est pas encore (limite de capacité, ...). Nous sommes dans l'anticipation.

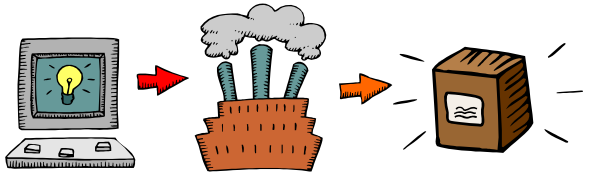
- « Exception » :
  - événement généré lorsqu'un service ou un équipement opérationnel est dans un état anormal. Il s'agit typiquement d'une violation d'un OLA/SLA. Nous sommes dans la réactivité.



Approche ITIL v3 - processus afférents

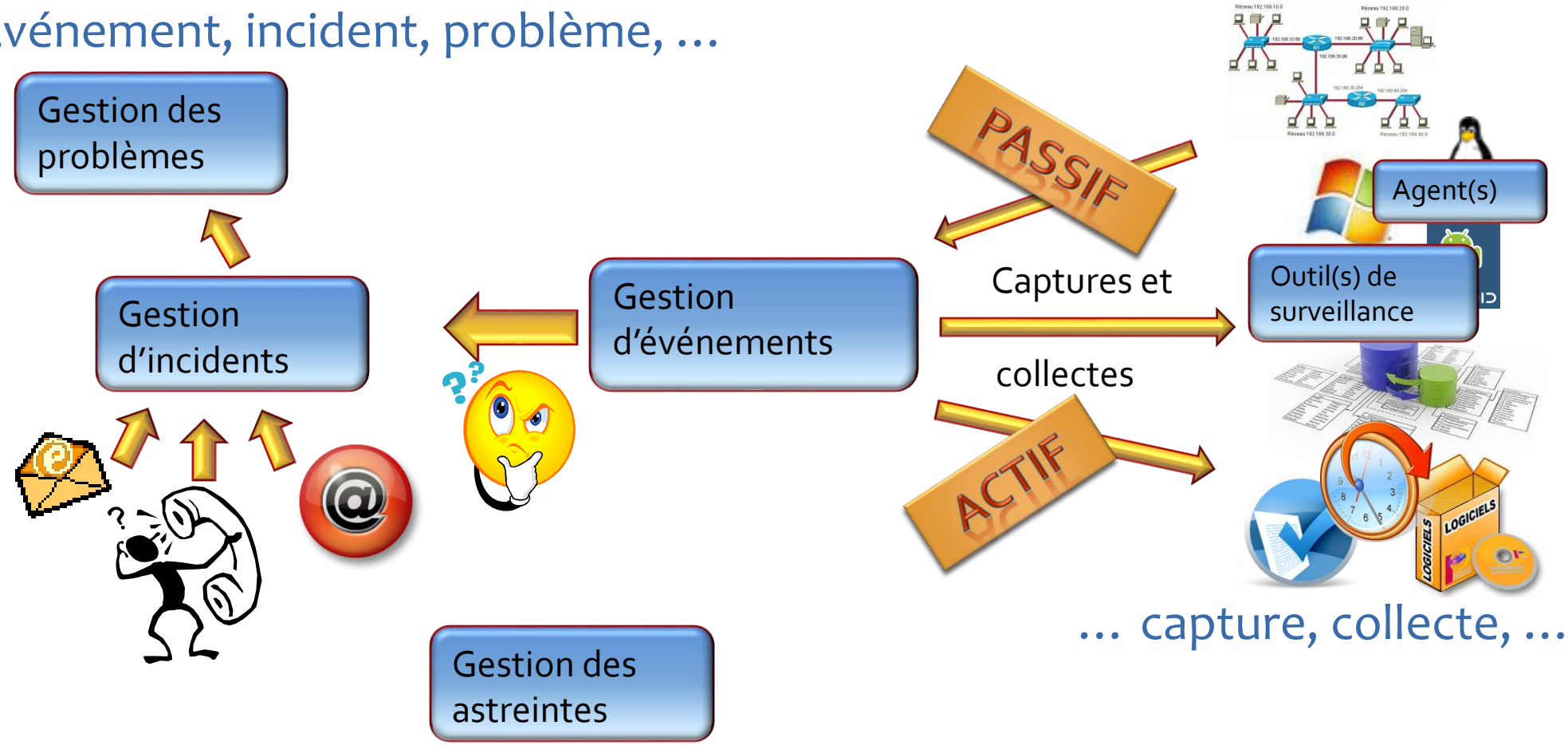
- Gestion des incidents/problèmes (entre autres)

- Le cycle de vie en relation avec
  - la gestion des configurations
  - la gestion des changements
  - la gestion des demandes
  - la gestion des appels
  - ...



Les plus directement liés

- Evénement, incident, problème, …



… capture, collecte, …

Avec la maturité

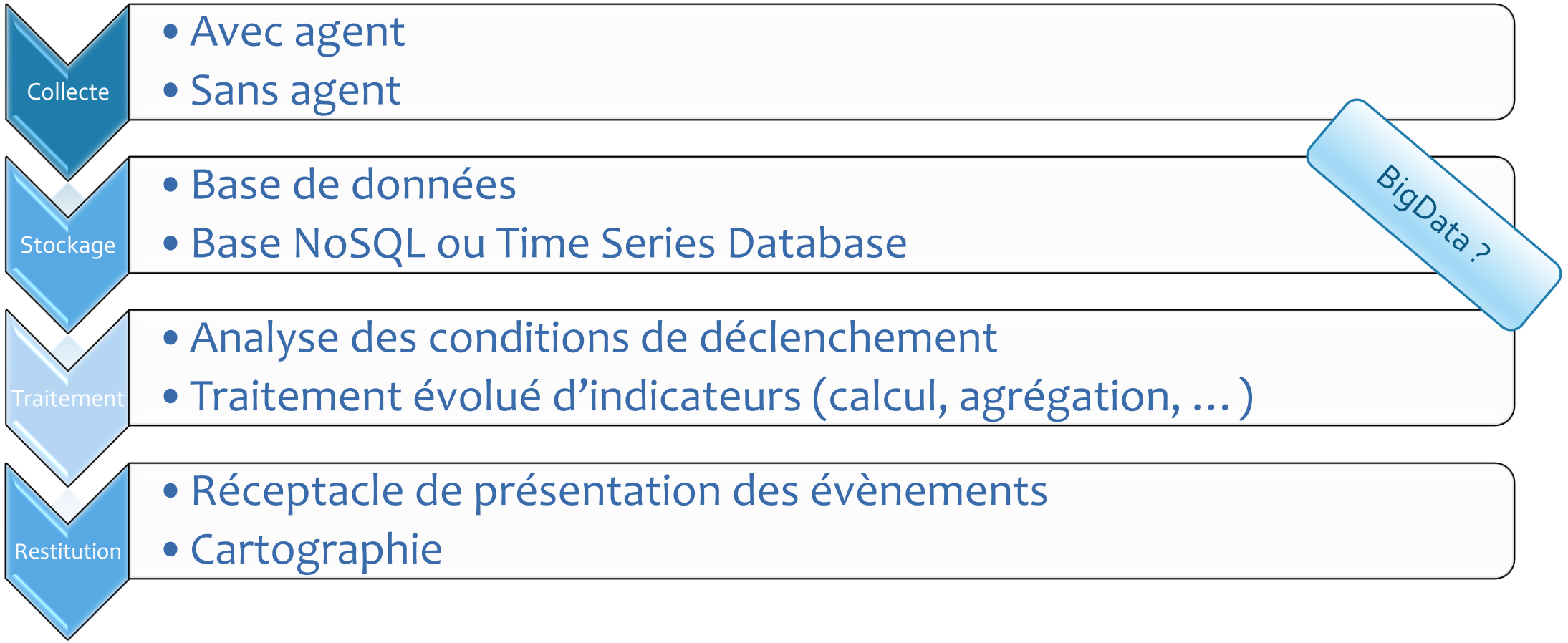
1. Etre alerté en cas de dysfonctionnement
   i. Alerte en cas de défaillance d'un service ou d'un composant
   ii. Alerte en cas de dépassement de capacité

2. Obtenir des informations proche du temps réel pour diagnostic **à chaud**
   i. Compléter le diagnostic une fois que l'on a été alerté
   ii. Consultation des indicateurs en temps proche du réel
   iii. Indicateurs à échantillonnage fin et stocker faiblement dans le temps

1. Prendre le temps d'effectuer un diagnostic **à froid**
   I. Analyse de journaux
   II. Compréhension du contexte et de analyse de la reproductibilité

2. Suivre des indicateurs dans le temps
   i. Analyse des tendances
   ii. Anticipation des saturations

Rapprochement avec le décisionnel



Le buzz

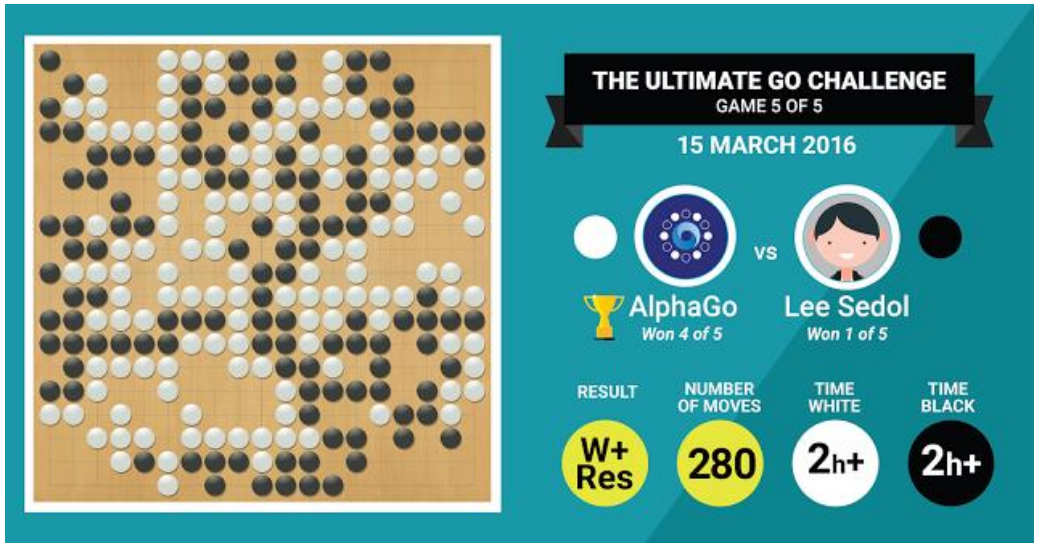
- Avec les aspects « BigData », que « markette » t-on ?

1. La surveillance comportementale
2. L'auto-apprentissage ou le « Machine Learning »

Rétrospective du combat entre l'homme et la machine

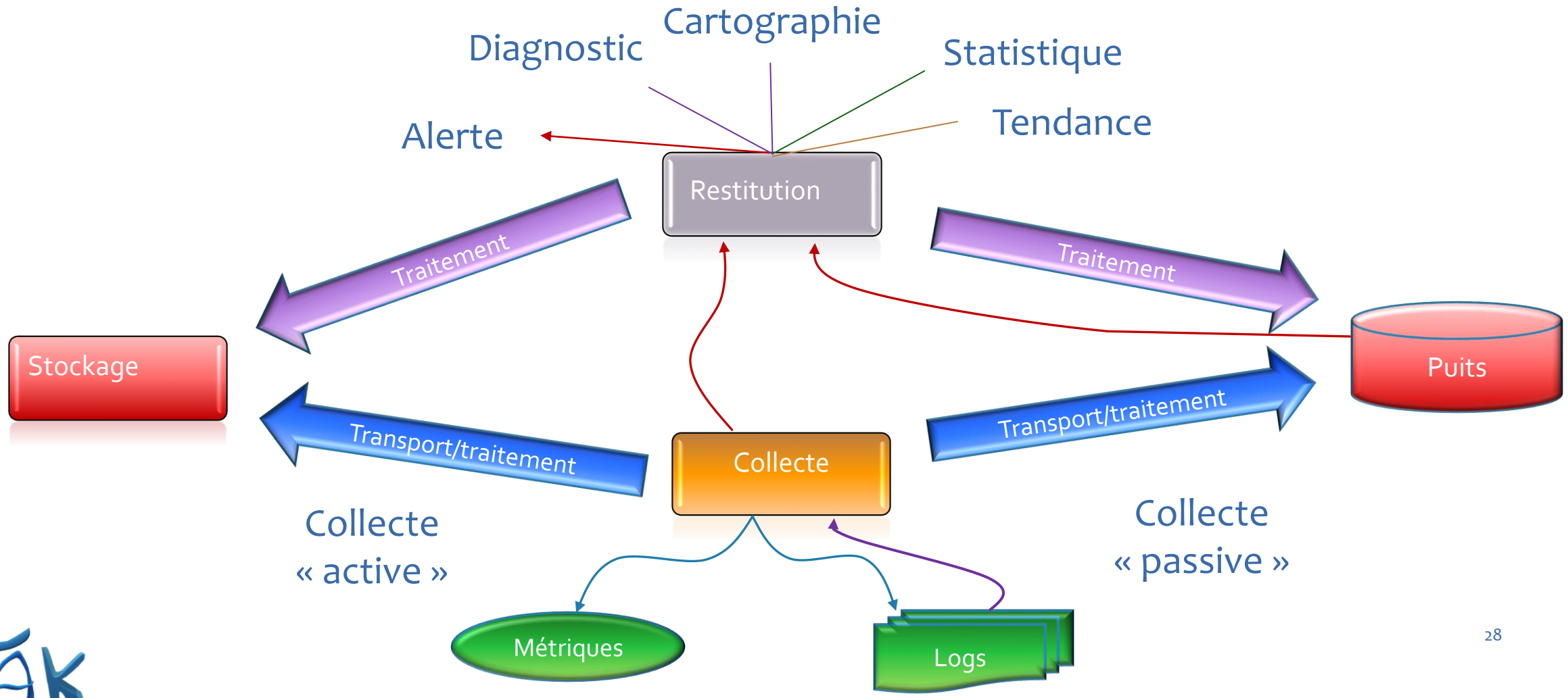
- 1952 le jeu du morpion (tic-tac-toe)
- 1992 le jeu de Backgammon
- 1994 le jeu de dames
- 1997 le jeu d'échecs (par Deep Blue de IBM)
- 2001 le jeu Jeopardy (par Watson de IBM)
- …

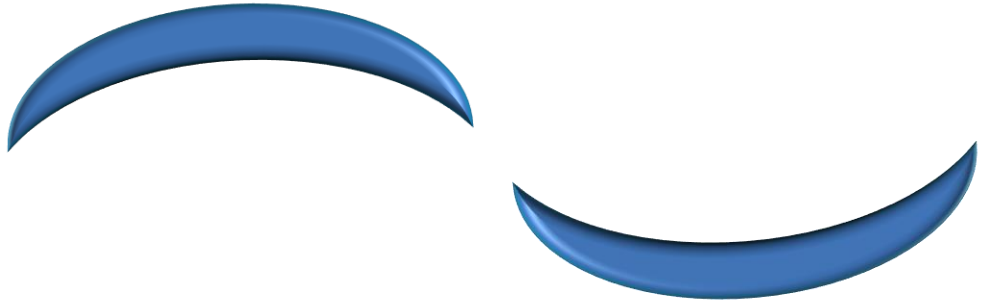
Le Go



- Heureusement, il reste le poker ;-)
  … et quelques autres !

Synthèse

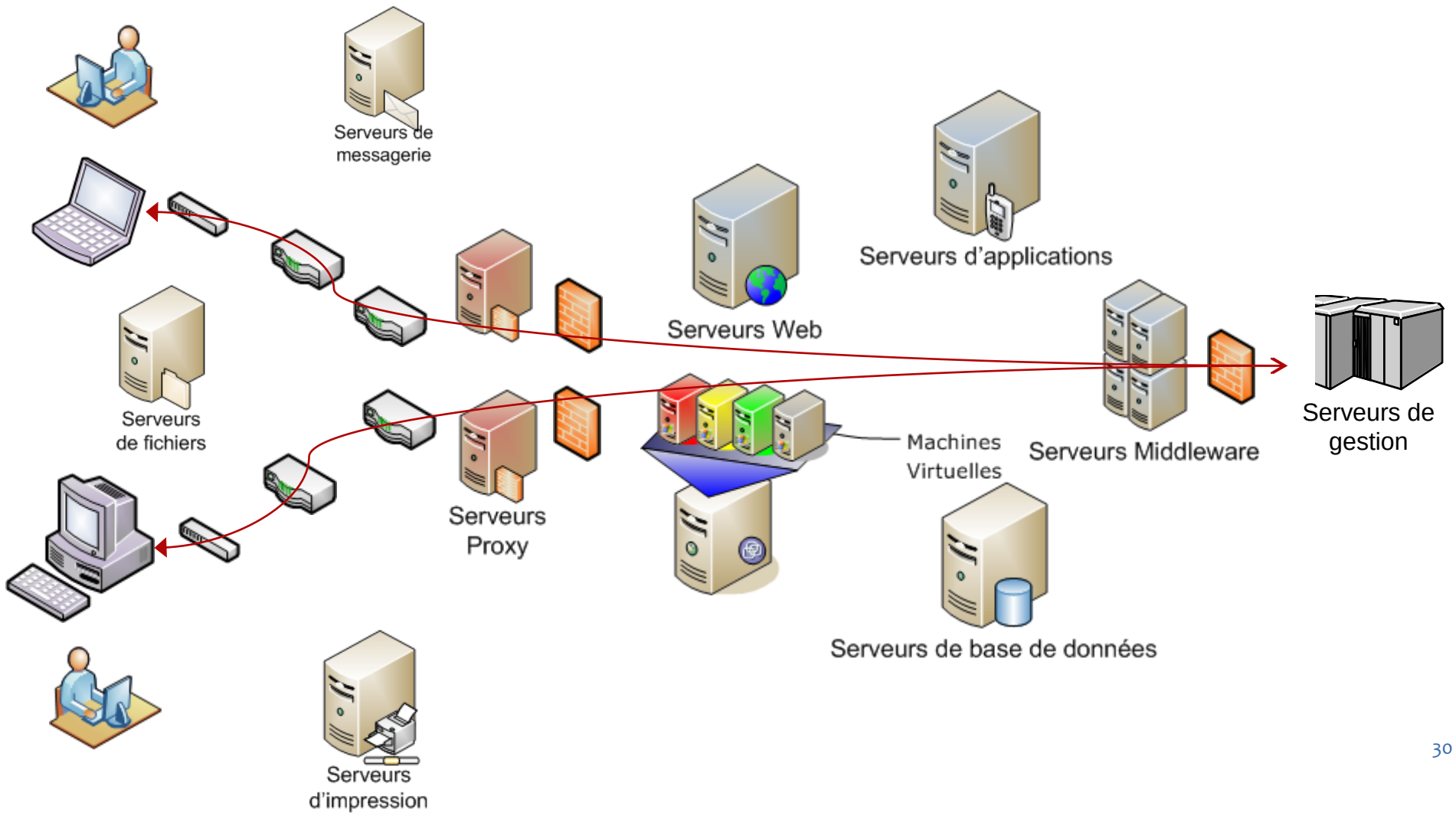

Diagnostic
Cartographie
Statistique
Alerte
Tendance
Restitution
Traitement
Traitement
Stockage
Puits
Transport/traitement
Transport/traitement
Collecte
Collecte
« active »
Collecte
« passive »
Métriques
Logs



Périmètre

Les panoramas de la supervision

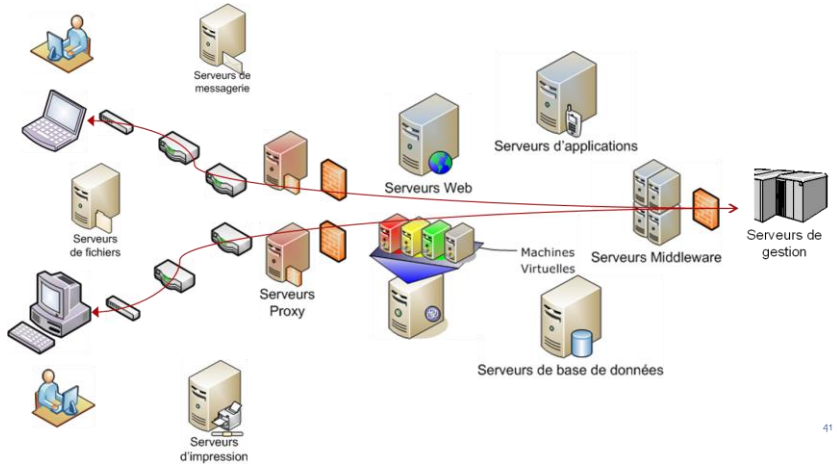
Le système d'informations



Les différentes spécificités

- Quelle est la cible de notre supervision ?
  - Le système d'informations, un élément de l'entreprise très vaste.

- Le système d'informations se décline en différentes spécificités :
  - Le réseau
  - Les systèmes d'exploitation
  - Le matériel
  - Les socles logiciels (IIS, apache, Oracle, DB2, …)
  - Les progiciels (logiciels vendus par un éditeur)
  - Les logiciels (applications propriétaires et/ou métiers)
  - La sécurité
  - Les utilisateurs
  - Le SAN, la virtualisation
  - La ToIP/VoIP,
  - Les services rendus
  - …



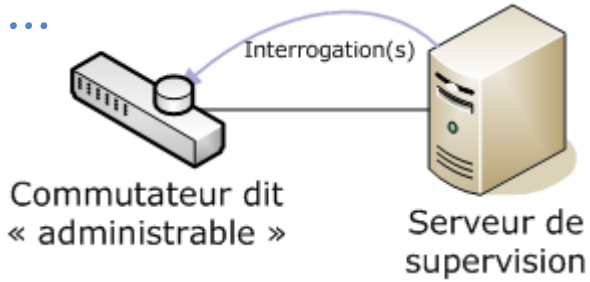
La terminologie

- Plusieurs types de supervision, plusieurs terminologies :
  - Périmètre et spécialisation
    - La supervision réseau
    - La supervision système
    - La supervision de la sécurité
    - La supervision applicative
    - La supervision métier
  - Technique
    - La supervision active
    - La supervision passive
    - La supervision locale
    - La supervision distante
    - La supervision de bout-en-bout
  - BigData… ou pas
    - La supervision comportementale
    - Le machine Learning

ICMP
SNMP

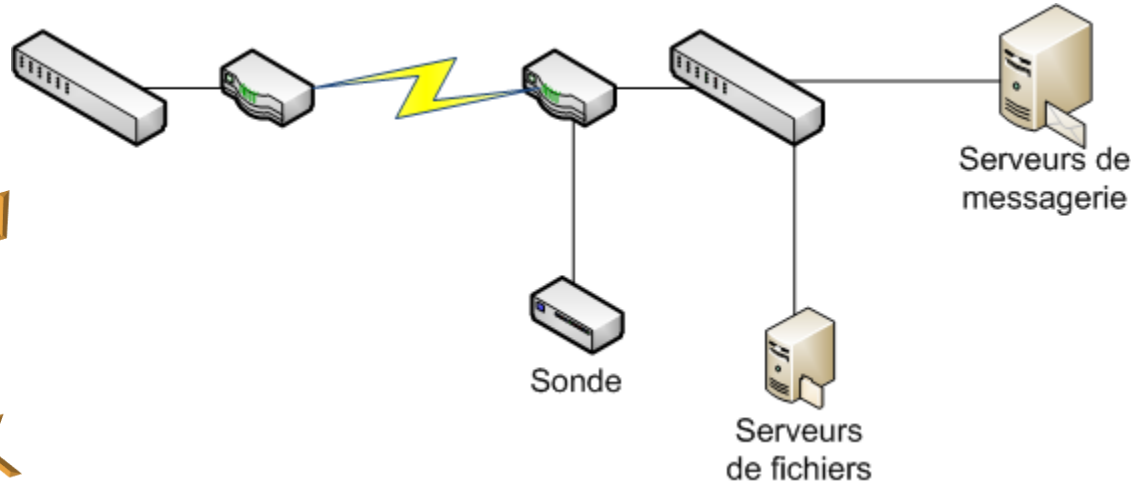
La supervision réseau

- Supervision des équipements sur le réseau
  - Historiquement basé sur le concept de supervision agent/manager, via des protocoles comme CMIS/CMIP, SNMP, …



Actif

  - Mais également sous forme de mécanisme de sonde



Passif

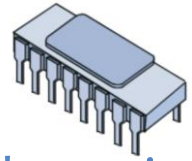
NetFlow
Sflow
IPFIX

UTAK

La supervision système

- Contrôle des fonctions du système d'exploitation et des services qu'il rend
  - Soit on reste basé sur la supervision vue précédemment (vision « réseau » du système d'exploitation et des services rendus), soit on veut contrôler :

    - des journaux,
    - des processus,
    - les ressources du système d'exploitation (CPU, mémoire, zone de pagination, tables système, …)
    - les espaces disques, …

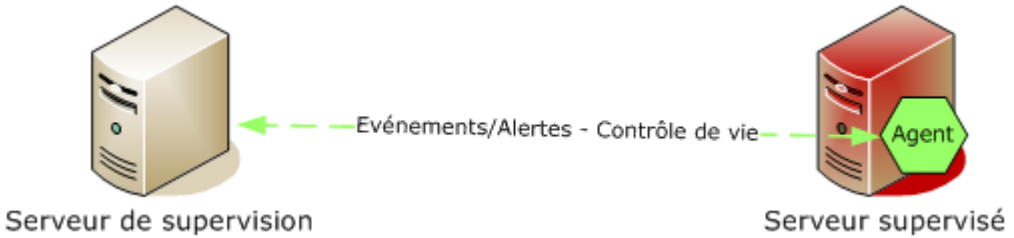


  - Voire, on souhaite pouvoir agir en tentant de corriger l'anomalie lors de sa détection.
    - On entends parfois le terme « remédiation »

La supervision système

- 2 possibilités :
  - La surveillance avec un agent installé sur le système d'exploitation à surveiller

Agent



Protocoles propriétaires

  - La surveillance sans agent (« agentless »)

Agentless

ssh, wbem, snmp, …

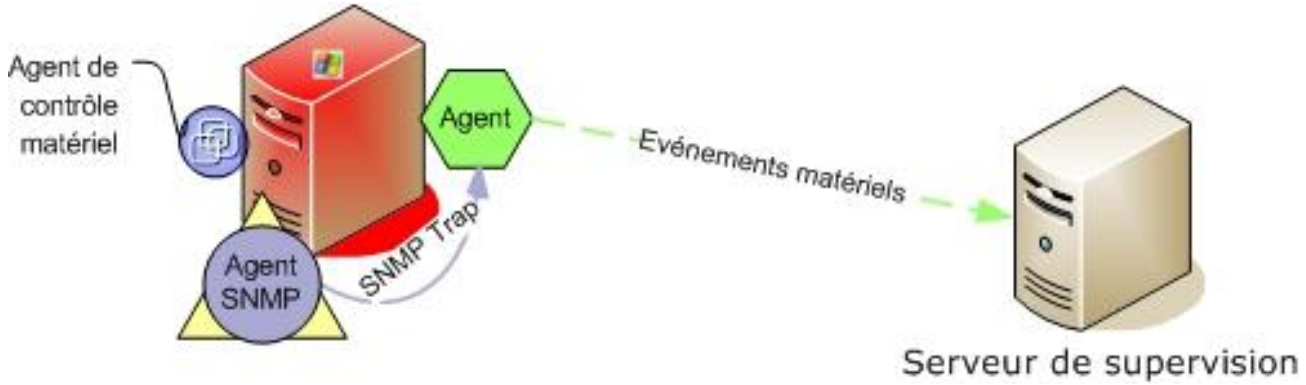
La supervision système

- Celle introduit obligatoirement une notion spécifique :
  - L'instrumentation, c'est-à-dire l'ensemble des scripts et exécutables qui vont permettre d'effectuer les contrôles souhaités
    - En fonction des solutions, l'instrumentation est plus ou moins importante
      - ✓ Exemple : Nagios, sans ses plugins n'est rien
  - Celle-ci sera à classer en fonction des différents systèmes d'exploitation cibles
    - Donc, plus on peut s'en passer, mieux cela sera

La supervision matérielle

- Détection de panne matérielle :
  - Désactivation de la redondance électrique
  - Barrette mémoire défectueuse
  - Disque défectueux
  - Ventilateurs HS
  - Température trop importante
  - …

IPMI



La supervision des applications

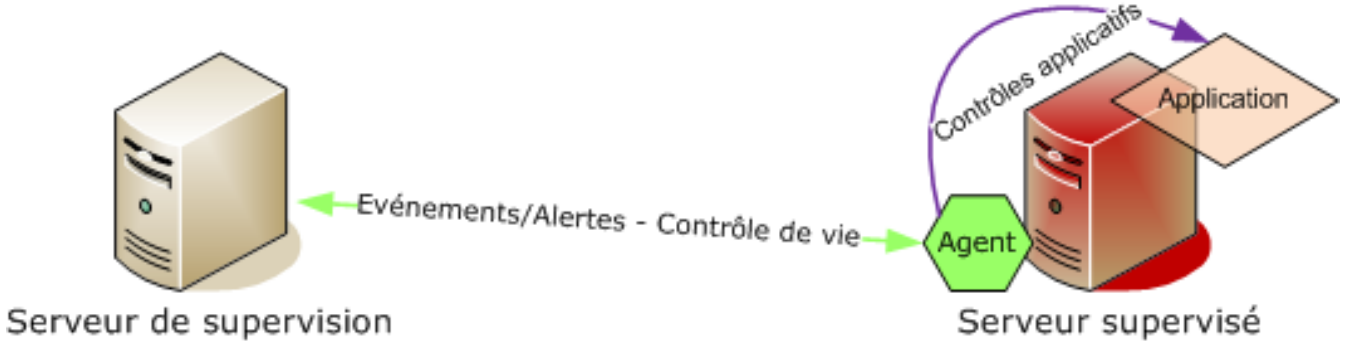
- On définit par application :
  - Les socles logiciels ;
  - Les progiciels ;
  - Les logiciels.

- La supervision de l'infrastructure d'une application consiste également à surveiller :
  - Les journaux techniques ;
  - Les processus ;
  - La présence ou l'absence de fichiers ou de données ;
  - La consultation des indicateurs fournis par l'application elle-même.

La supervision des applications

- 2 possibilités :
  - La surveillance avec un agent installé sur le système d'exploitation où est installée l'application à surveiller

Protocoles propriétaires



  - La surveillance sans agent (« agentless »)

sql, http(s), [rmi], …

La supervision de la sécurité

- Une supervision parfois à part :
  - Contraintes classiques :
    - Pas d'accès ICMP ;
    - Pas d'accès SNMP ou seulement v3 ;
    - Seuls les mécanismes de type « syslog » sont tolérés ;
    - Protocole de contrôle et de journalisation propriétaire à la solution de sécurisation.
  - Frontières parfois floues :
    - Reverse Proxy
    - Répartiteur de charge
    - Serveur d'anti-virus
    - …

Supervision active

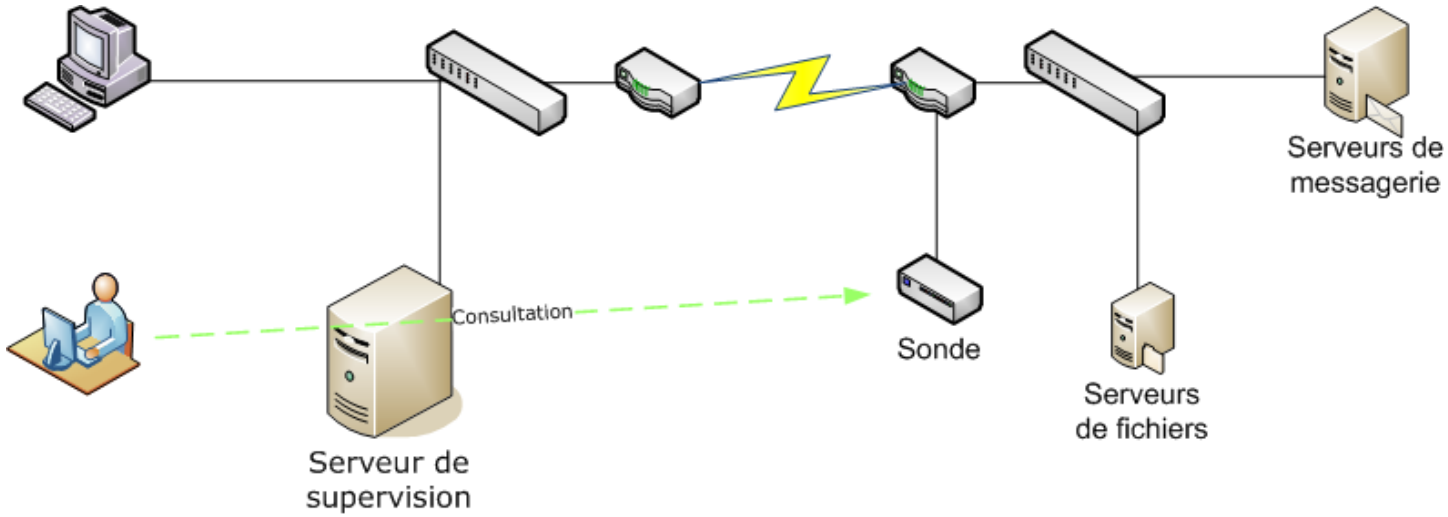
- Supervision active (qualifiée intrusive) : la solution de supervision va puiser l'information là où elle est présente
  - impacte obligatoirement le système supervisé

Dans cet exemple, l'agent installé sur le serveur supervisé aura un impact permanent sur ses ressources :

- CPU, mémoire, …

Supervision passive

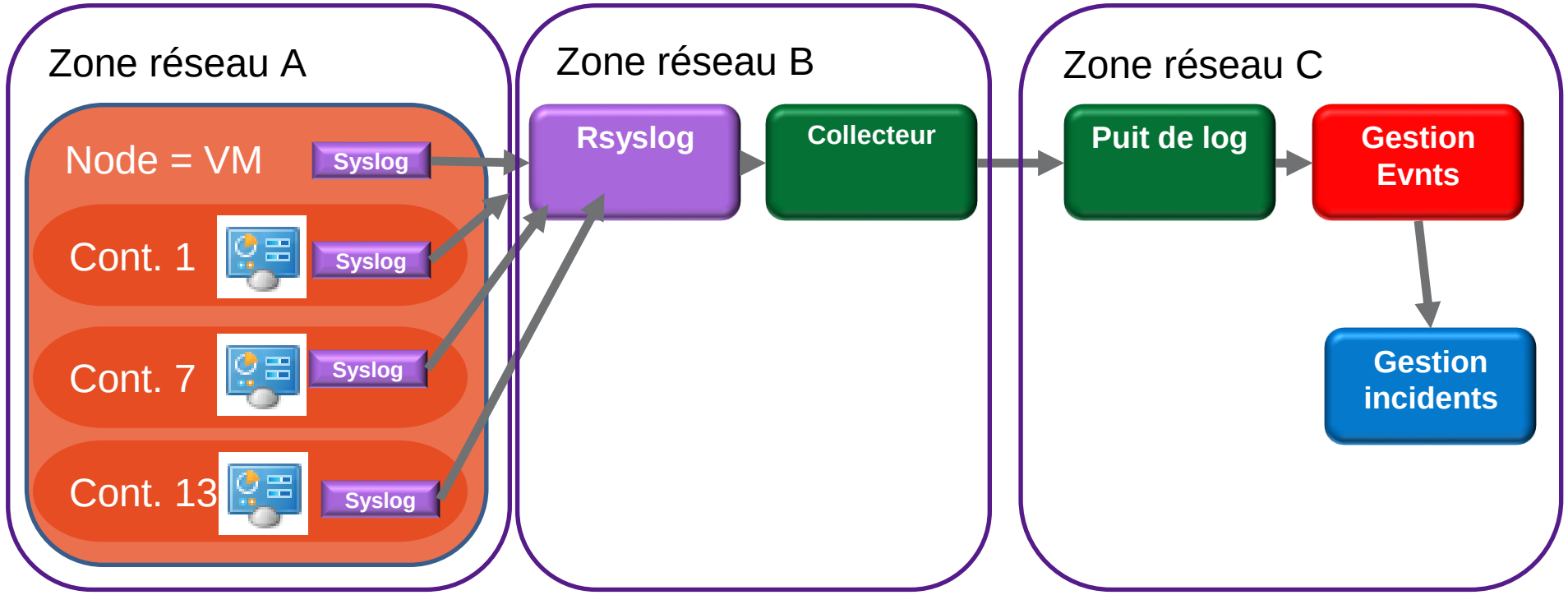
- Supervision passive (qualifiée moins intrusive) : l'information vient à la supervision
  - impacte moins (voire peu ou pas) le système supervisé



Cette supervision est basée sur des sondes, elles-mêmes positionnées sur des réseaux TAP, voire des ports SPAN.

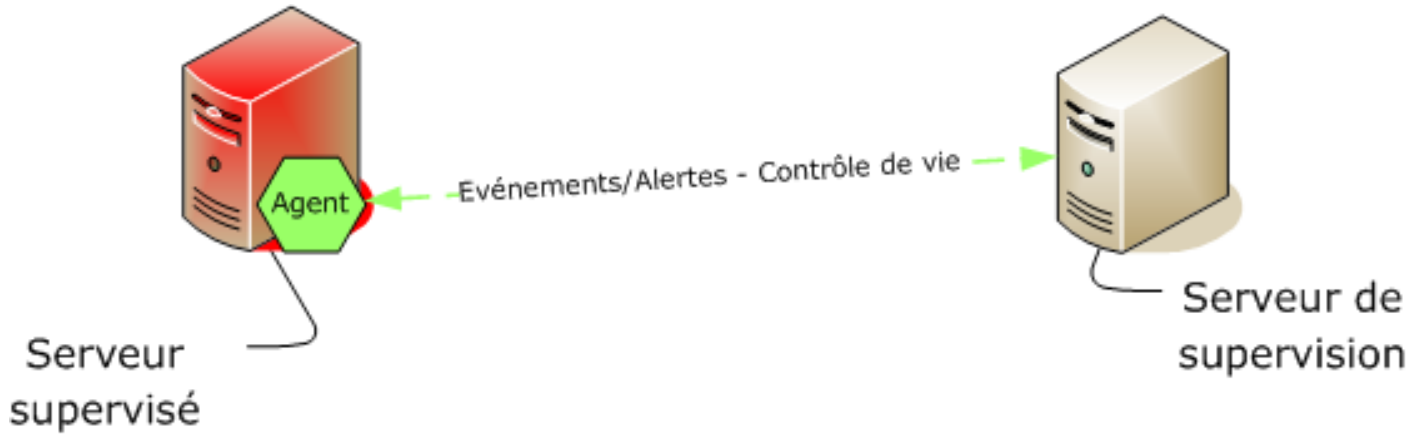
Supervision passive

- Un second exemple très actuel



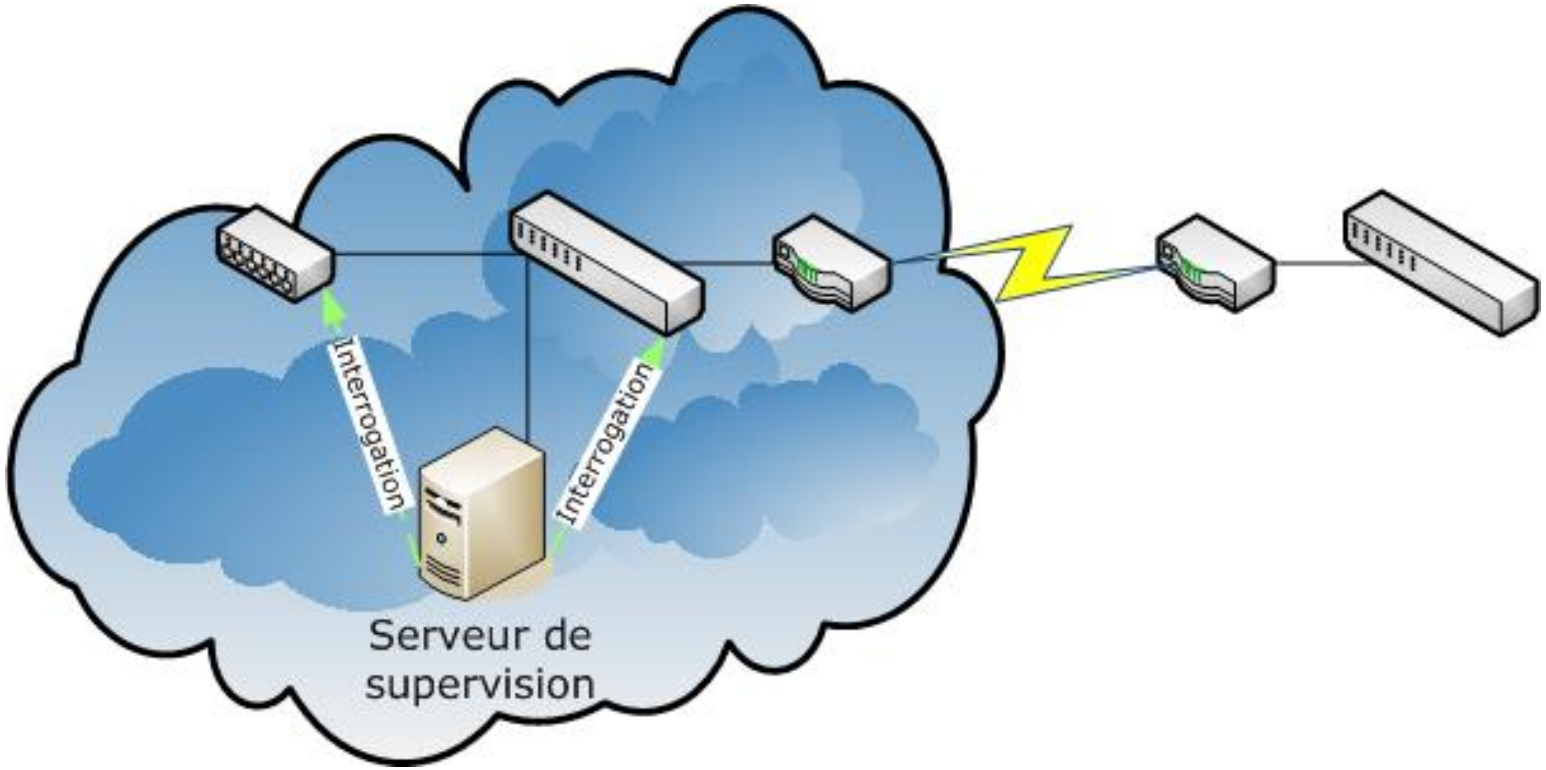
Supervision locale

- Supervision système ou applicative
  - présence d'un agent installé sur le système d'exploitation ou sur le système applicatif ;



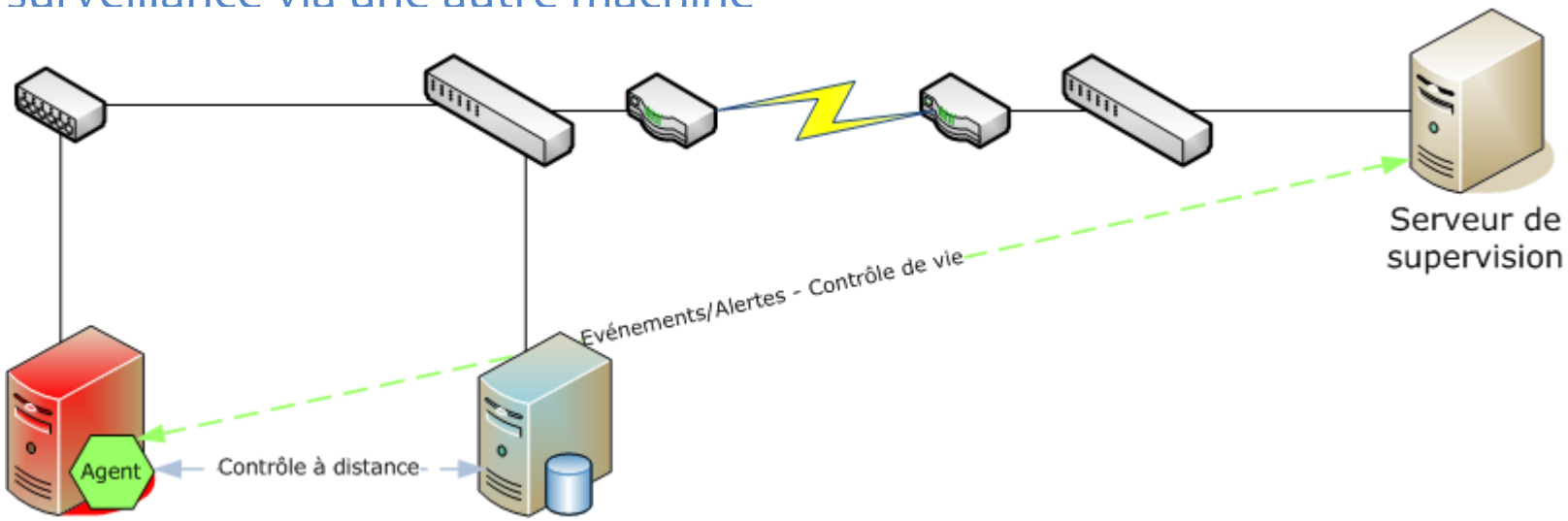
Supervision locale

- Supervision réseau
  - les contrôles sont faits sur un LAN



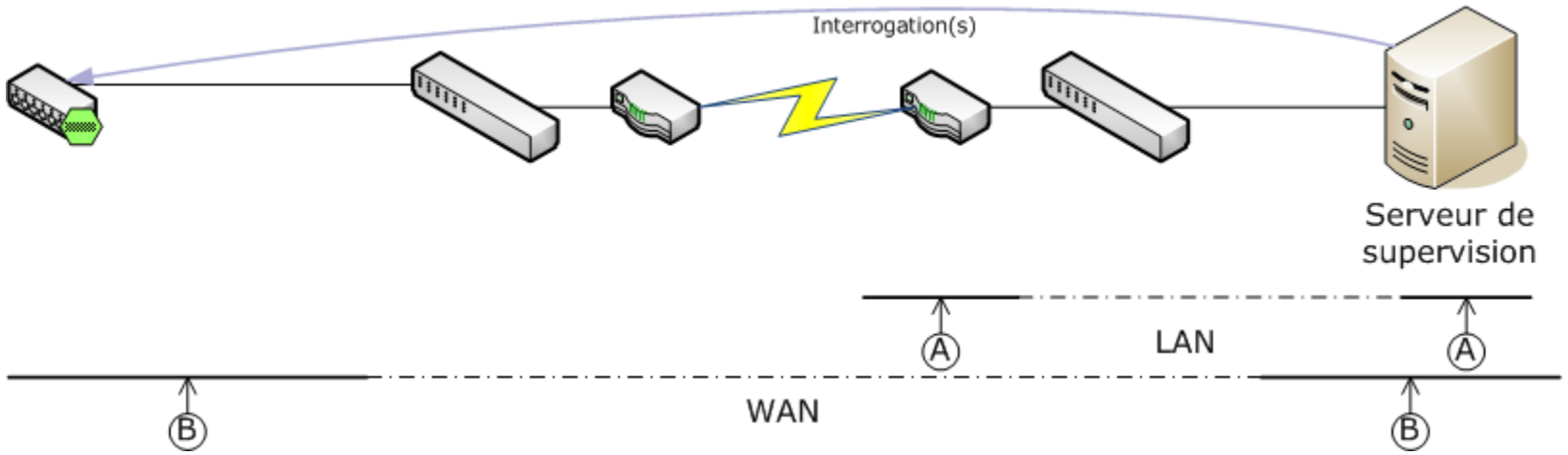
Supervision distante

- Supervision système ou applicative
  - Interrogation à distance de la cible
  - surveillance via une autre machine



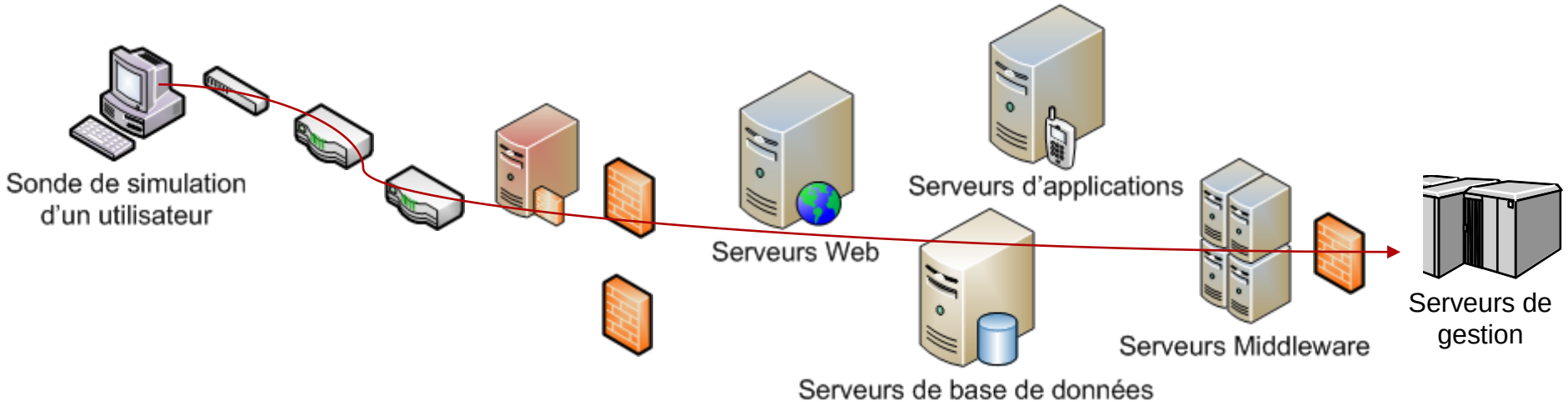
Supervision distante

- Supervision réseau
  - Les contrôles sont faits au travers du réseau WAN



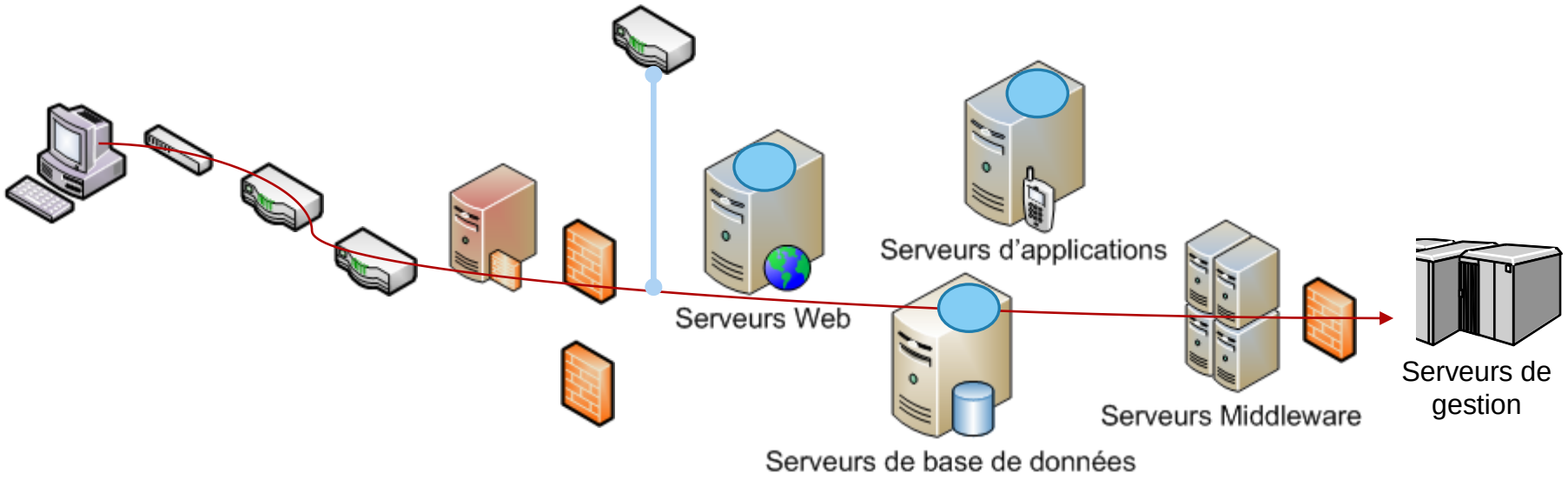
La supervision de bout-en-bout

- … ou end-to-end, voire du « ressenti utilisateur »
  - Quelle que soit l'infrastructure en place, on contrôle la disponibilité et la dégradation des performances d'un service informatique en simulant ou en écoutant des connexions utilisateurs.



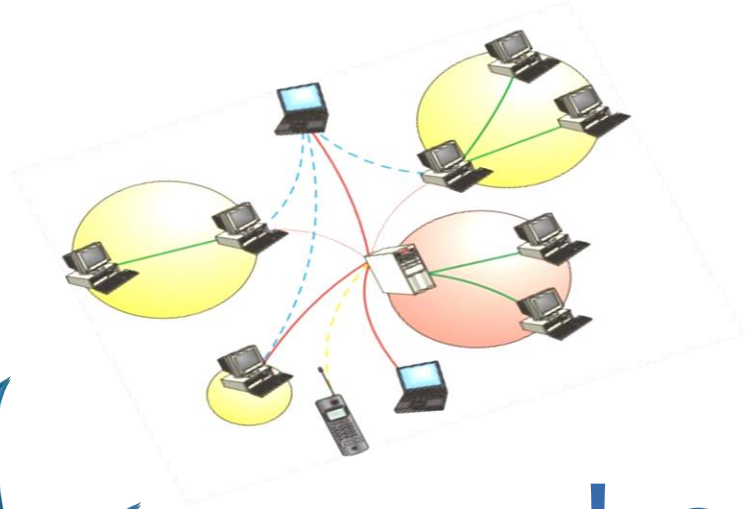
Avec en évolution…

- L'APM pour Application Performance Management



Quelques questions subsistent…

- Que choisir ?
- Quelle priorité mettre ?
- Faut il un seul outil généraliste ou une multitude d'outils ?
- Faut il une solution toute faite ou une boite à outils ?
- Comment exploiter et administrer cette solution de manière pérenne ?
- Tout dépendra de votre périmètre, de votre organisation, de votre budget pour élaborer le projet



Les panoramas de la supervision

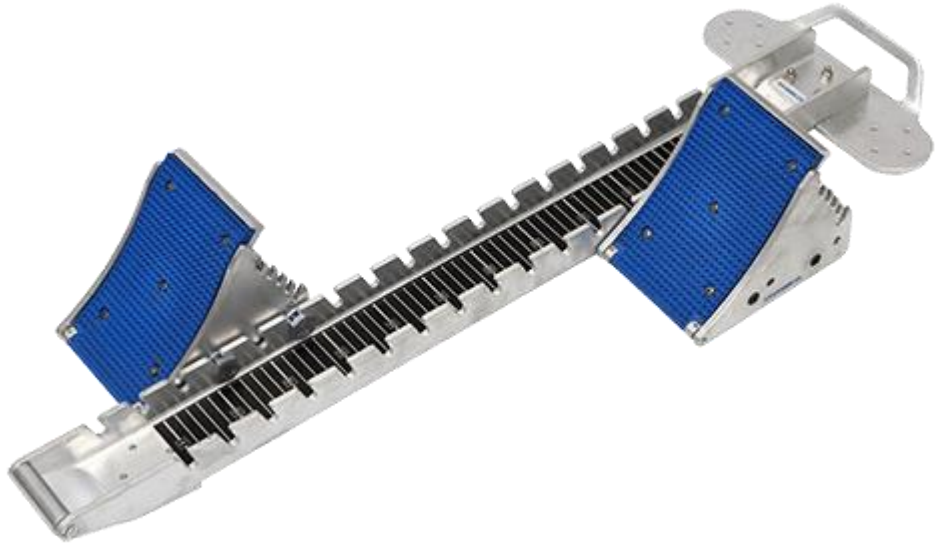
La supervision réseau

Les origines de la communication

-35000 ?	?	Langage parlé
~ -3300	Sumériens	Ecriture cunéiforme
?	?	Pigeons voyageurs
?	Amérindiens	Signaux de fumées
1843	Code de Morse	Télégraphe
1875	Bell & Gray	Téléphone
1895	Marconi	Radio
1943	Angleterre	Ordinateur Collossus
1948	Bell Labs	Transistor
1969		Réseau ARPANET (4 ordi. reliés)
1972	Ray Tomlinson	Messagerie sur ARPANET
1973	Xerox Intel Dec	Ethernet
1976	CCITT / IBM / Bull	Norme X25, SNA, DSA
1978	DGT / CCITT	Transpac / Modèle OSI (7 couches)
1980	Vinton Cerf	Interconnexion ARPANET CSNET
1982	CCITT	ARPANET sous TCP/IP

Supervision… les débuts

- 1987 : Le démarrage
  - La supervision réseau et quelques protocoles : ICMP et la dualité CMIS/CMIP & SNMP
- 2 notions
  1. La supervision réseau : surveillance des équipements réseaux fédérée en un point.
  2. L'administration réseau : gestion de la configuration des équipements réseaux fédérée en un point.



ICMP

- Internet Control Message Protocol

```
~$ ping obelix01
PING obelix01 (54.37.156.175) 56(84) bytes of data.
64 bytes from obelix01 (54.37.156.175): icmp_seq=1 ttl=57 time=0.302 ms
64 bytes from obelix01 (54.37.156.175): icmp_seq=2 ttl=57 time=0.348 ms
64 bytes from obelix01 (54.37.156.175): icmp_seq=3 ttl=57 time=0.314 ms
64 bytes from obelix01 (54.37.156.175): icmp_seq=4 ttl=57 time=0.353 ms
^C
--- obelix01 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.302/0.329/0.353/0.025 ms
```

Travaux

1. Recherche sur tous ce que l'on peut faire à base de « ping » ou du protocole « icmp »
2. Recherche d'outils, de package autour de ce protocole
    1. Exemples : fping

        - http://igm.univ-mlv.fr/~dr/XPOSE2010/IPSLA/presentation.html

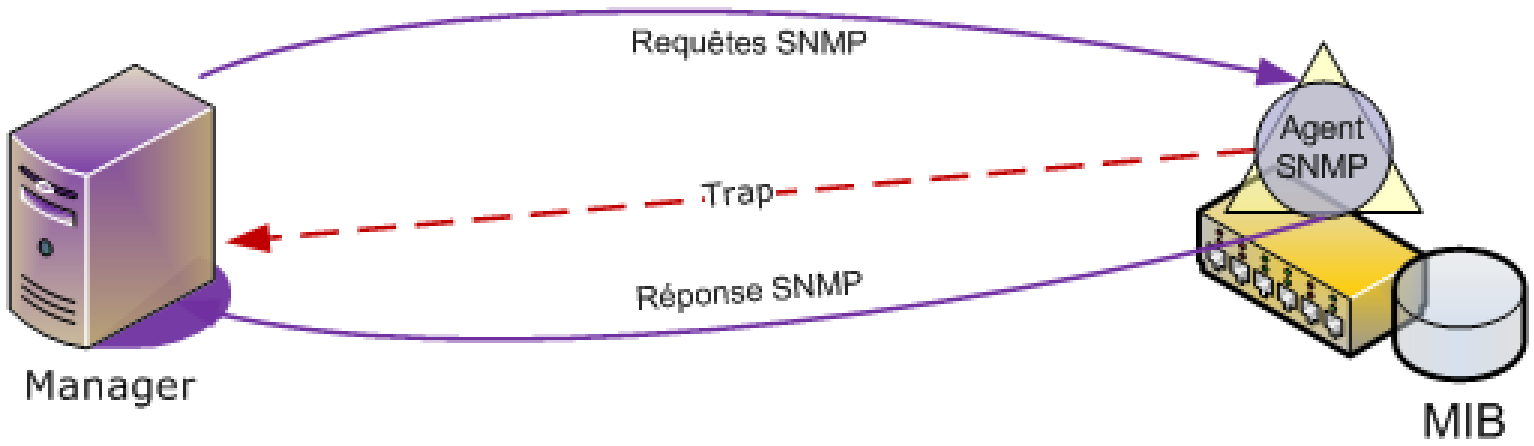
Histoire… les premiers acteurs

- 3 solutions phares :
  - SNMP
    - SUN Microsystems avec Sunnet Manager ;
    - Hewlett-Packard avec HP OpenView ;
  - CMIS/CMIP
    - BULL avec ISM (Integrated System Management)

- Rapidement, la solution de Bull s'aligna sur la couverture du protocole SNMP

La supervision SNMP

- Elle est basée sur un protocole de communication dédié entre le point central (appelé manager) et les équipements réseaux (appelé agent) :
  - SNMP : Simple Network Management Protocol



La MIB

- Management Information Base

Les numéros des entreprises sont données dans le RFC 1700

Les versions du protocole SNMP

- SNMP V1 (1987)
  - la plus connue des versions et surtout la plus répandue au niveau des équipements réseaux
- SNMP V2 (1992)
  - Amélioration de la sécurité, la lecture groupée de variable, …
  - Quelques versions intermédiaires :
    1. V2P : première mise à jour de SNMP v1
    2. V2C : Nouvelles fonctionnalités, mais peu sûres
    3. V2U : Ajout de l'authentification
    4. V2 : Meilleures parties de V2P et V2U
  - Version peu suivie par les équipementiers
- SNMP V3 (2002)
  - Une version compatible avec la sécurité qui est devenu le standard en 2002. Pourtant, celle-ci est encore faiblement utilisée

SNMP simple ?

- Simple car 6 opérations :
  - Get : aller chercher un OID
  - GetNext : aller chercher une suite d'OID
  - Set : valoriser un OID
  - Trap : alerte SNMP
  - GetBulk : aller chercher massivement un ensemble d'OID
  - Inform : relai d'un OID d'un serveur de management SNMP à un autre

SNMP complexe ?

- Complexe, car beaucoup de MIB, beaucoup d'indicateurs
- Aller chercher l'OID d'un routeur Cisco 2801 pour obtenir son numéro de série
- www.oidview.com/mibs
- Utilitaire Windows/Linux des commandes de requêtes SNMP => netsnmp
- Site de fourniture de MIB :
- Recherche de « Browser » de MIB : tkmib, qtmib, snmpb, …
- Topologie réseau et protocole de découverte réseau
  - FDB (Forwarding DataBase)
  - Propriétaire : CDP (Cisco Discovery Protocol), EDP (Extreme DP), …
  - Normalisation : LLDP (Link Layer Discovery Protocol)