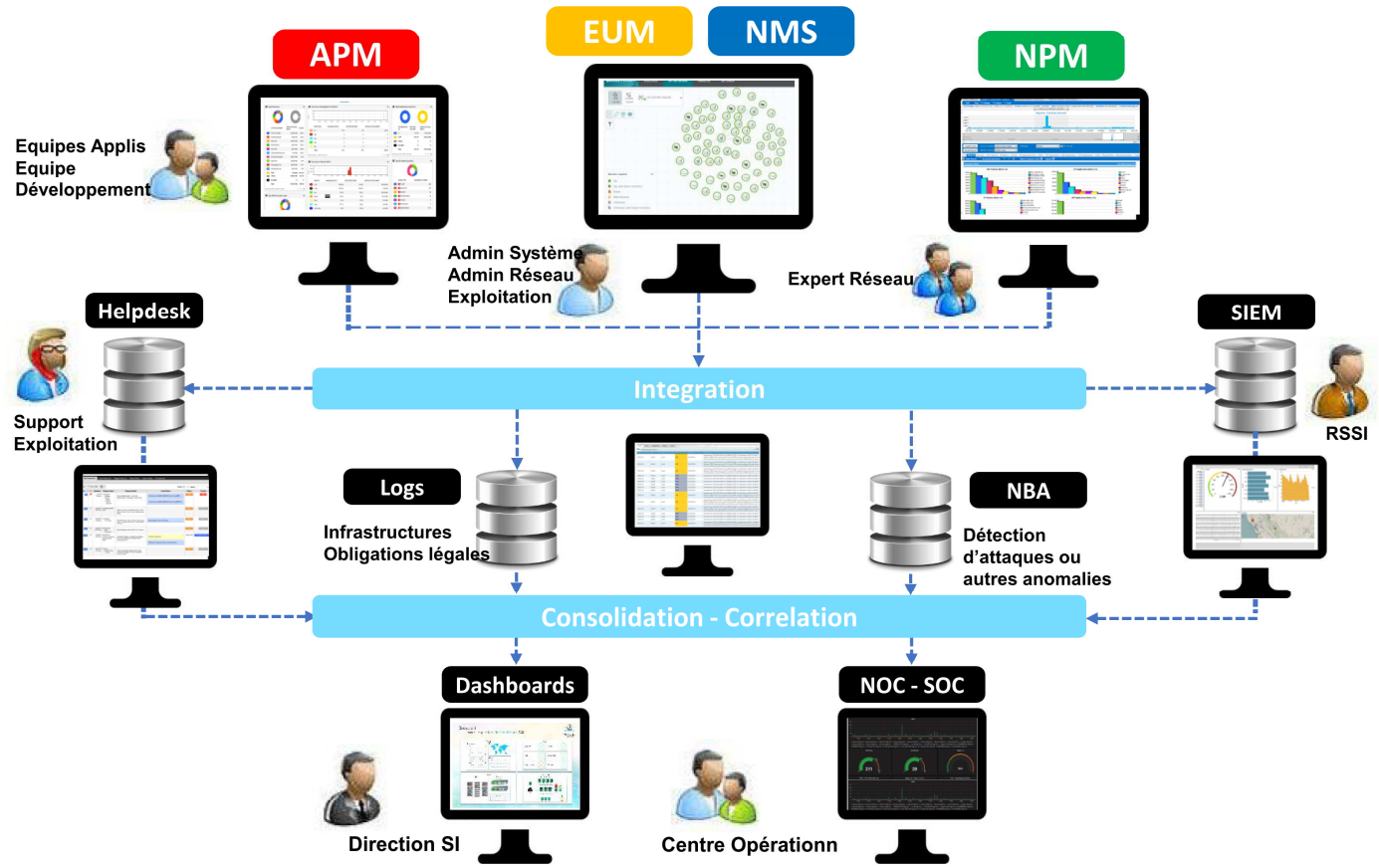
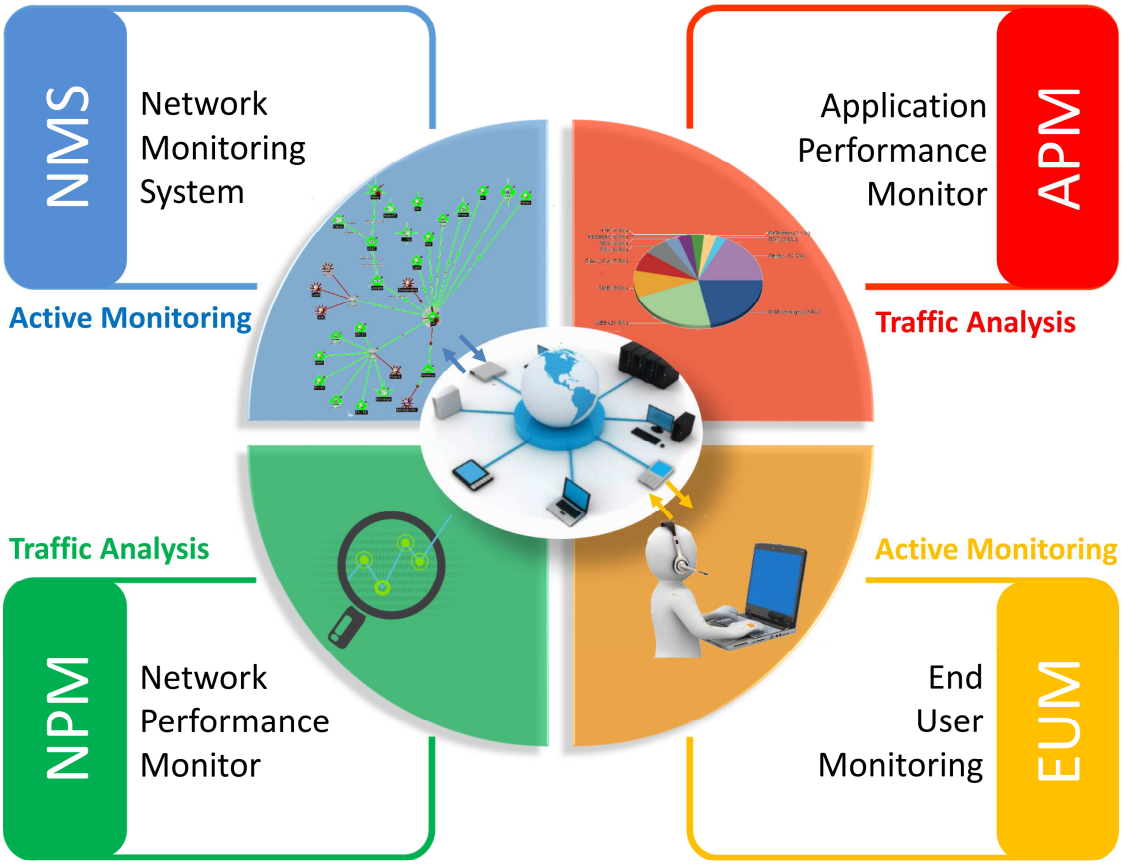
Présentation Générale

Supervision

Offre NMC - Cockpit Supervision IT



Marques et solutions distribuées



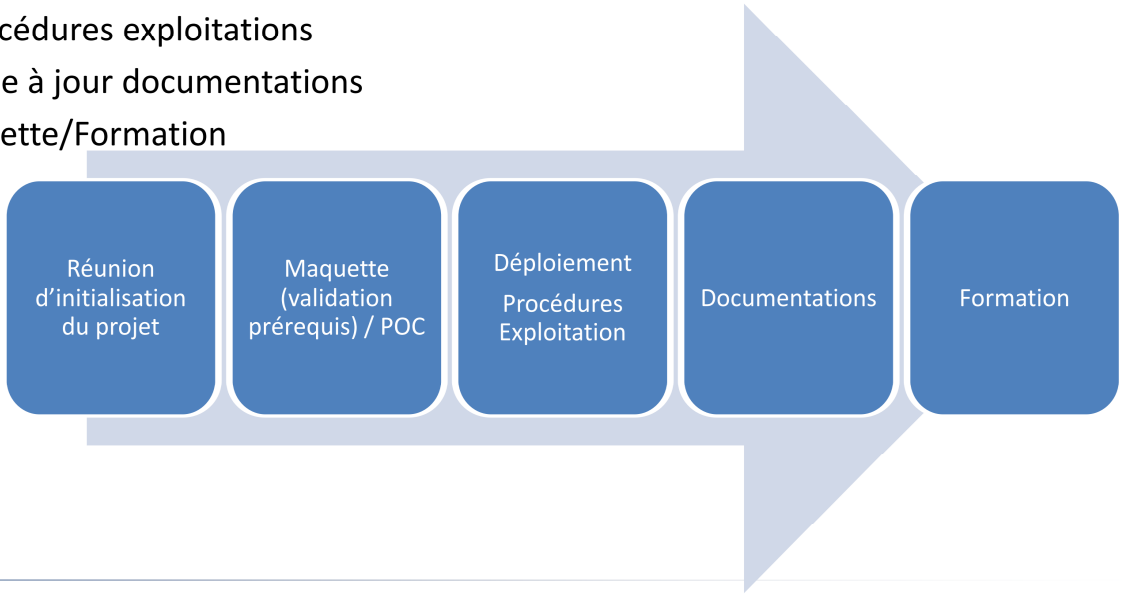
ORSENNA NMS SERVICES

IPSWITCH WhatsUpGold

Mise en œuvre d'un projet supervision

Mise en œuvre d'un projet supervision

- Audit initial,
- Spécifications détaillées & Architecture
- Maquette/POC : Mise en œuvre pré requis
- Déploiement
- Procédures exploitations
- Mise à jour documentations
- Recette/Formation



Audit Initial - Objectifs

– Existence de multiples outils au sein de l'entreprise
  - Outils Constructeurs (CiscoWorks, OpenManage, …)
  - Console Supervision basique (Nagios, WhatsUp V8, …)

– Existence de périmètres distincts dans l'entreprise
  - Infrastructure, Serveurs , Applications, Virtualisation

– Stratégie d'évolution à définir :
  - Migration vers un outil unique d'entreprise.
  - Consolidation des outils existants.
  - Mixte

Audit Initial – Nature du projet

Moyen mis en oeuvre : 1 personne
Processus simple
Outils personnels

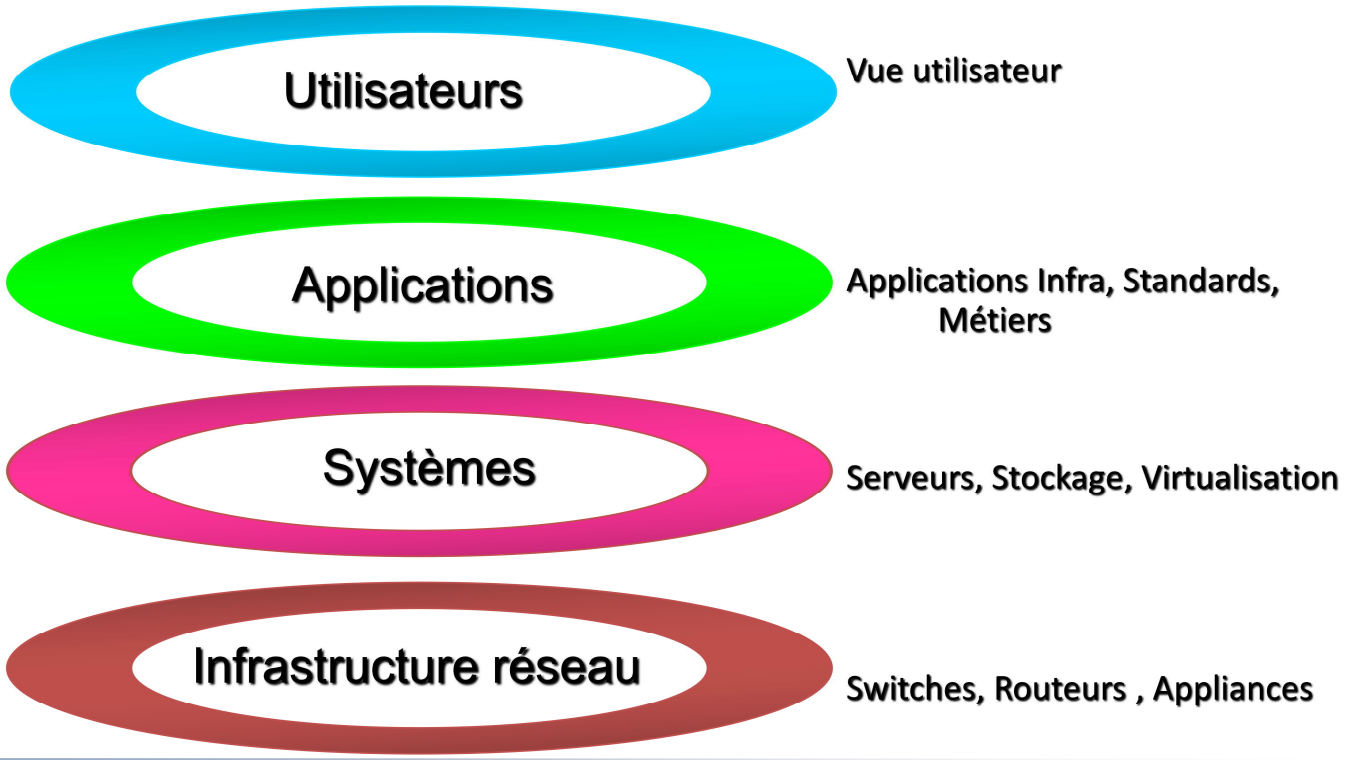
Audit Initial – Nature du projet

Moyens: Equipe professionnel
Plan préalable
Processus + complexe
Outils professionnels

Audit Initial - Objectifs

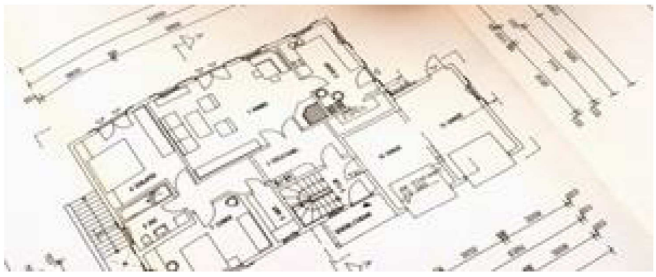
- Axes à définir :
  - Surveillance pro active
    - → Alertes simples à mettre en place
  - Diagnostic et résolution de problèmes
    - → Liens avec les outils existants
  - Statistiques de la qualité de service
    - → Aspect rapports et base de données
  - Collecte et mesure de performances
    - → Volumétrie de la collecte

Audit Initial - Périmètre



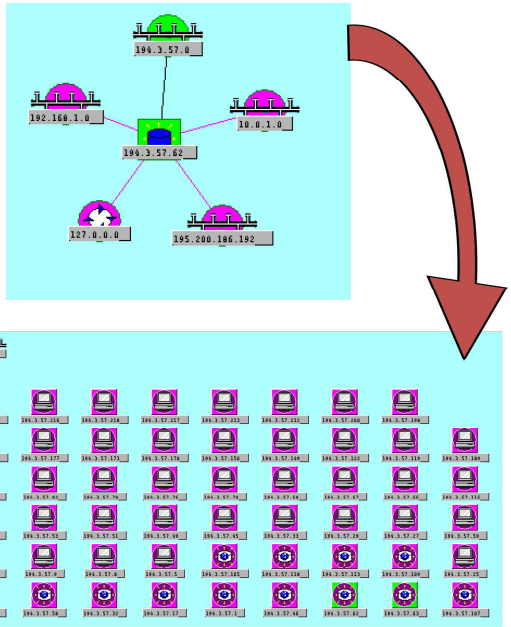
Spécifications & Architecture

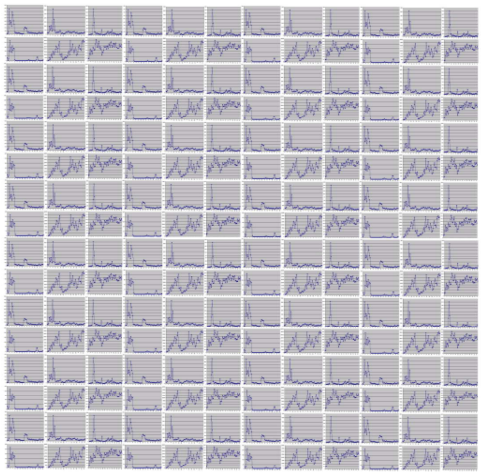
- Afin de respecter les objectifs



Spécifications & Architecture

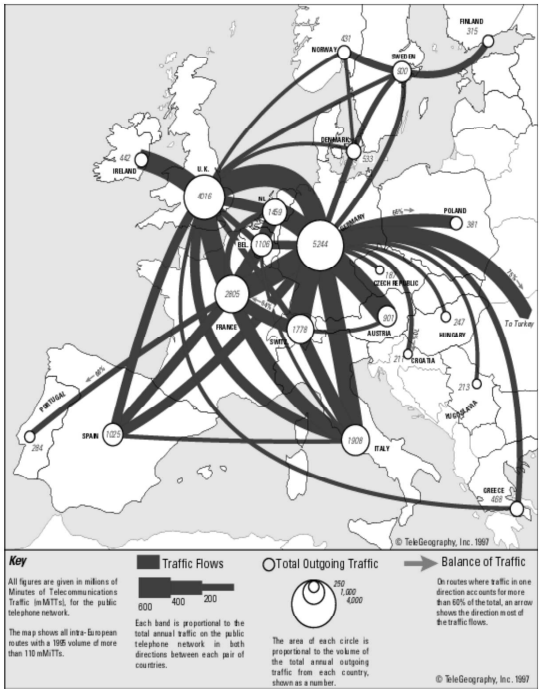
- Pour éviter des collectes inutiles de données

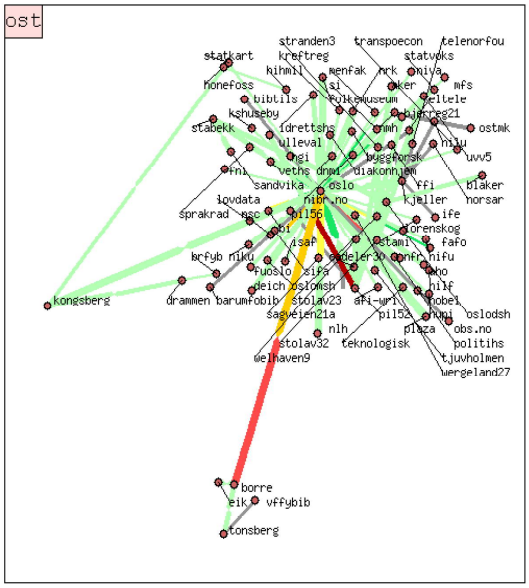




Spécifications & Architecture

- Pour éviter une cartographie inexploitable





Maquette/POC

- Mise en œuvre prérequis
- Périmètre initial
  - Infrastructure réseau
  - Systèmes
  - Applicatifs
  - Transaction utilisateur
- Cartographie, Web
- Gestion des événements & des alertes
- Diagnostics/ Rapports

Mise en œuvre

- Synthèse des documents existants
- Pour chaque type de composant :
  - Accessibilité SNMP, IP, SSH, WMI,…
  - Possibilité Syslog, Netflow, IP SLA
  - Outils spécifiques disponibles (Outils constructeurs)
  - Criticité du composant
  - Descriptif des états et évènements à gérer (Service NT, Etat interface 1 ,..)
  - Descriptif rapide des procédures de diagnostic et de dépannage (Appel astreinte,..)

Périmètre Infrastructure Réseau

- Routeurs

- Firewall

- Switchs

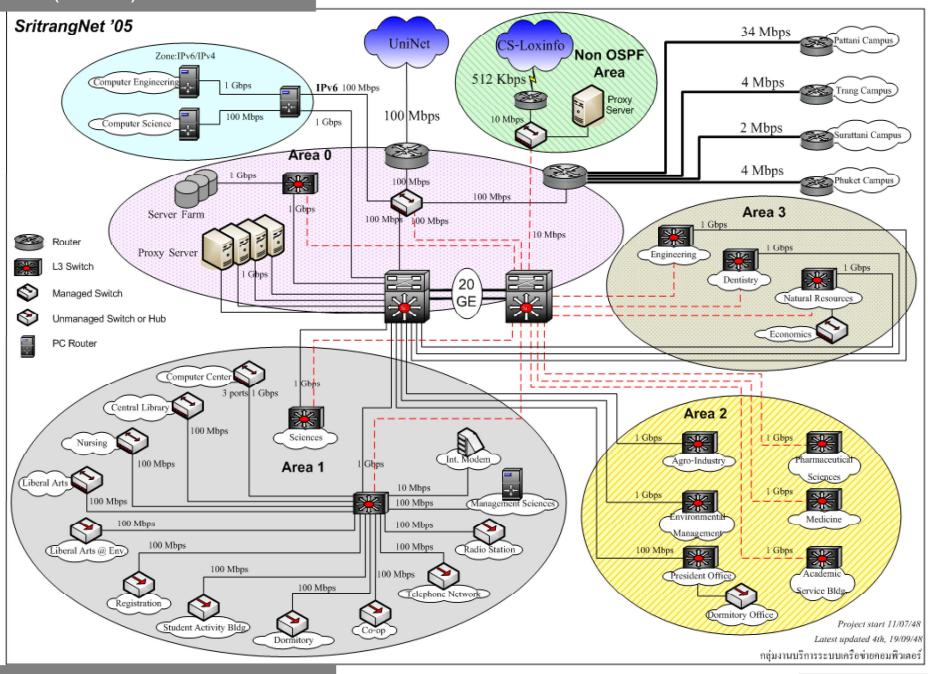
- Appliances

Suivi d'utilisation de l'infrastructure
- Monitoring des compteurs (SNMP)
- Monitoring des interfaces (SNMP)

- SNMP
- ICMP

Suivi des flux
Statistiques applicatives
(Netflow/Sflow,....)

•Sondes



Suivi détaillé de l'infrastructure
- Monitoring + complexe BGP, STP (SNMP)
- Monitoring status (SSH)

- SNMP
- SSH

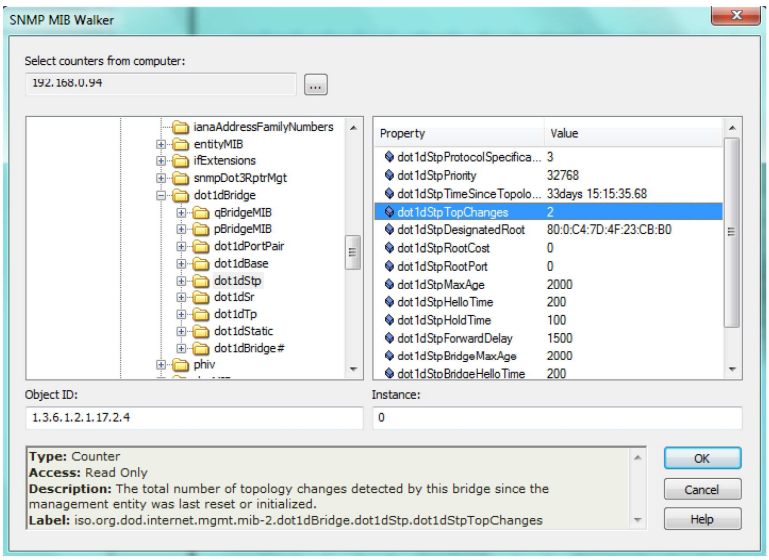
Suivi temps de réponse
Opérations IP SLA

•IP SLA (Cisco)

ORSENNA NMS SERVICES
IPSWITCH WhatsUpGold

Exemple Monitoring Spécifique Switches – Routers MIB

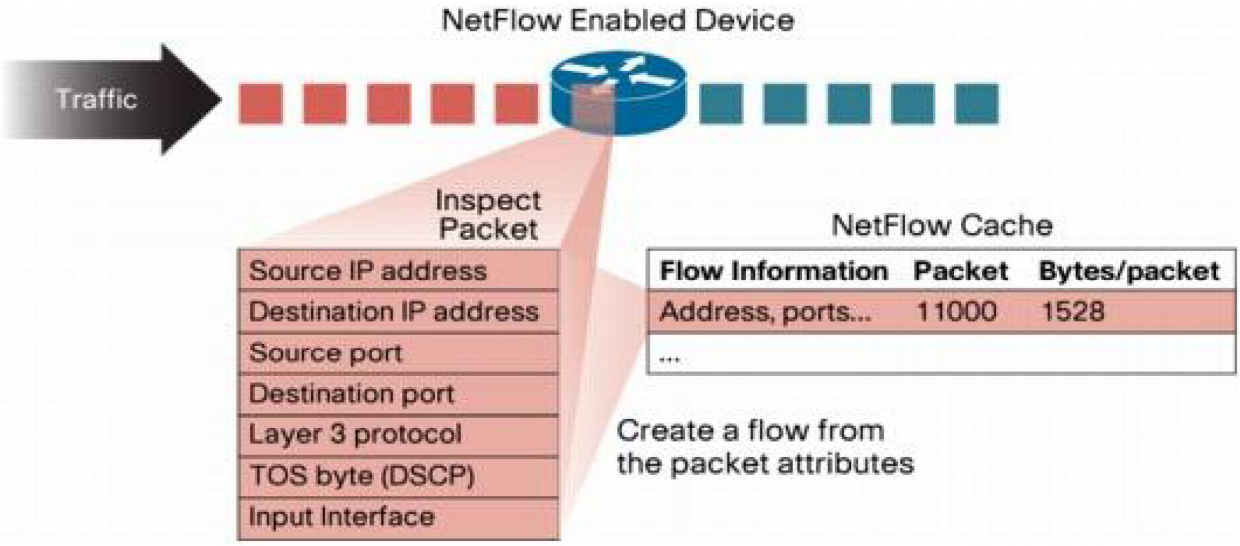
- MIB dot1dBridge (ex: spanning tree)



Périmètre – Prérequis
Exemple : Netflow

- Analyse Simple – objectifs
  - Netflow Top 10
  - Lien Internet
  - 10 Mb/s de trafic – chargé à 20 %
- Analyse + Complexe – objectifs
  - Netflow – diagnostic Lan
  - Lien Backbone
  - Liens 1Gb/s – chargé à 50 %

NetFlow

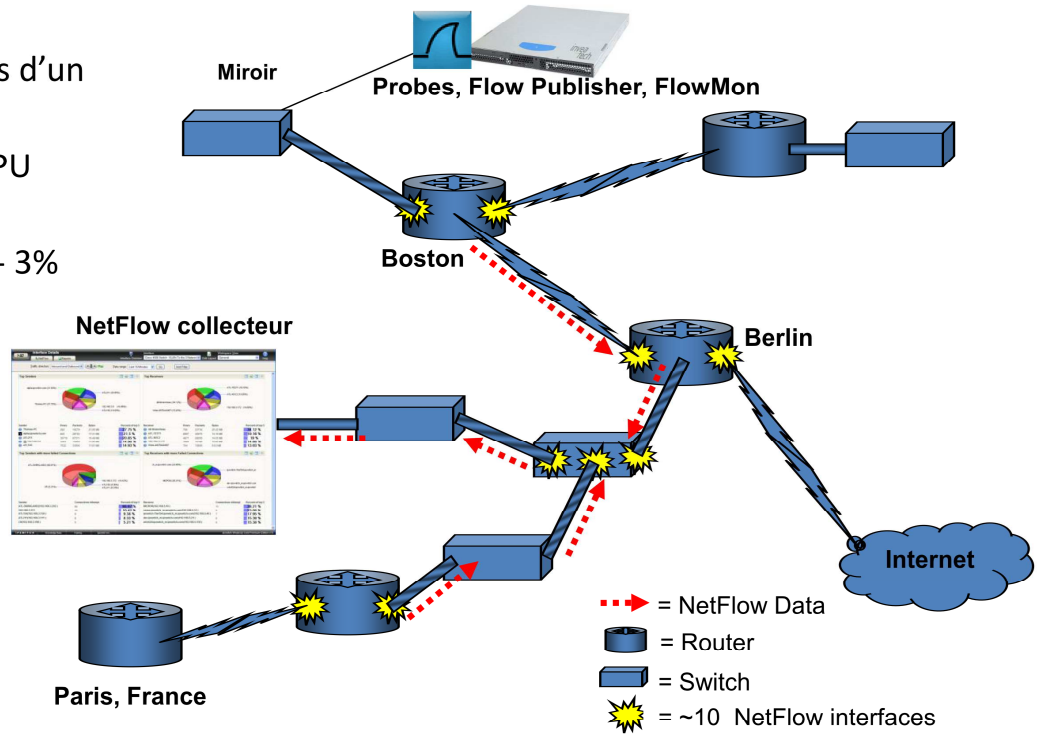


"YOU CAN THINK OF NETFLOW AS A FORM OF TELEMETRY PUSHED FROM ROUTERS AND LAYER 3 SWITCHES, EACH ONE ACTING AS A SENSOR."

JOHN CORNELL, CISCO IT TECHNICAL STAFF

Analyse de flux distribuée

- 90% des bénéfices d'un analyseur réseau
- 2% - 3% charge CPU
- Traffic réseau augmente de 1% - 3%



Limite de la stratégie "Top 10"

Top hosts, conversations, protocols

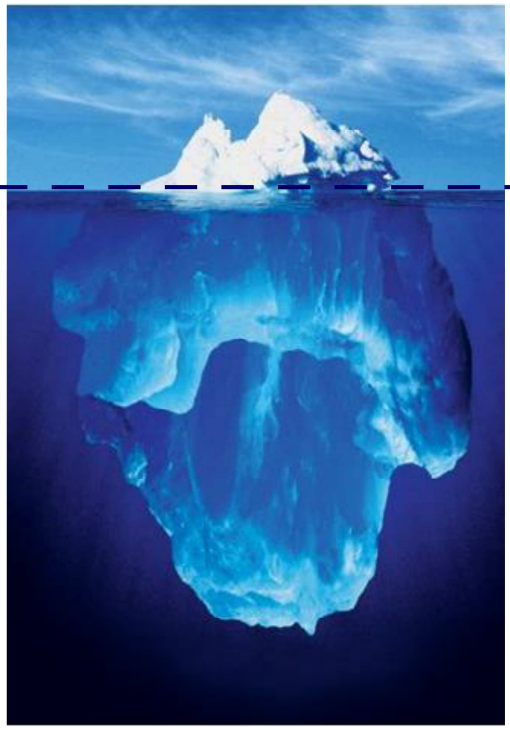
Serveurs chargés

Evènements sur le réseau

"Other"

Limite de la stratégie “Top 10”

Top hosts, conversations, protocols



Serveurs chargés

Evènements sur le réseau

- Voix
- Virus
- Hacking
- Multicast
- DNS
- Peer-to-peer
- Worms

Exemple MS-SQL Slammer

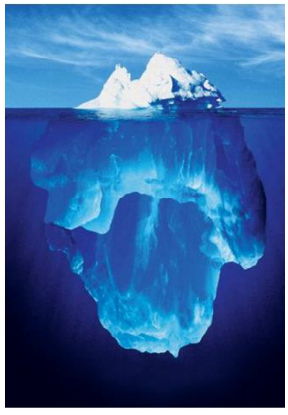
Conversations

Time Range: 14-Aug-2007, 16:56 IST - 16:57 IST
Source Address: 116.32.207.100
Dest Application: MS SQL

Results 1 to 233 of 22772

Source Address	Source App.	Dest. Address	Dest. App.	Traffic	% of Total Traffic	Packets	% of Total Packets
116.32.207.100	6000/TCP	149.153.0.0	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.1	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.2	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.3	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.4	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.5	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.6	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.7	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.8	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.9	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.10	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.11	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.12	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.13	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.14	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.15	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.16	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.17	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.18	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.19	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.20	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.21	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.22	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.23	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.24	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.25	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.26	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.27	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.28	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.29	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.30	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.31	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.32	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.33	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.34	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.35	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.36	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.37	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.38	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%
116.32.207.100	6000/TCP	149.153.0.39	1433/TCP (MS SQL)	5.33 bps (40 B)	<1%	0.02 /s (1)	<1%

22,772 Conversations sur UNE MINUTE!



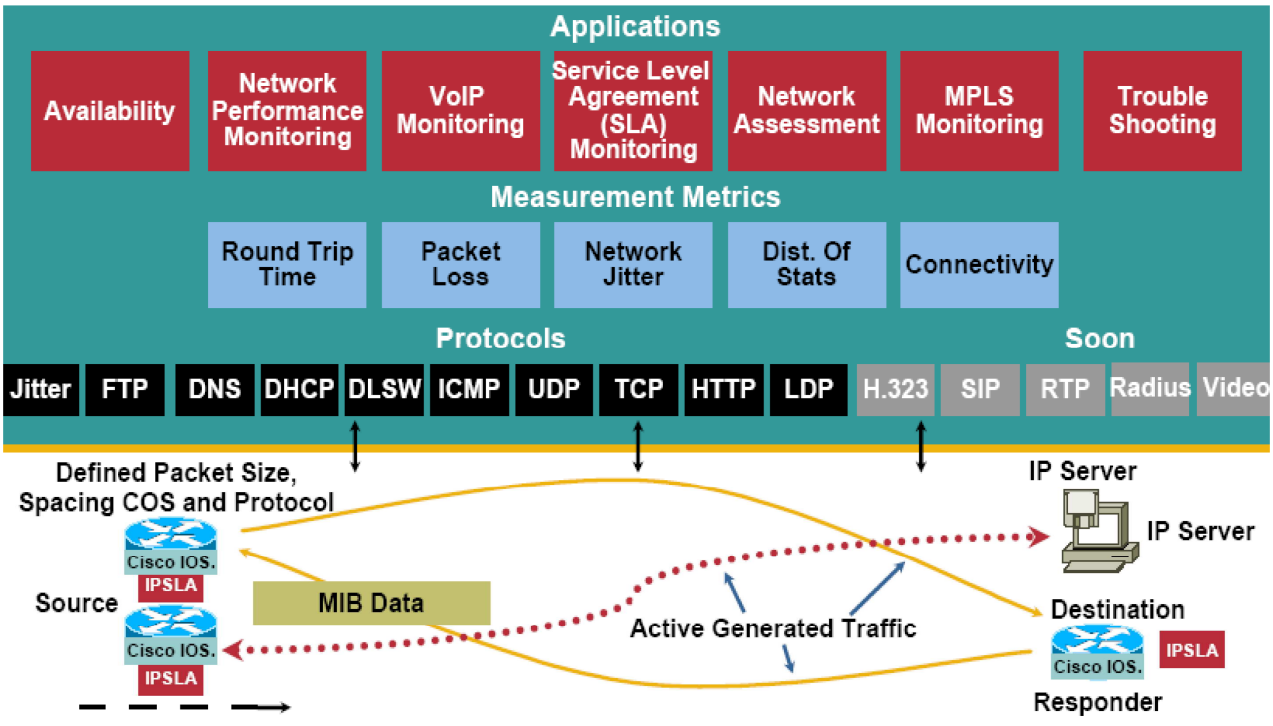
- De 900KB

Périmètre – Prérequis
Exemple : Netflow

– Analyse Simple – Solution
  - Flow Monitor
  - Stockage 15 Go/an

– Analyse + Complexe – objectifs
  - Appliance
  - Stockage 4 To/an

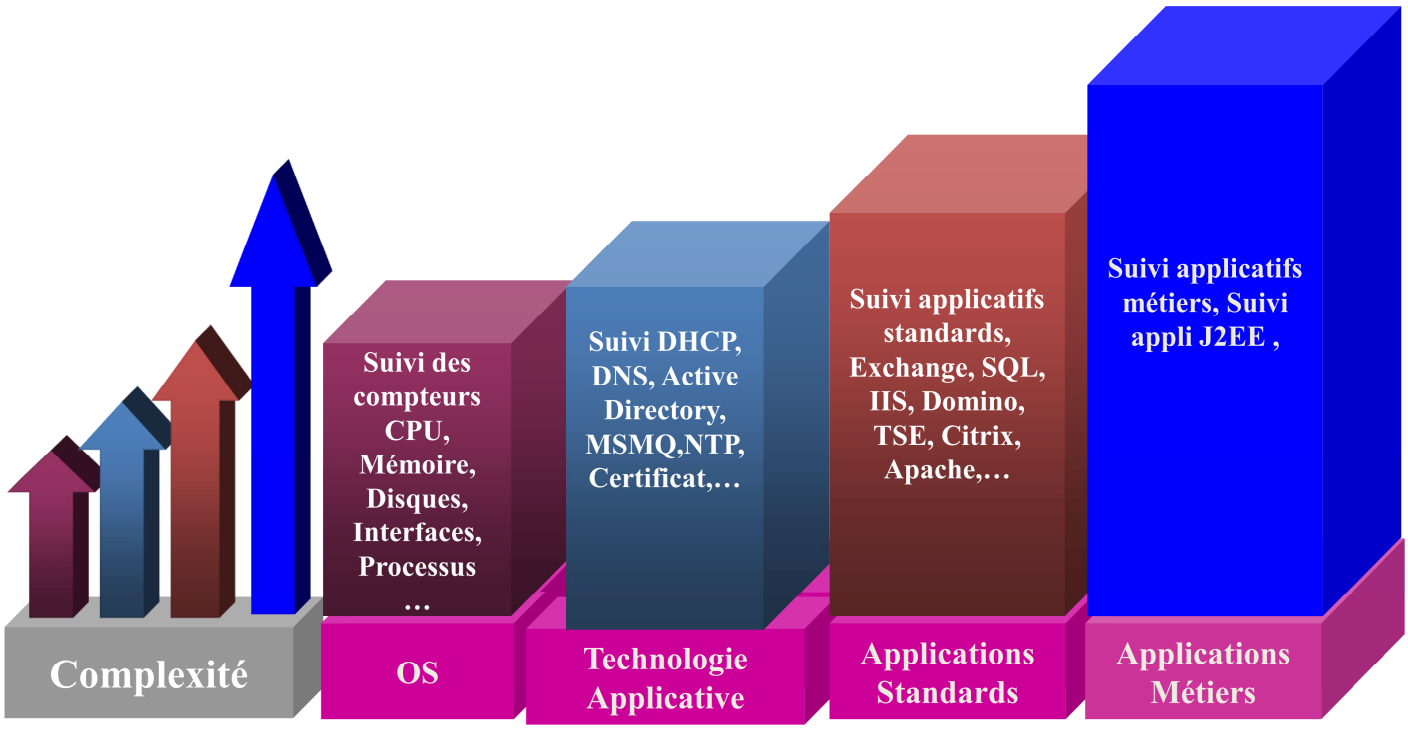
Mesures Cisco IOS IP SLAs



Maquette/POC : Bilan Infrastructure

- Pré requis mis en œuvre
  - SNMP
  - IP SLA
  - Netflow/Sflow
  - Gestion évènements (Syslog, Traps)
  - SSH
- **Niveau d'analyse est déterminant**

Périmètre Systèmes et Applications



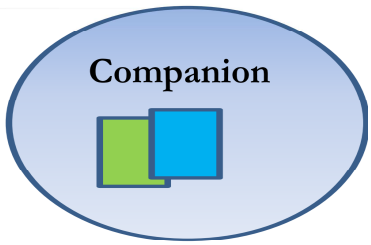
Périmètre Systèmes

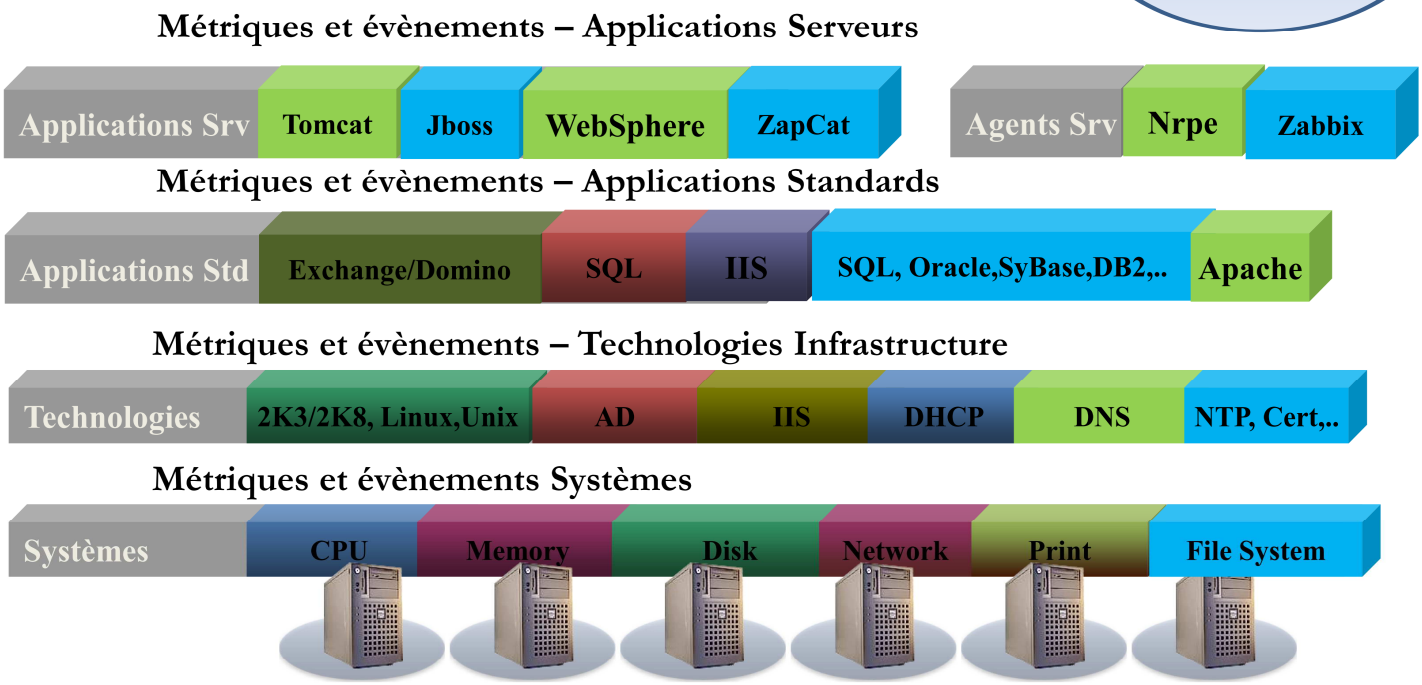
- Hardware – Agents SNMP constructeurs
  - IBM, HP, DELL, Fujitsu,…
- OS – SNMP-WMI-SSH-Agents NRPE/Zabbix
  - Serveurs Windows 2K3, 2K8
  - Workstation (XP, Vista, Seven)
  - Linux Serveurs (Redhat, Debian, …)
  - BSD (FreeBSD, OpenBSD,…)
  - HP-UX, Solaris,…
  - VmWare ESX

Applications

- Standards – WMI-SNMP-Template TCP
  - Active Directory, Citrix, Exchange, Lotus, SMTP,…
- BDD – Clients OCI , .. - Companion
  - Oracle, MySql, MsSQL, Informix, DB2,…
- Web – HTTP Monitor - Companion
  - URL, Apache, IIS, intranet,…
- Production – Journaux , WMI
  - Anti-Virus, Backups,…
- Application Servers - Companion
  - Websphere, People Soft, Web Logic, Java Syst App Server,…

Monitoring Applicatif

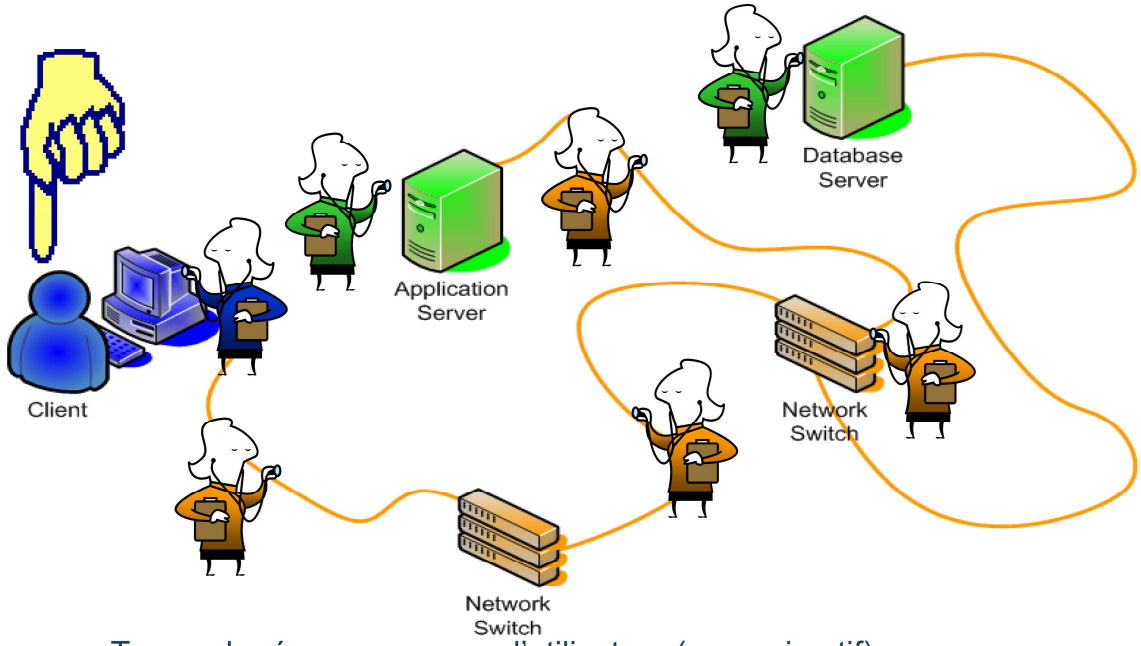




Maquette/POC : Bilan Systèmes et Applications

- Pré requis mis en œuvre
  - Agents SNMP constructeurs
  - WMI/SSH/Agents
  - Clients DB , Journaux, HTTP traitement
  - JMX, Parsing XML, Gestion fichiers
  - Scripting
- **Niveau d'analyse est déterminant**

Monitoring transactions



Temps de réponse – vu par l'utilisateur (approximatif)

"Cela prend 1 à 2 minutes"

Temps de réponse effectif

0.5 secs | **0.8 secs** | **1.2 secs**

Monitoring transactions

- Mesure des performances clientes
- SLA client

SLA *(Client)*

Client | Network | Server — 3 Secs

Temp réponse *(SLA OK)*

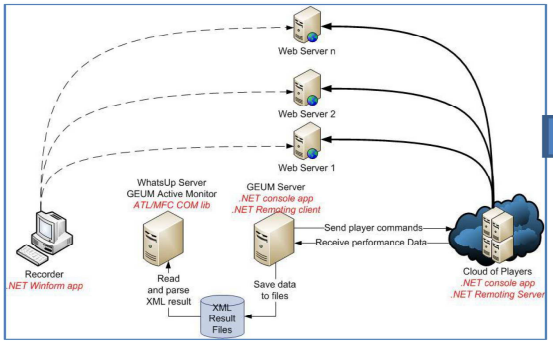
Client | Network | Server — 2,8 Secs

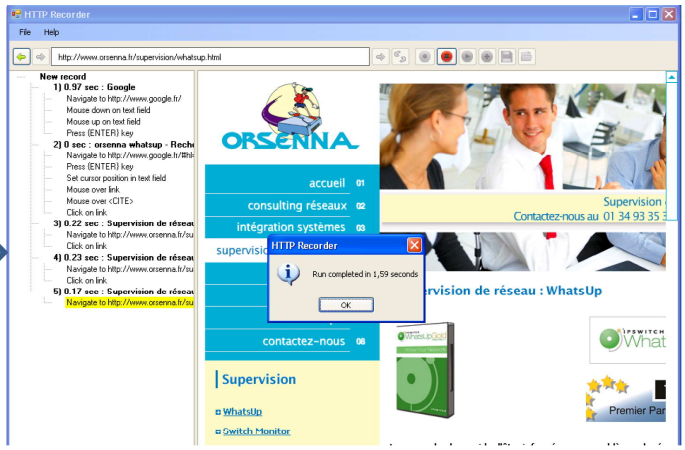
Temps réponse *(SLA KO)*

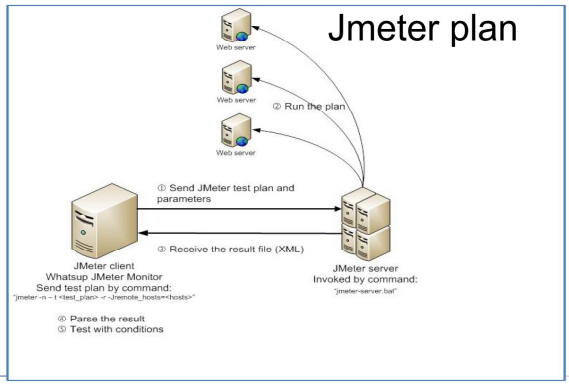
Client | Network | Server — 3,5 Secs

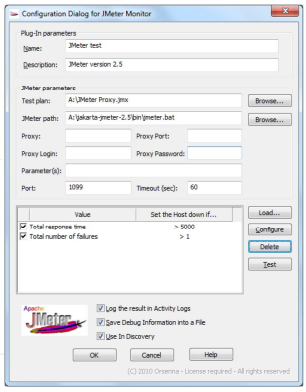
Monitoring transactions : Les outils

HTTP record/playback







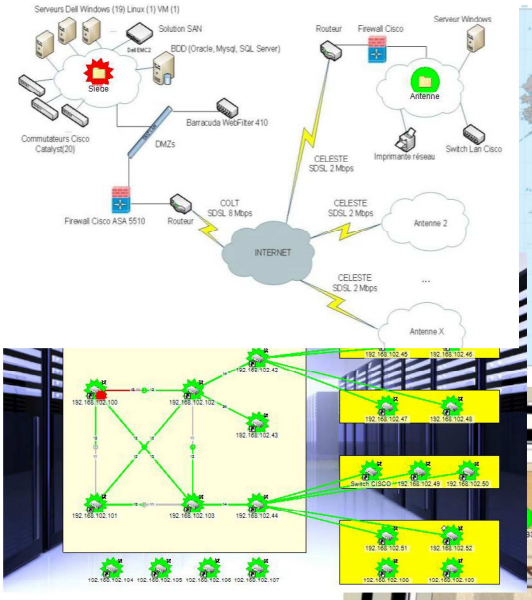


Maquette/POC : Bilan Transactions Utilisateurs

- Pré requis mis en œuvre
  - Agents (GEUM)
  - Outils (Jmeter)
  - HTTP Content monitor
- **Niveau d'analyse est déterminant**

Cartographie-Web

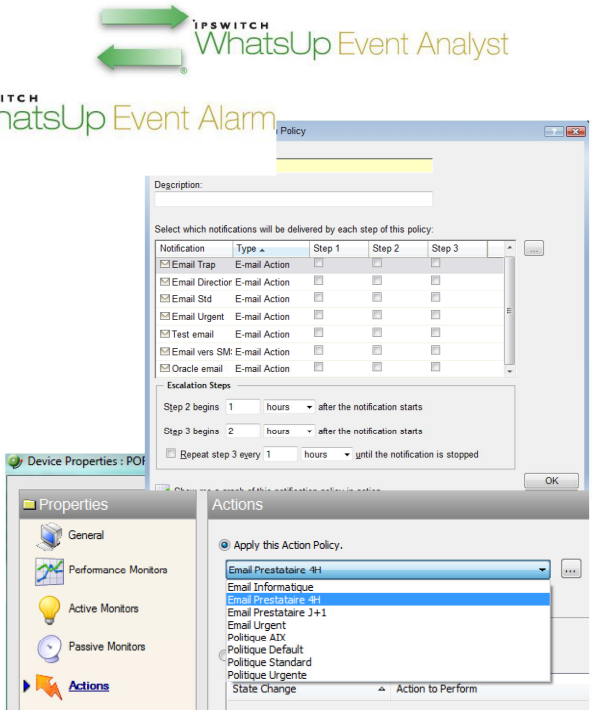
- Choix des cartes / Exploitation



- Créer différents workspaces suivant les besoins de la société.
- Créer différents comptes web pour vos équipes (système, réseau, web, applicatifs,…) pour leur donner accès uniquement à leurs informations.

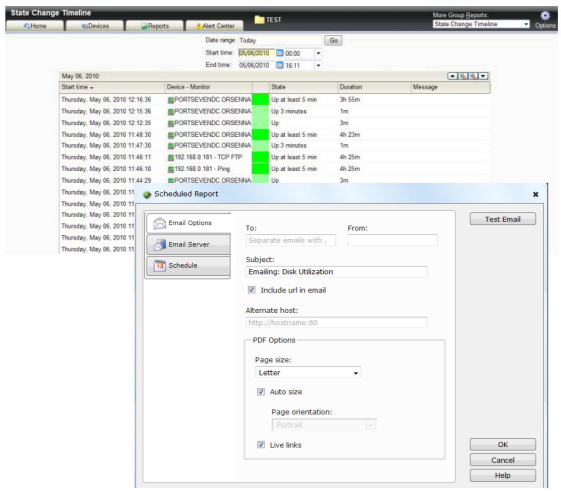
Gestion des événements & Alertes

- L'ensemble des évènements et données collectées sur le réseau constituent une base d'informations sur laquelle un filtrage sera effectué en terme de seuil, de comptage, d'état. La volumétrie est à vérifiez vis-à-vis des tailles de base.
- Les types d'alertes et les informations associées sont à définir. Les processus externes à déclencher sont à décrire.



Diagnostics & Rapports

- Des outils de diagnostic sont à intégrer dans l'interface Web
  - Console d'administration
  - Outils constructeurs
  - Outils de diagnostics spécifiques
- Les types de rapports souhaités sont à définir :
    - Rapports de disponibilité
    - Rapports de performances
    - Etats des Exceptions
    - Historiques



Reporter

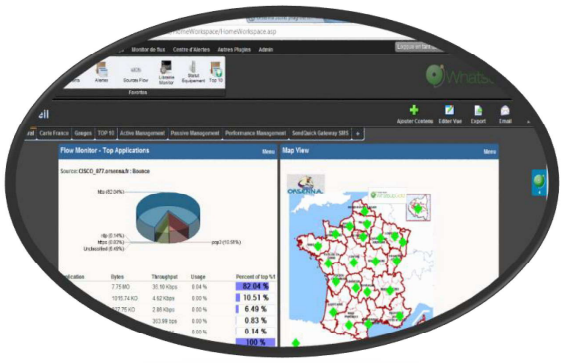
- Outil Visual Studio Reporting services

Déploiement - Pré-production

- Après la validation du (POC) ou de la maquette, le passage en pré-production s'accompagne de :
  - Finalisation de la configuration des équipements (Access-list SNMP, compte mail supervision, installation des agents pour les logs, description de l'accès aux bases de données…)
  - Tuning de la supervision SNMP, WMI, SSH, Oracle, SQL,…
  - Finalisation des cartes relatives à l'environnement (backbone, LAN, servers, financial service, Internet services,…)
  - Eléments additionnels: scripts, seuils, MIBs spécifiques…

Planning & Ressources

- Une mise en place standard s'effectue sur 4 à 8 semaines avec une charge de 10 jours :
  - Pré-Etude technique des composants
  - Description détaillée des objectifs
  - Maquette Pré-production
  - Mise en production



Tuning de performances

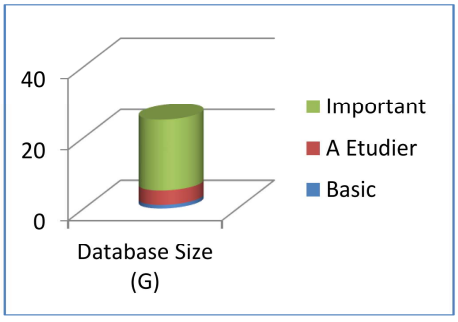
Symptômes

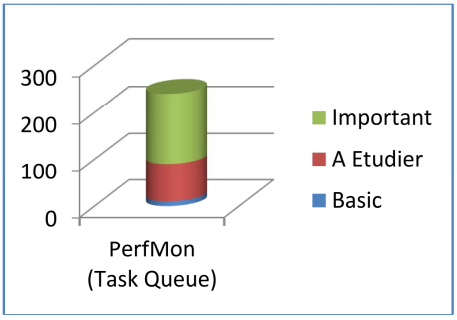
- Base de données importante (plusieurs Go)
- Temps important de rafraichissement d’une modification globale.
- Faux positifs , nombreux timeouts .
- Lenteur Web.

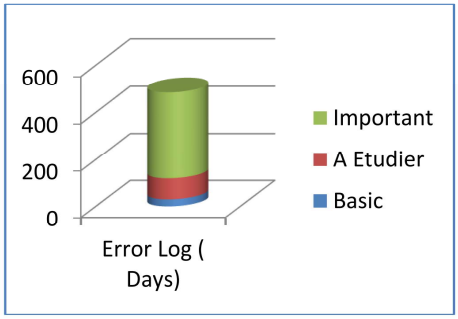
Mesures

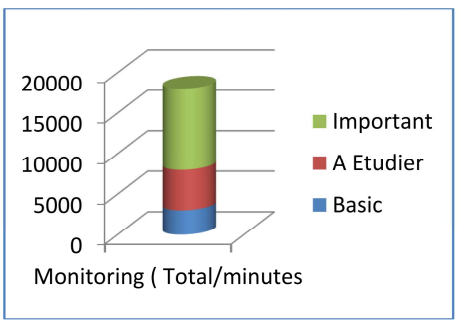
- Occupation des tables
- Suivi compteur de performances.
- Lectures journaux d'erreurs.
- Mesures monitoring.

Mesures









Bilan

- Optimisation taille de bases
- Outils de mesures préinstallés.
- Suivi erreurs et compteurs performances
- Pré-étude des extensions des surveillances

Questions ?