

Cloud computing

2013-14

Laurent Wargon
laurent@wargon.org



Déploiement & Supervision



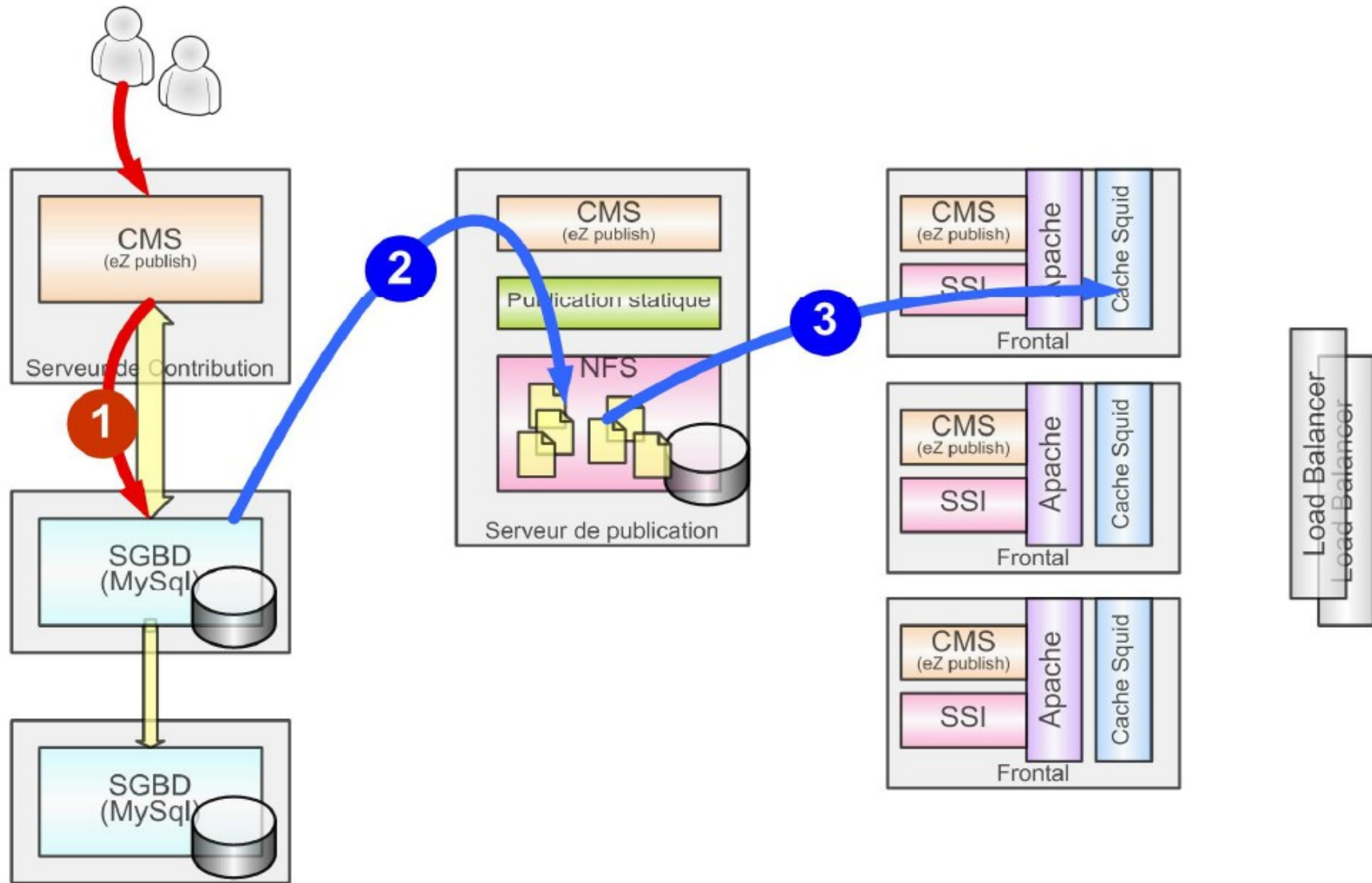
Déploiement



Déploiement

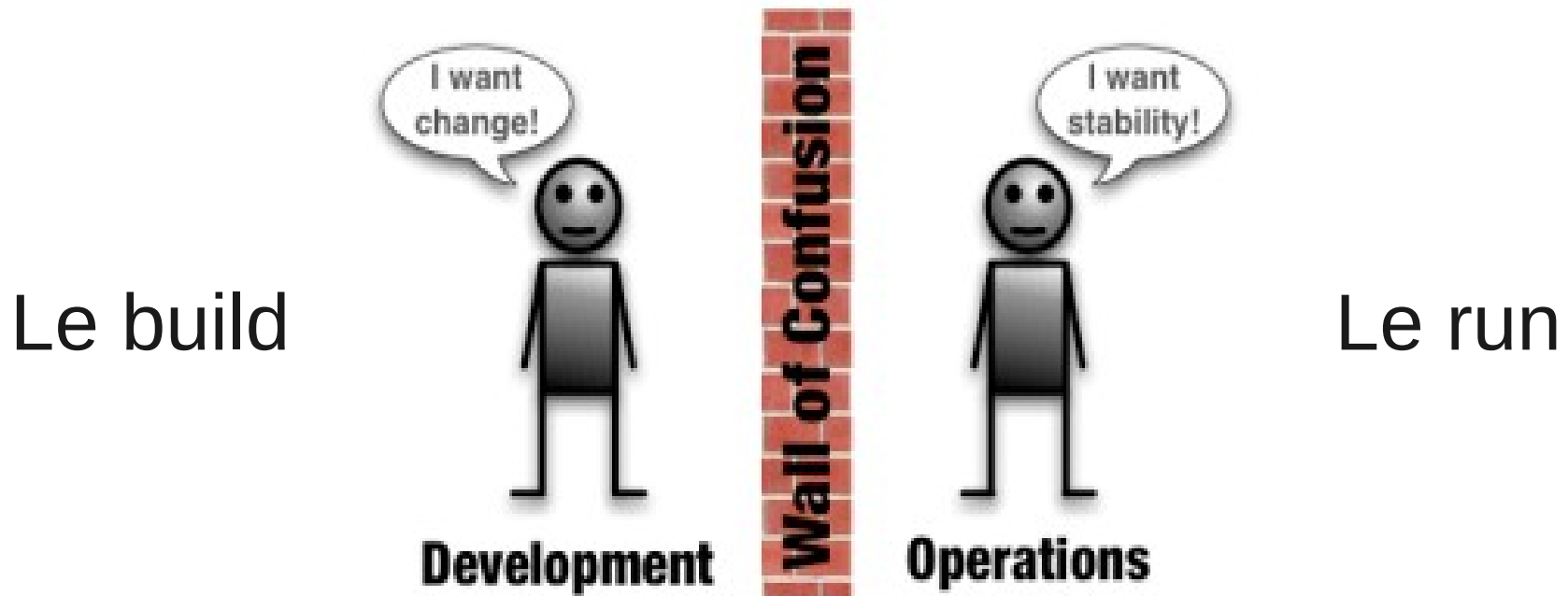
- L'exploitation reçoit du développement
 - Un code
 - Une documentation ?
- L'exploitation a pour mission
 - L'installation en pré-production
 - L'installation en production
 - L'installation des mises à jour
- 50 % temps de l'équipe exploitation

Mise en production complexe : Sport 24



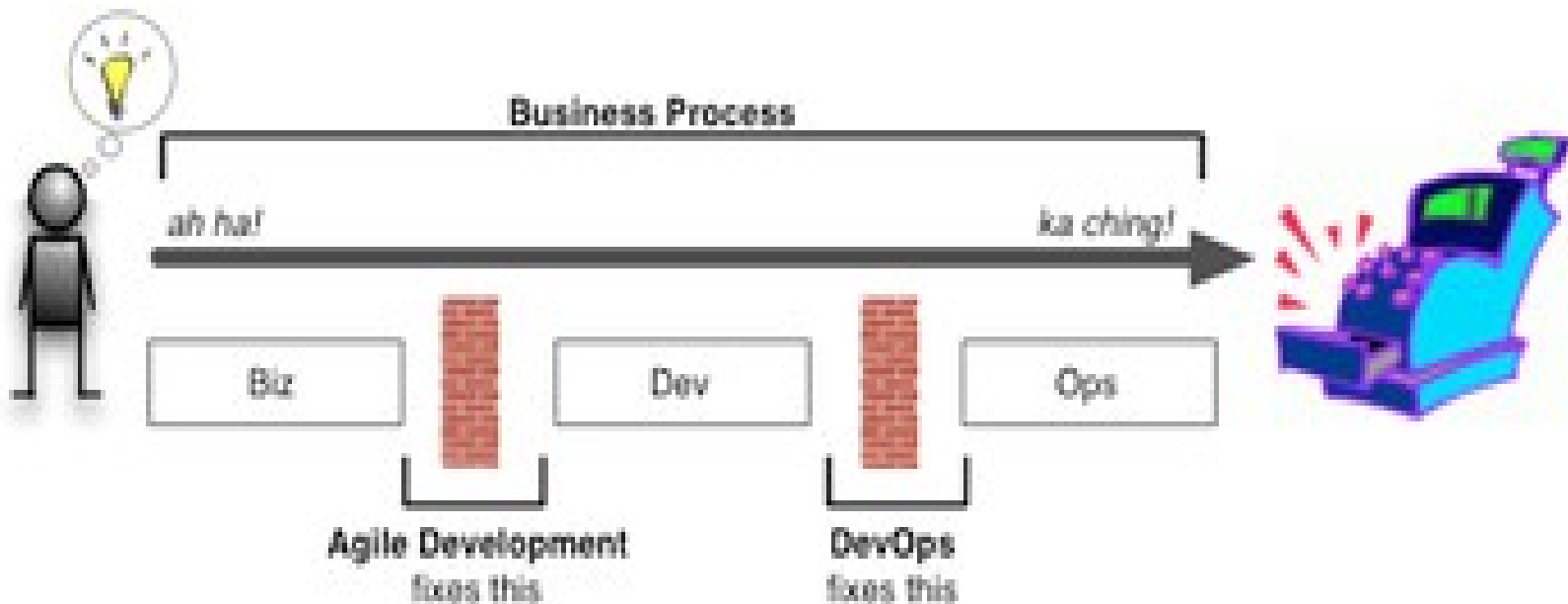
Le développement et la production

Devops : terme issu de la contraction des mots anglais "development" (développement) et "operations" (exploitation)



Objectif Devops

Un mouvement visant à l'alignement du SI sur les besoins de l'entreprise (à commencer par l'alignement développement / exploitation)



DevOps

- Culture
- Automatisation
- Partage
- Mesure



La culture Devops

- Privilégier les connaissances de chacun
- Favoriser le mode projet en opposition au mode pompier afin de capitaliser sur les compétences de chacun.
- Encourager l'autonomie
→ épanouissement personnel.
- Valoriser le travail créatif

Installations automatisées ?

- à la main
 - Impossible avec un grand nombre de machines
- Scripts
 - Repos Git
 - Problème du parc multi-distribution
- Gestionnaire de configuration des machines
 - Réponses aux problèmes précédents
 - Mais ticket d'entrée

<http://blog.nicolargo.com/2012/03/en-route-vers-puppet-chef-cfengine.html>

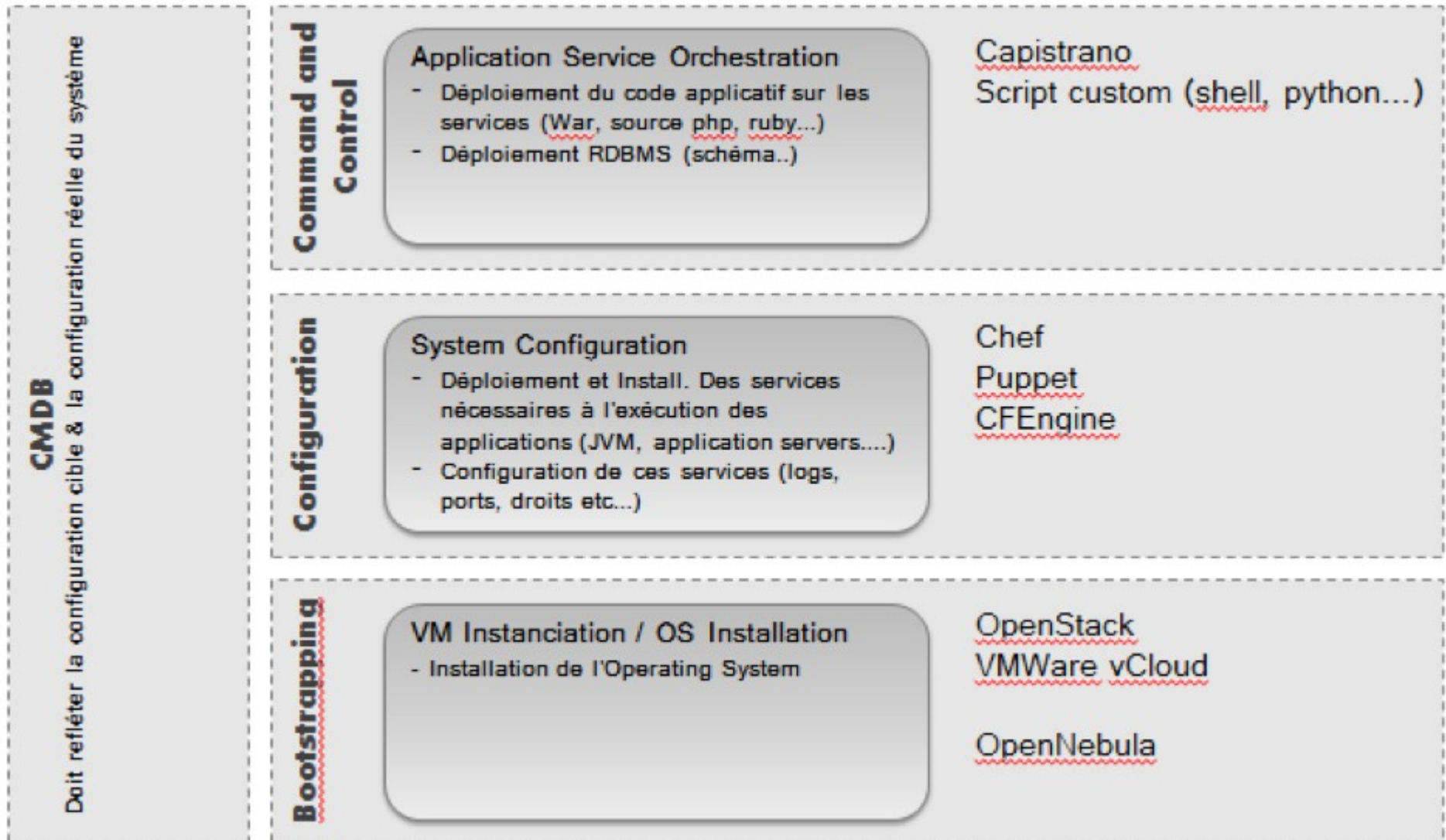


L'automatisation Devops

- CMDB Configuration Management DataBase
- Instancier une VM
 - VMWare vCloud, OpenStack, API
- Configurer la VM
 - Chef, Puppet, CFEngine,
- Installer le code
 - Script, capistrano

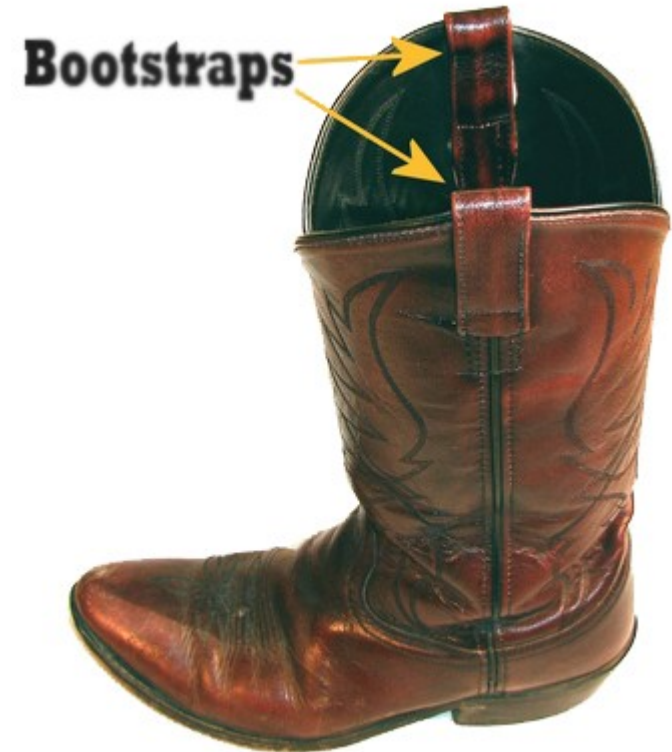


L'automatisation Devops



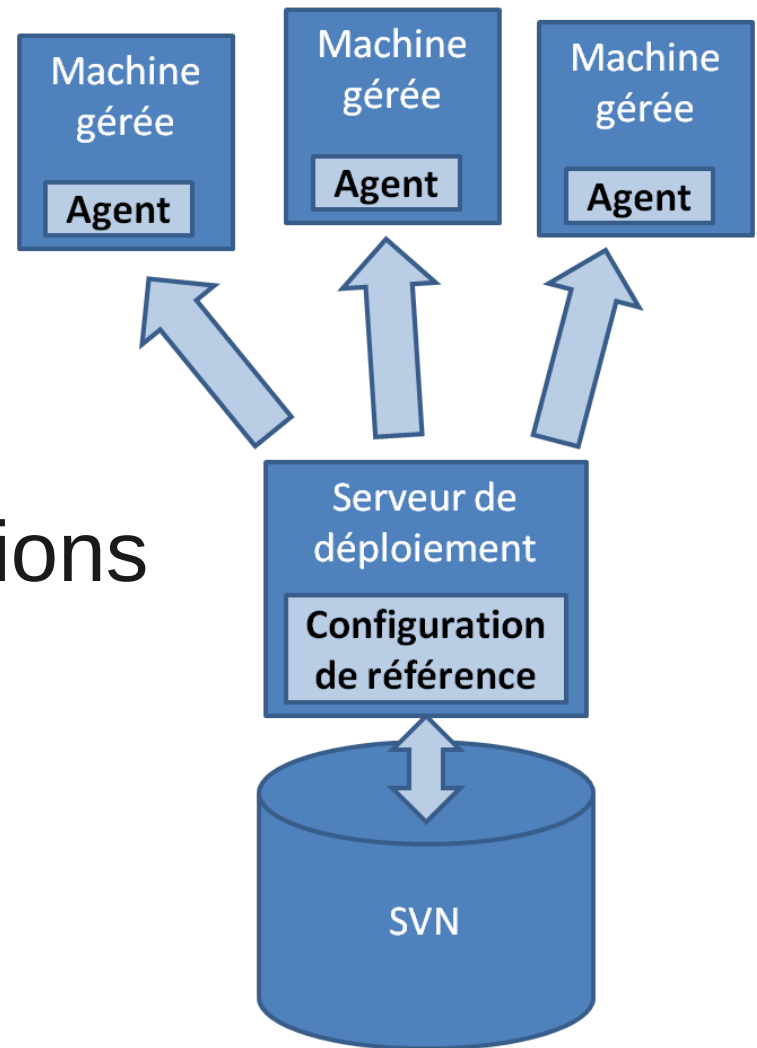
Bootstrap

Un petit programme
d'amorçage qui permet
d'en lancer un plus gros
pull oneself over a fence
by one's bootstraps
se tirer au dessus d'une
clôture par ses
bootstraps



Automatisation : configuration

- Configuration
 - Chef
 - Puppet
 - CFEngine
- Logiciel de gestion de versions
 - Subversion (SVN)
 - Git (Linus Torvalds)



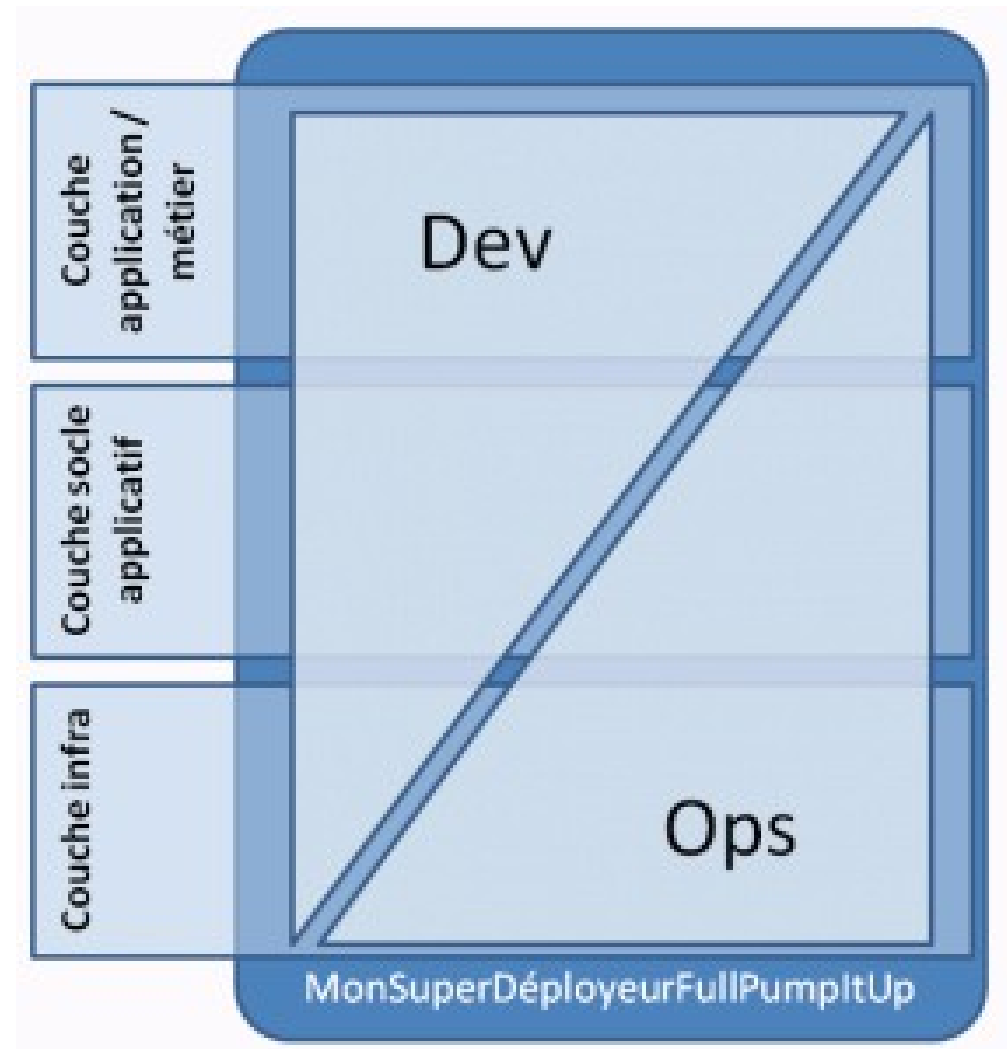
Le partage Devops

- Vision commune
- Problèmes communs
- Glossaire commun
- Connaissance commune
- Outils communs



Le partage Devops

Dev et Ops
utilisent
un même outil



Les mesures Devops

- KPI Key Performance Indicator
indicateurs clés de performance
- but : aligner l'ensemble des acteurs de
l'entreprise sur un but commun
- Temps de réponse d'une requête }
Indicateurs de taux de panne }
Incidence sur le chiffre d'affaire ←

Supervision



Quels sont les risques

- Mise en production d'une nouvelle version,
- Erreur de console,
- Flux réseau inattendu
- Montée en charge due au succès
- Malveillance, vol de données,
- Panne matérielle sur un serveur,
- Panne de climatisation, d'électricité,
- Inondation, incendie, ...

Objectifs de la supervision

- Réduire (annuler) le délais début de panne - début de l'intervention
- Prévention des problèmes
- Analyser la situation

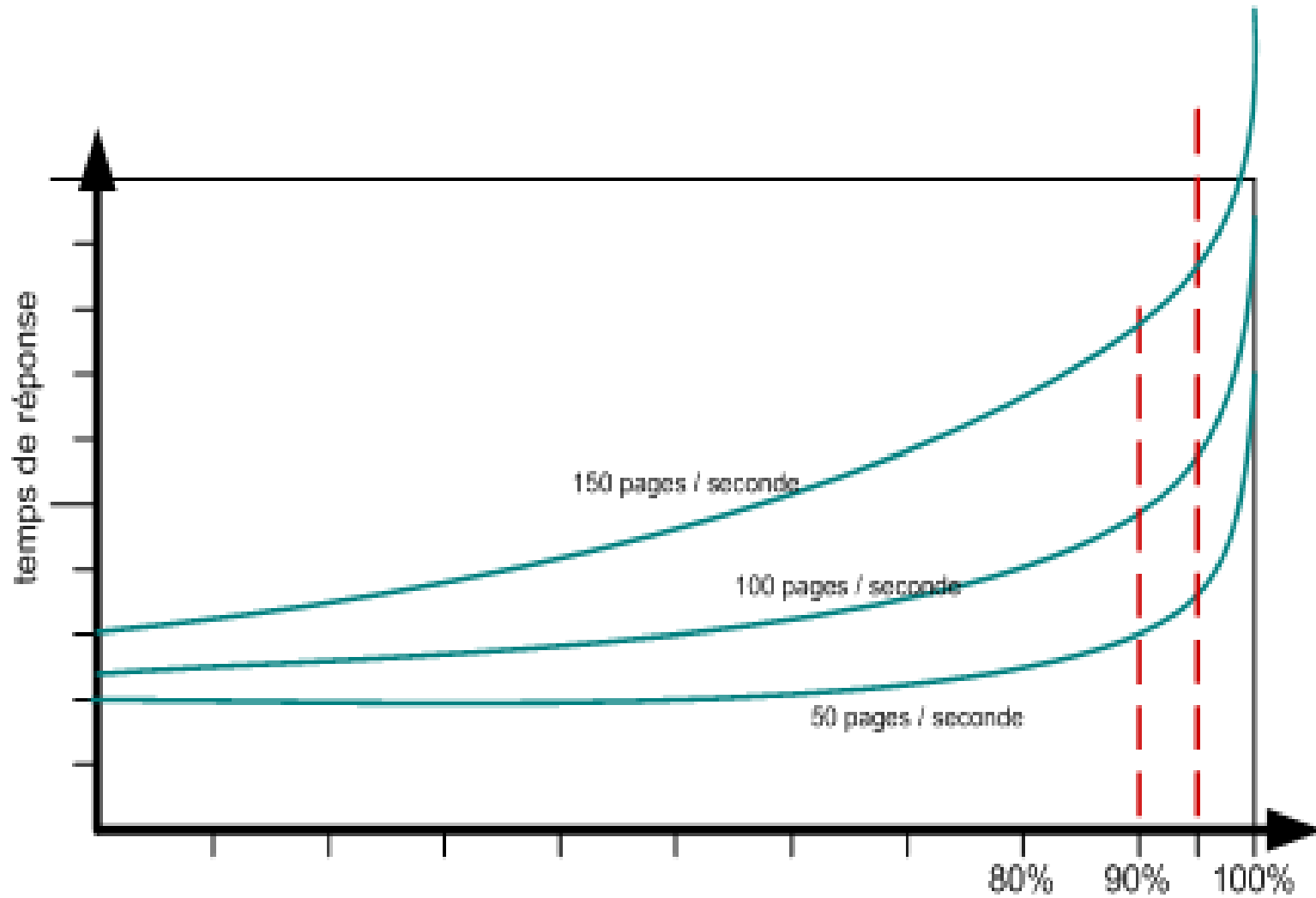
Les équipements à superviser

- Le réseau et ses équipements
 - routeurs
 - commutateurs
- Les serveurs
 - mesures techniques
- Les applications
 - mesures métiers

Faire des mesures

- Présence des machines sur le réseau
- Occupation des disques durs, Swap, RAM
- Load CPU
- Flux réseaux
- Taux d'accroissement d'un indicateur
- Mesures métiers
- Ressenti utilisateur
- Temps de réponses

Temps de réponse



Fonctionnalités de la supervision

- Sondes
 - Simple Network Management Protocol (SNMP) réseau, disques, swap, RAM, Load
 - agent de l'outil de supervision (NRPE)
 - requête web, ssh commande, requête SQL
 - requête métier, code propriétaire
- Templates
 - gabarits de configuration

Fonctionnalités de la supervision

- Définition des seuils (Warning / Alerte)
- Notifications
 - Popup, son, fax, mail, SMS, IRC, Jabber, tél
 - Périodes de notification
 - Définition de groupes / créneaux horaires
 - Répétition des notifications jusqu'à acquittement
 - Escalade des notifications

Fonctionnalités de la supervision

- Actions réflexes
 - par exemple instancier un frontal de plus
- Cartographie
- Analyses
 - Graphiques
 - mesures détaillée
- Dépendance :
Équipement inaccessible et non en panne

Produits de supervision

- Outils commerciaux
 - Tivoli (IBM), Openview (HP), Patrol (BMC), Unicenter TNG (Computer Associates)
- Outils libres
 - Nagios, Centreon, Icinga, Shinken
 - OpenNMS, ZABBIX, Cacti, ...

http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems



Centreon : liste des alertes

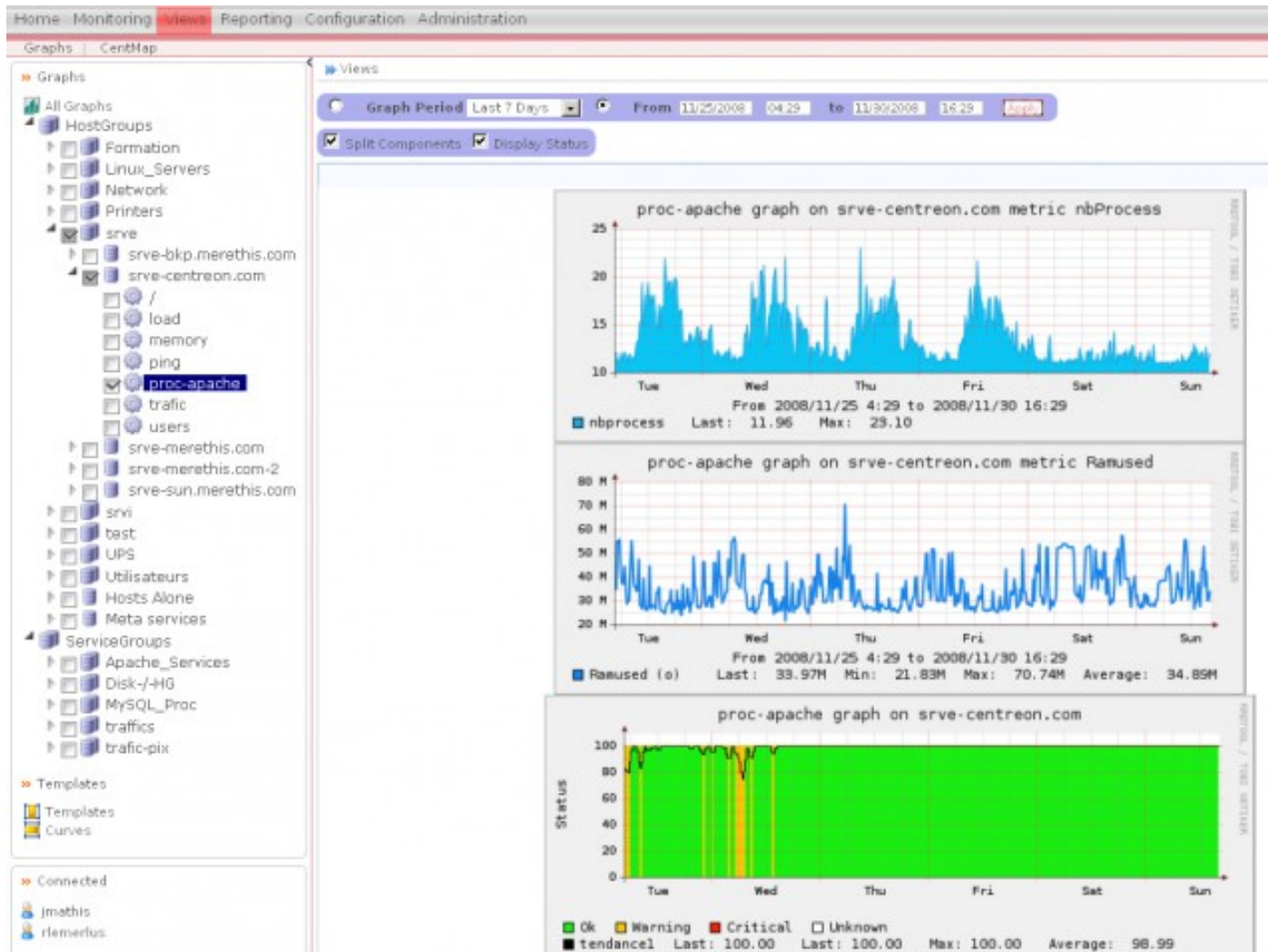
The screenshot displays the Centreon monitoring interface. The main window shows a list of alerts for the 'Last 14 Days' period, from 08/17/2008 04:10 to 11/06/2008 15:30. The alerts are filtered by 'Alerts' and 'Hard Only'. The table below shows the details of these alerts.

Day	Time	Host	Services	Type	R	Description
2008/11/05	23:04:02	rt-voip-1	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 176.679/192.692/204.948/15.507 ms
2008/11/05	23:02:32	rt-voip-2	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 162.661/173.412/182.883/8.312 ms
2008/11/05	23:01:17	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 49.632/50.047/50.395/0.315 ms
2008/11/05	22:46:18	internet	ping	WARNING	HARD 3	GPING WARNING - rtt min/avg/max/mdev = 207.291/214.681/221.926/5.987 ms
2008/11/05	22:41:21	internet	ping	WARNING	HARD 3	GPING WARNING - rtt min/avg/max/mdev = 207.291/214.681/221.926/5.987 ms
2008/11/05	22:39:02	rt-voip-1	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 176.679/192.692/204.948/15.507 ms
2008/11/05	22:38:52	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 162.661/173.412/182.883/8.312 ms
2008/11/05	22:33:07	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 49.632/50.047/50.395/0.315 ms
2008/11/05	22:32:32	rt-voip-2	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 176.679/192.692/204.948/15.507 ms
2008/11/05	20:41:12	sw-3com1	traffic-4	ERROR	HARD 3	Error: Interface is not ready - status: down
2008/11/05	10:34:08	sw-3com1	traffic-4	OK	HARD 3	Traffic In: 3.77 Gb, Out: 1.28 Gb
2008/11/04	20:59:07	sw-3com1	traffic-4	ERROR	HARD 3	Error: Interface is not ready - status: down
2008/11/04	18:14:12	sw-3com1	traffic-14	ERROR	HARD 3	Error: Interface is not ready - status: down
2008/11/04	14:32:55	rt-voip-2	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 176.679/192.692/204.948/15.507 ms
2008/11/04	14:29:35	sw-3com1	traffic-3	OK	HARD 3	Traffic In: 615.76 b/s (0.0%), Out: 1.68 kb/s (0.0%) - Total Rx Bits In: 380.22 MB, Out: 1.28 Gb
2008/11/04	14:07:56	rt-voip-2	ping	WARNING	HARD 3	GPING WARNING - rtt min/avg/max/mdev = 207.291/214.681/221.926/5.987 ms
2008/11/04	13:53:25	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 162.661/173.412/182.883/8.312 ms
2008/11/04	13:39:35	sw-3com1	traffic-3	ERROR	HARD 3	Error: Interface is not ready - status: down
2008/11/04	13:32:46	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 49.632/50.047/50.395/0.315 ms
2008/11/04	12:51:25	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 49.632/50.047/50.395/0.315 ms
2008/11/04	12:26:01	internet	ping	OK	HARD 3	GPING OK - rtt min/avg/max/mdev = 49.632/50.047/50.395/0.315 ms
2008/11/03	19:23:07	sw-3com1	traffic-12	ERROR	HARD 3	Error: Interface is not ready - status: down
2008/11/03	18:07:27	sw-disco-1	traffic-FastEthernet0/10	OK	HARD 3	Traffic In: 14.29 kb/s (0.0%), Out: 19.27 kb/s (0.0%) - Total Rx Bits In: 25.91 GB, Out: 6.43 Gb
2008/11/03	18:07:27	sw-disco-1	traffic-FastEthernet0/9	OK	HARD 3	Traffic In: 613.67 b/s (0.0%), Out: 2.91 kb/s (0.0%) - Total Rx Bits In: 91.58 MB, Out: 385.25 Mb
2008/11/03	18:05:57	sw-disco-1	traffic-FastEthernet0/24	OK	HARD 3	Traffic In: 3.57 Mb/s (3.6%), Out: 1.31 Mb/s (1.3%) - Total Rx Bits In: 32.14 GB, Out: 28.99 Gb
2008/11/03	18:05:17	sw-disco-1	packetErrors	OK	HARD 3	Status OK on all interfaces
2008/11/03	18:05:17	sw-disco-1	traffic-FastEthernet0/21	OK	HARD 3	Traffic In: 0.00 b/s (0.0%), Out: 2.77 kb/s (0.0%) - Total Rx Bits In: 0.00 Mb, Out: 300.40 Mb
2008/11/03	18:04:32	sw-disco-1	traffic-FastEthernet0/20	OK	HARD 3	Traffic In: 6.93 b/s (0.0%), Out: 2.77 kb/s (0.0%) - Total Rx Bits In: 0.07 Mb, Out: 300.01 Mb
2008/11/03	18:04:32	sw-disco-1	traffic-FastEthernet0/20	OK	HARD 3	Traffic In: 18.13 kb/s (0.0%), Out: 3.49 kb/s (0.0%) - Total Rx Bits In: 3.92 MB, Out: 300.01 Mb

A dialog box titled 'Opening EventLog.csv' is overlaid on the table, asking 'What should Firefox do with this file?' with options 'Open with OpenOffice.org 2.3', 'Save File', and 'Do this automatically for files like this from now on'.



Centreon : graphiques



Deux types de supervision

- Les exploitants
 - Gestion de la disponibilité
 - Supervision technique
- Les responsables fonctionnels
 - Gestion de la performance
 - Supervision de bout en bout
 - End User Experience
 - Quality of Experience QoE

Ressenti utilisateur

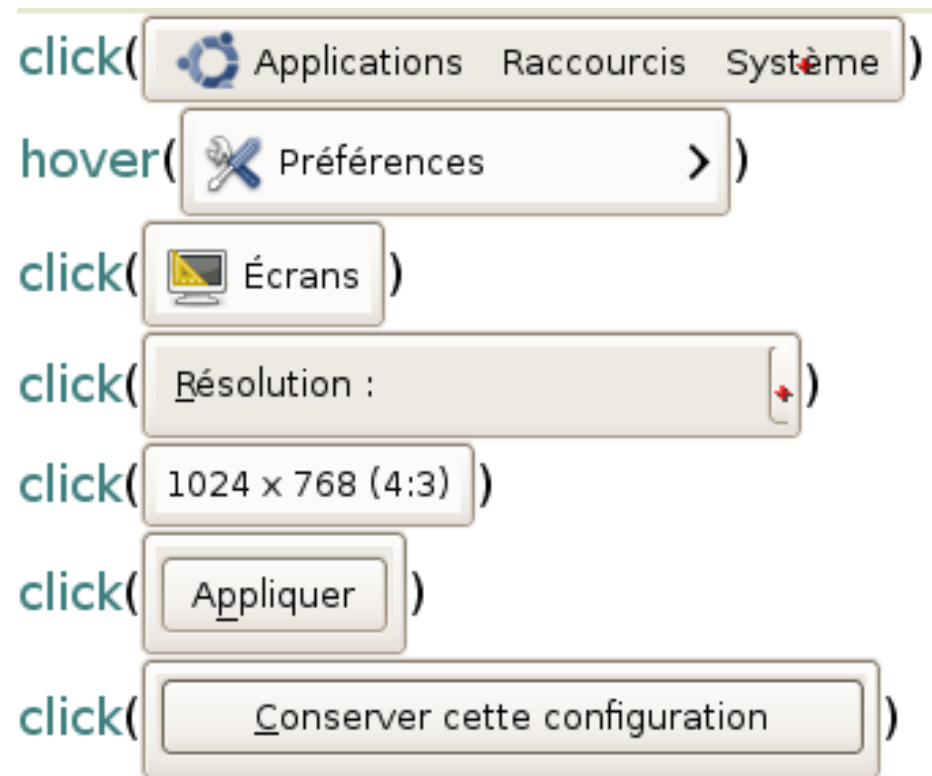
- **Cucumber** : un responsable fonctionnel décrit le comportement du logiciel en « langage naturel »
- **Watir** : un code contrôle le navigateur de la même manière qu'un utilisateur
- **WebDriver** : pilotage unifié pour IE, Firefox, Chrome, ...
- **Cucumber-Nagios** : exécuter les tests et les restitue à Nagios/Shinken

<http://wiki.monitoring-fr.org/supervision/eue/start>

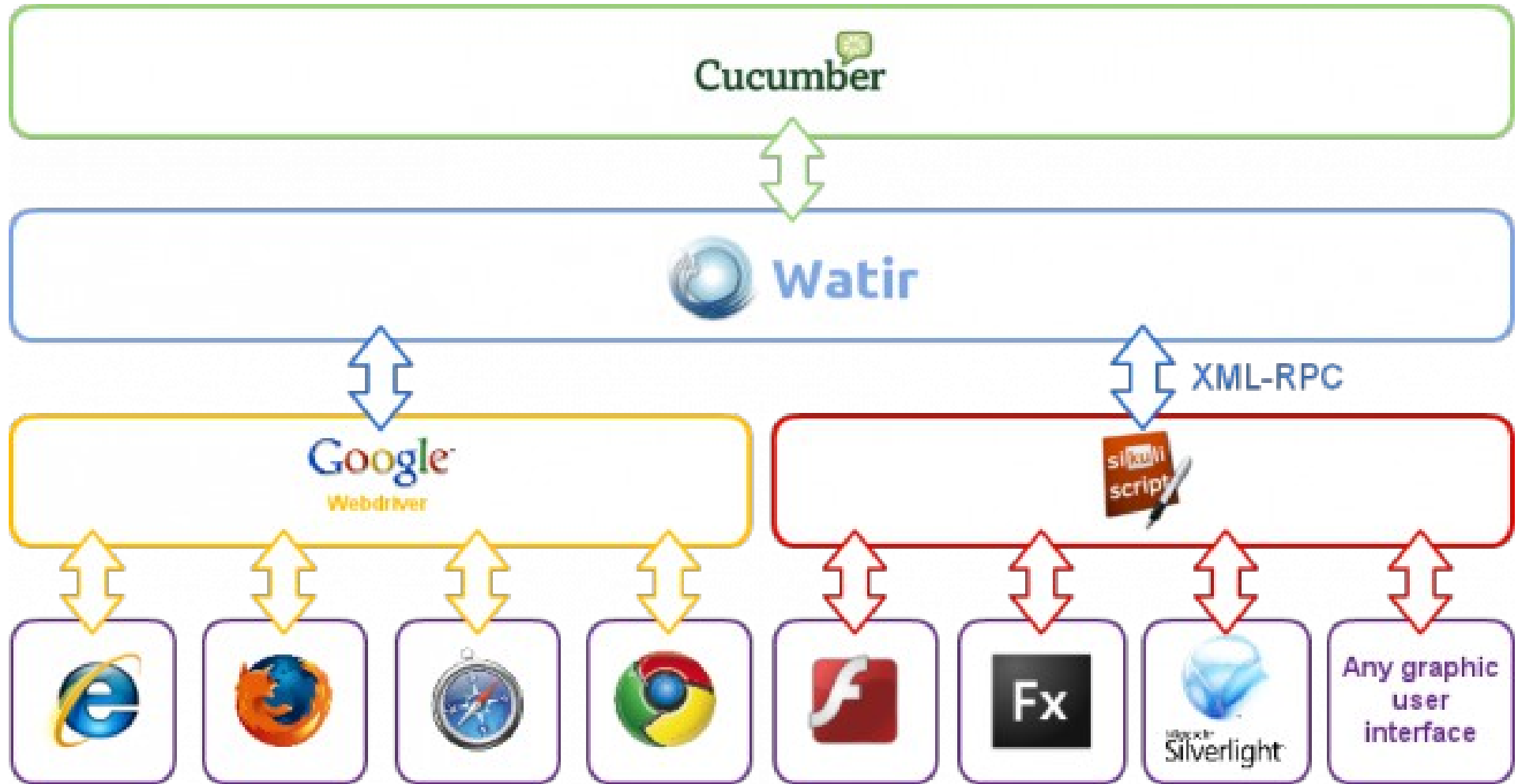


Ressenti utilisateur

- Reconnaissance optique et conditions
 - Sikuli
 - wintask
 - SuperMacro



Ressenti utilisateur



Bibliographie

- Linux Magazine Hors-Série n°62
Ne quittez plus vos serveurs des yeux !
- <http://devops.fr/presentations.html>
- <http://blog.octo.com>



Questions



Amélioration continue du cours

- Vos réactions, impressions et remarques
 - adapté au public
 - qualité / quantité
- Ma présentation
 - support de cours
 - présentation orale
 - le TP
- Toutes les remarques sont bienvenues



Révisions



NIST : Essential Characteristics

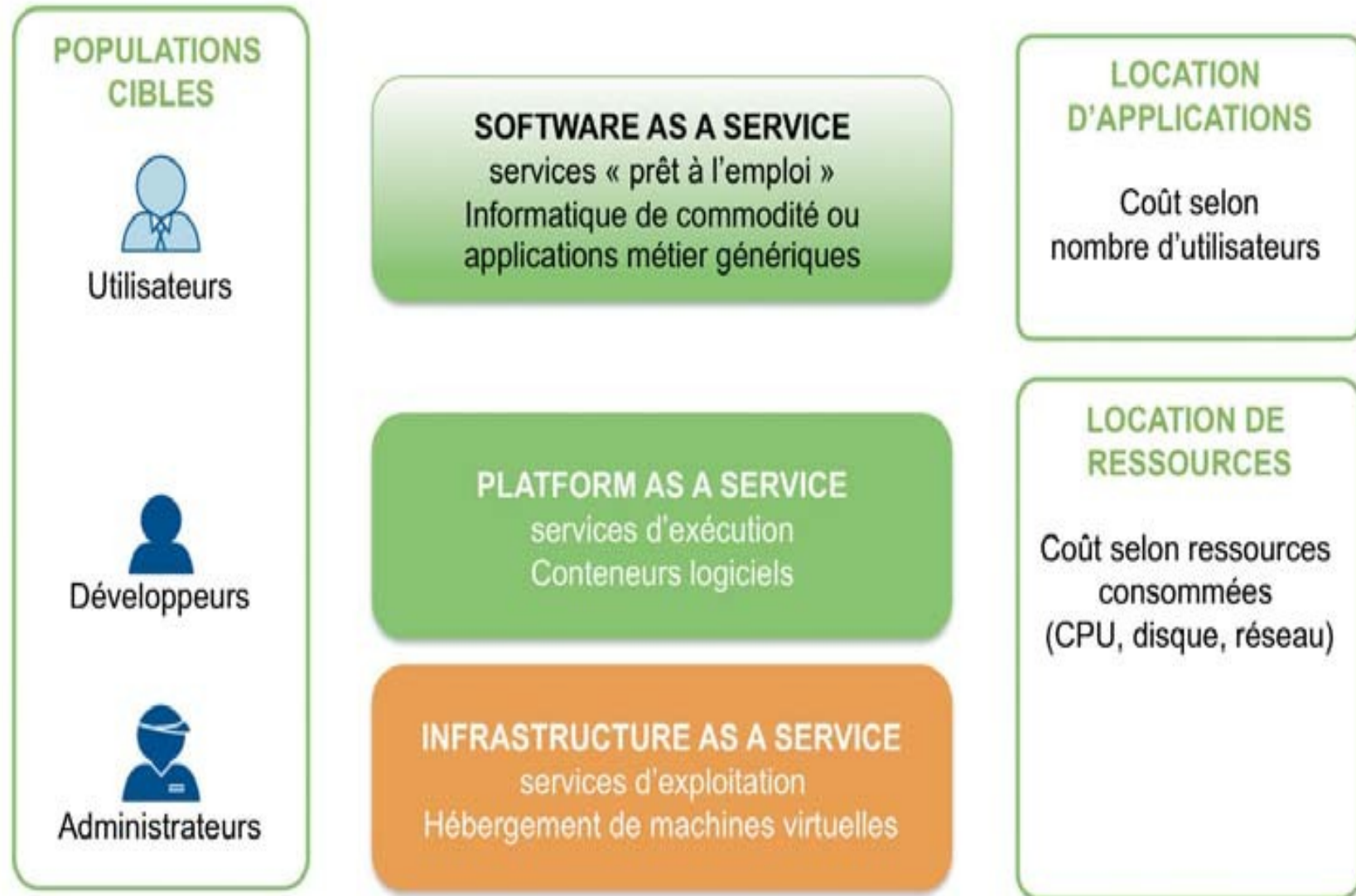
National Institute of Standards and Technology

- On-demand self-service
- Rapid elasticity
- Broad network access
- Resource pooling
- Measured Service

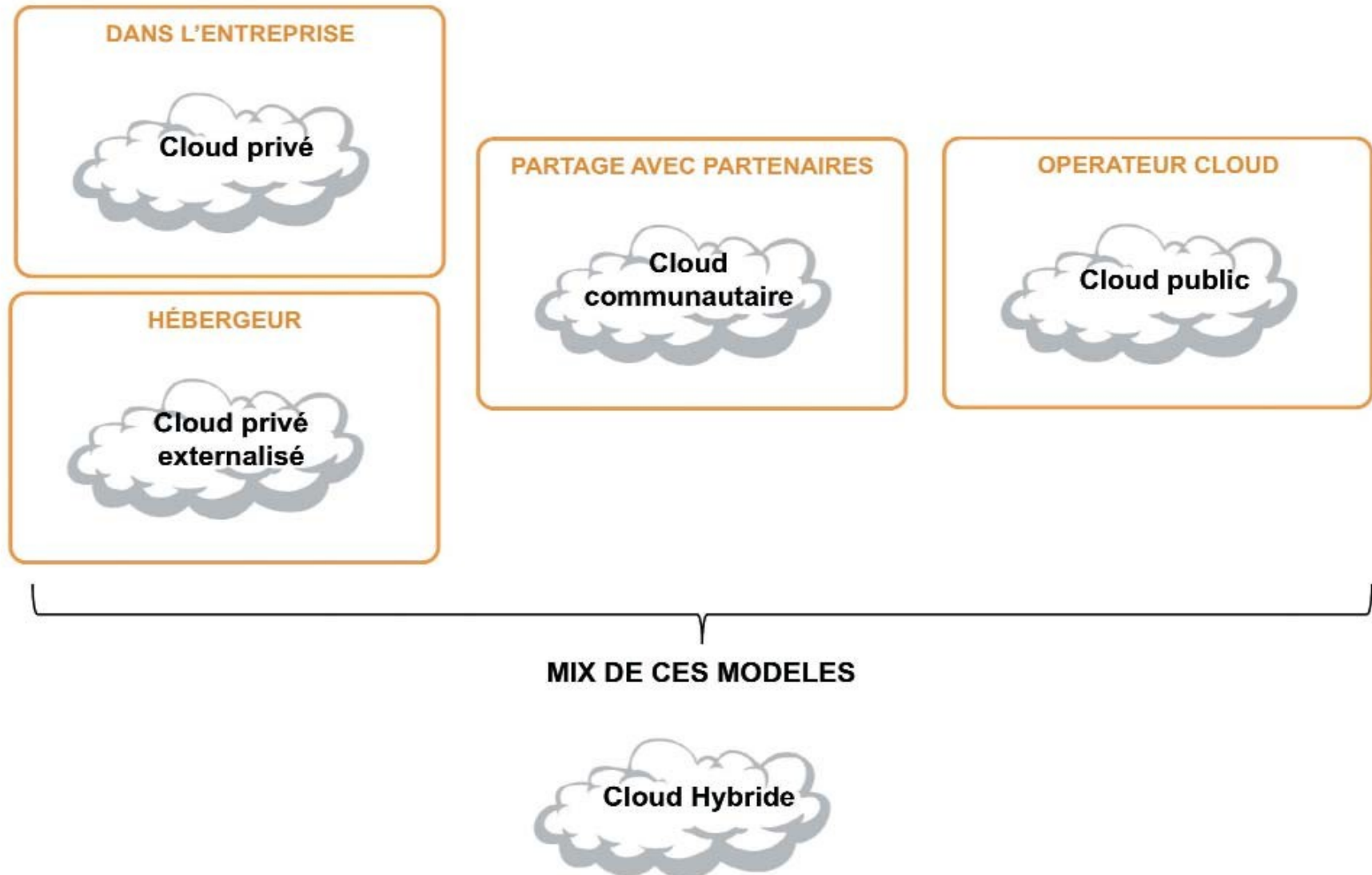
<http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>



Modèle de services



Modèle de déploiement



Des enjeux énergétiques

- Google : 0,01% électricité mondiale
création de la filiale Google Energy
- Free-cooling
- P.U.E. : Power Usage Effectiveness
Consommation globale du site / consommation
des équipements informatiques pendant 1 an.
[1,2 - 3]
- Taxe carbone

Opérations sur les machines virtuelles

- Allocations dynamique des ressources RAM, CPU, Disques, Bande Passante
- Installation, sauvegarde, déplacement
- Répartition des machines virtuelles (VM) sur les machines physiques pour optimiser les charges système et la consommation d'énergie
- Sécurité, environnement de test
- Livraison d'applicatif (appliance virtuelle)

USA Patriot Act

Uniting and Strengthening America by Providing
Appropriate Tools Required to Intercept and Obstruct
Terrorism Act of 2001

Les services de sécurité américains peuvent accéder aux
données à caractère personnel

Cela concerne les données hébergées

- sur le continent américain par n'importe quelle société
- par des sociétés de droit américain n'importe où

http://www.fincen.gov/statutes_regs/patriot/

Secure Socket Layer SSL

Protocole simplifié

- 1) Le client fait une demande de transaction sécurisée au serveur.
- 2) Le serveur envoie son certificat.
- 3) Le client vérifie que le certificat délivré est valide. Si la vérification est correcte alors le client envoie au serveur une clé symétrique chiffrée à l'aide de la clé publique du serveur qui sera donc le seul à pouvoir déchiffrer.
- 4) Cette clé sera utilisée pour échanger les données en toute sécurité.

Licence Affero-GPL

à destination des services types SaaS

- Dérivée de la licence GPL
- Plus l'obligation de délivrance des codes sources lors de l'usage du logiciel sur le réseau
 - Garantit la reproductibilité et l'évolutivité d'un logiciel hébergé
 - La licence porte uniquement sur le logiciel et non sur les données transmises par son biais



Protection de la vie privée

Utiliser

- les logiciels libres
- le chiffrement point à point
- des systèmes décentralisés

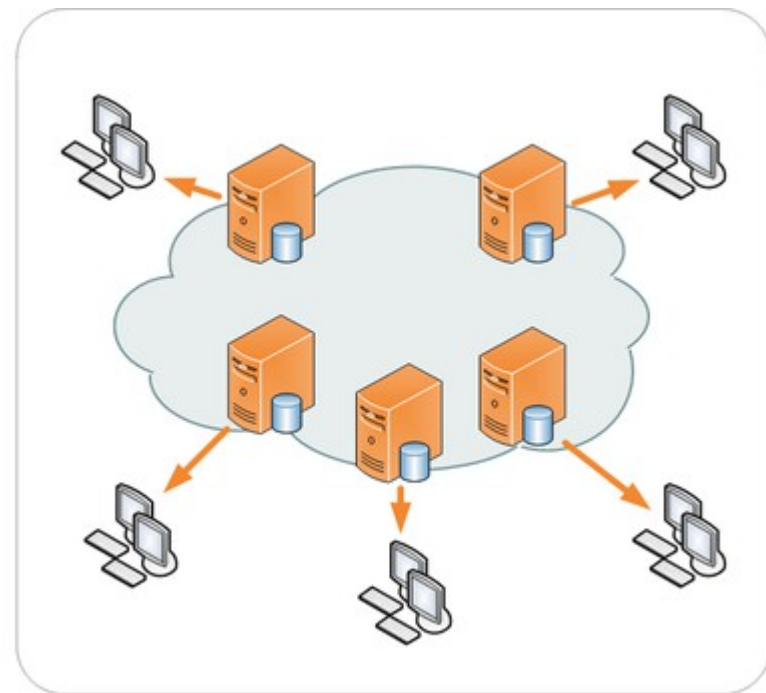
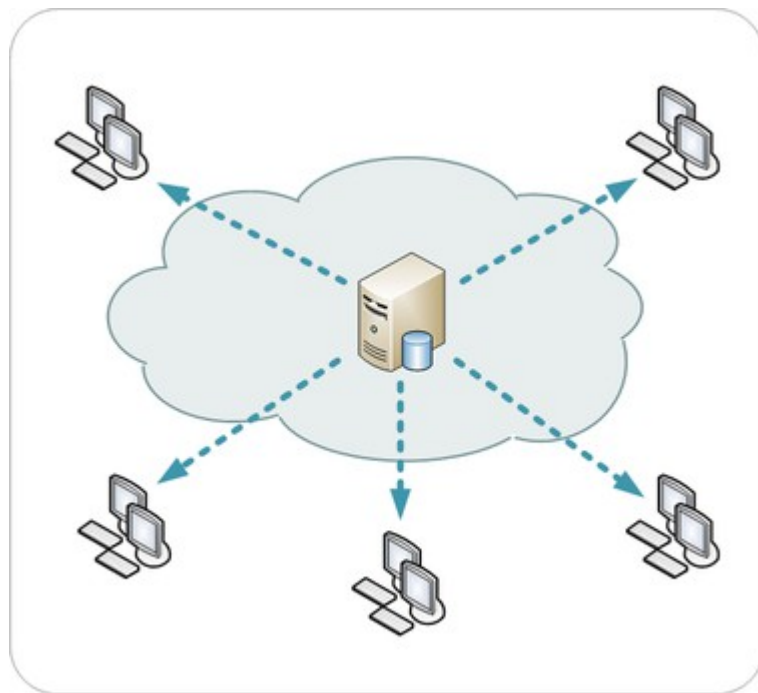
La gestion des données des critiques

- Transaction début – fin (commit - rollback)
- Propriétés ACID
 - Atomicité → une transaction en tout ou rien
 - Cohérence → respect des contraintes
 - Isolation → transactions simultanées
 - Durabilité → résistance aux pannes
- Pseudo transactionnel
- Difficulté : combiner prop. ACID et élasticité

Les Content Delivery Network (CDN)

- Paris – Californie : + 45 ms
Paris – Sidney : + 85 ms
- Amazon a estimé que 100 millisecondes de temps de chargement supplémentaires entraînent 1% de ventes en moins
- Fabriquer des noeuds où les contenus statiques sont répliqués au plus proche de l'internaute

Les Content Delivery Network (CDN)



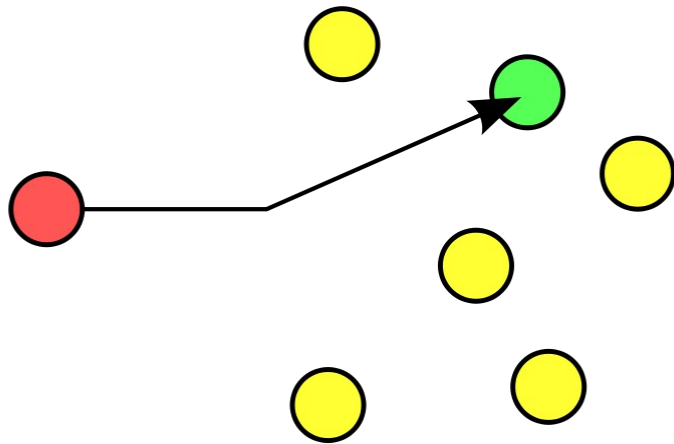
Les métriques des CDN

- Géographique → GeoDNS
- Réseau → DNS Anycast
- Calculée en temps réel
- Pair à pair

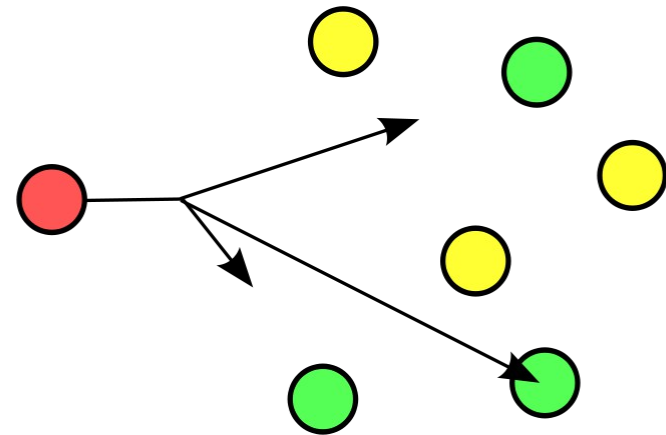
CDN : Métrique géographique GeoDNS

- Base de données géographique des adresses IP (produits de la société maxmind : GeoIP)
- Configuration particulière du DNS
- Faible coût

Adresse anycast (RFC 4786)



Adresse IP Unicast



Adresse IP Anycast

CDN : Métrique réseau

- Le DNS possède une adresse anycast et renvoie une adresse unicast d'un serveur HTTP proche.
- Le DNS possède une adresse quelconque et renvoie une adresse anycast de serveur HTTP qui répond par un redirect HTTP vers un serveur unicast proche.

Systeme à CDN Multiples

- Base de données Cedexis : collecte de données
(1,3 milliard de mesures / jour)
 - des éditeurs web livrent des pages qui contiennent des sondes pour faire des mesures sur les Cloud et CDN
- Utilisation de mesures temps réel (cdn-tech.com)

Évaluer les temps de réponse

www.cedexis.com/fr/radar/speedtest.html#cdn

- 1) Temps de connexion http = temps de résolution dns + temps de connexion tcp (petit objet)
- 2) Temps de réponse http = utilise la connexion tcp ouverte par la première mesure (petit objet)
- 3) Débit HTTP = utilise la connexion tcp déjà ouverte (gros objet)

Systeme à CDN Multiples

l'url de la ressource est : `cdn.mon_domaine.org`

c'est un CNAME vers `789456.cedexis.com`

Suivant les mesures collectées, ce nom de domaine sera :

- soit un CNAME vers `132456.akamay.com` ou
- soit un CNAME vers `456963.cdn77.net`

Le TTL est paramétrable (20s)



Systeme à CDN Multiples

- Netflix (30 % du trafic descendant aux US)
- Utilisation de plusieurs CDN en simultané pour le streaming vidéo
- Changement de CDN si débit $< 100\text{Kbps}$
- groupe de travail CDN Interconnection (cdni) de l'IETF → plusieurs RFC

Systeme pair-à-pair

- Chaque client est aussi un serveur
- Fichiers, Flux (streaming), calcul réparti, service (téléphonie, bureau distant ...) ...
- Élasticité
- Architectures
 - centralisées
 - décentralisées structurées : recherche logarithmique
 - décentralisées : recherche exponentielle



WebRTC

- Web Real-Time Communication
- Communications temps réel entre navigateurs : voix sur IP, visioconférence, pair-à-pair
- API javascript et HTML5
- 58 % des navigateurs
- projet porté par Google, Mozilla and Opera
- Depuis 2011 : API (W3C), protocole (IETF)

CDN pair à pair

- PeerCDN (bêta)
- Réduction de bande passante
- Javascript
- Plus de visiteurs → plus d'hébergeur
- Utilisation de WebRTC
- Fonctionne avec les autres CDN
- Sécurisé, Fiable

Amazon Simple Storage Service S3

- Calcul de coût pour un projet à +2To/an en progression linéaire, on recherche une visibilité sur 5 ans

First 1To 1 GB / mois = \$0,125

Next 49To 1 GB / mois = \$0,110

1\$ = 0,772€

10 To / 5 ans = ? €

- Transfert in \$0, out \$0,120
- Requête GET \$0,01/10 000 autres \$0,01/1000