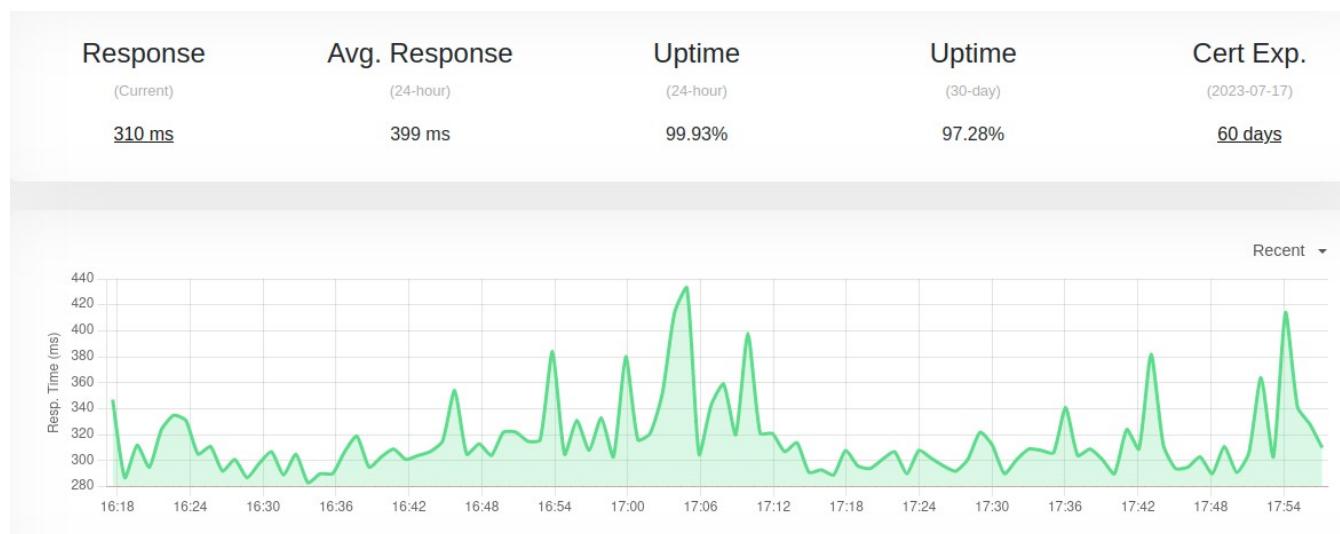


# Supervision et métrologie



# Introduction

---

# Introduction

- **Objectifs du cours :**

- Comprendre les notions de « *supervision* » et de « *métrie* »
- Comprendre les enjeux de la supervision et de la métrologie dans le *contexte* d'une entreprise, d'un point de vue technique comme d'un point de vue économique
- Être capable d'identifier les *assets* à superviser et de sélectionner les méthodes et outils adaptés
- Partager des *retours d'expériences* et débattre sur des cas d'usage ou des approches

# Introduction

- **Plan de cours :**

- La supervision « traditionnelle »
  - Pourquoi superviser ? 
  - Protocoles utilisés
  - Cas d'usage
- La métrologie
- La supervision « étendue »
  - Logs, sécurité, réseau...
- Gouvernance et « hypervision »

# Introduction

- **Évaluations :**

- 1 QCM (15 min) à la fin de chaque cours
    - 3 notes sur 15
  - 1 note de TP
    - 1 note sur 15 répartie en plusieurs petits exercices

# Introduction

- **Qui suis-je ?**

- Sysadmin, netadmin, gestion de projet, formation
- Aujourd'hui chez 3Liz, éditeur Open Source de SIG et hébergeur SaaS
- Plusieurs expériences professionnelles :
  - FAI, équipementier, sécurité/IAM, SSII, hébergeur/infogéreur, Cloud provider...
- Plusieurs centres d'intérêts :
  - Stockage, sauvegarde, réseau, logiciel libre...
  - Les trains, Snowrunner, WoW, les 4X, le tir à l'arc et la cuisine (végétarienne/végane)



# Introduction

LizMap Demo

Montpellier - Transports

Street, City

Locating

Districts

Sous-Quartiers

Legend

- Edition layers
- Points of interest
- Bicycle rides
- Areas of interest

- Transport
- Bus
- Stops
- Bus lines

- Tramway
- Stops
- Tramway lines

- Districts
- Sous-Quartiers

Base Layer

MapQuest OSM

2 km 1 mi 1 : 144 000

Data CC-By-SA by OpenStreetMap Powered by 3Liz

3Liz

# La supervision

---

# **Supervision : études de cas**

# Etudes de cas : énoncé

- **Contexte :**
  - 4 profils d'entreprise = 4 groupes
- **Objectifs :**
  - Lister les assets à superviser (listes non exhaustives !)
- **Vous avez 15 min** 

# Vos 4 entreprises

- **1 : TPE/PME industrielle** 
  - 1 usine de production avec machines-outils et hangars, 2 agences de bureaux, des connexions directes avec les fournisseurs/clients/transporteurs pour l'optimisation des flux de production
- **2 : Centre Hospitalier** 
  - 3 sites, 80 serveurs, 500 PC (administratif et salles d'examens), 2000 équipements médicaux
- **3 : Fournisseur d'accès à Internet** 
  - 2 datacentres, 9 POP, 4 transitaires, 4000 fibres/xDSL
- **4 : Cloud Provider** 
  - 20 datacentres, 200000 serveurs, 1,5 millions d'instances VPS, 1 million de clients

# Etude de cas : entreprise 1

- **TPE/PME industrielle**
  - Les PC de contrôle + les machines-outils (télémaintenances tierces ?)
  - L'état des liaisons avec les partenaires (tunnels de commandes, VPN, API...)
  - Les éléments de sécurité (caméras, alarmes, détecteurs...)
  - Les switchs et bornes Wifi de l'usine, des hangars et des bureaux
  - Les serveurs applicatifs et de gestion du parc (si existants)
  - *Les PC des employés ?*
  - **Un arrêt des tunnels de commandes = un arrêt de production = perte financière**

# Etude de cas : entreprise 2

- **Centre hospitalier**

- Les serveurs et VM de gestion du parc (applications métiers/médicales)
- Les switchs et bornes Wifi (roaming appareils médicaux)
- **Les téléphones et systèmes d'alertes des personnels médicaux**
- **Les PC des salles d'examens et d'opérations**
- **Les équipements médicaux (télémaintenance avec une entreprise spécialisée)**
- ***Le site internet de l'hôpital ?***
- **Un équipement médical indisponible ou un PC de salle d'opération trop long à ouvrir une session = des vies en jeu**



# Etude de cas : entreprise 3

- **Fournisseur d'accès à Internet**

- Les serveurs et VM de gestion du parc
- **Les équipements réseaux :**
  - Cœur de réseau
  - Équipements de collecte sur les POP
  - Équipements de livraison chez les clients
- **Les liens avec les transitaires (sessions BGP)**
- **La latence vers différents points vitaux d'Internet (serveurs racine DNS, NTP...)**
- ***L'état des zpools des serveurs de sauvegarde ?***

# Etude de cas : entreprise 4

- **Cloud Provider**

- Le parc de serveurs physiques (état du matériel, état des stocks...)
- Le taux d'occupation et les capacités électriques et de refroidissement des salles
- Les plateformes de virtualisation (état, capacité...)
- Les connexions vers l'extérieur (transits, peering, liens inter-datacentres...)
- **L'état des sites web hébergés (codes de retours, temps de réponse...)**
- **Les délais de livraisons des instances VPS aux clients**
- ***L'état des barrettes mémoires des serveurs ?***

# Bilan de l'étude de cas

- **Ne pas se focaliser uniquement sur l'IT !**
- Garder en tête :
  - Le but de l'entreprise (*qu'est-ce que nous livrons à nos clients ?*)
  - La qualité de service (*est-ce que le service est rendu dans de bonnes conditions ?*)
  - Les moyens à mettre en œuvre pour superviser les assets (*coûts financiers, techniques et humains*)

# La supervision : pourquoi ?

# Définition

« La supervision est une technique **industrielle** de suivi et de pilotage informatique de procédés de fabrication automatisés. La supervision concerne l'acquisition de données (mesures, alarmes, retour d'état de fonctionnement) et des paramètres de commande des processus généralement confiés à des automates programmables.

**Dans l'informatique, la supervision est la surveillance du bon fonctionnement d'un système ou d'une activité. »**

Source : Wikipédia

# Pourquoi superviser ?

(pour le plaisir de se faire réveiller la nuit en astreinte !)



- D'un point de vue **technique** :
  - Valider l'état de fonctionnement d'une machine ou d'un service
  - Anticiper le dépassement des capacités d'un environnement
  - Anticiper les pannes et les remplacements de matériel, ou les mises à jour applicatives
- D'un point de vue **fonctionnel** :
  - Valider le service rendu aux clients (SLA...)
  - Mieux gérer et anticiper les budgets (achats, formations, JH...) A small icon of a dollar bill with wings, symbolizing money that can fly or be used effectively.

# **La supervision : comment ?**

# Comment superviser ?

- Plusieurs types de supervision :
  - **Système** (CPU, RAM...)
  - **Réseau** (débits, disponibilité...)
  - **Applicative** (validation fonctionnelle)
- Utilisation de différents protocoles et de différentes méthodologies selon les besoins
- Les protocoles « classiques » sont pensés à la fois pour **superviser et administrer**
- **Une bonne supervision requiert un bon *inventaire* !**

# Une histoire d'assets...



# Qu'est-ce qu'un asset ?

- Un asset est un **composant du système d'information**
- Un asset possède une **valeur** pour l'entreprise, des **attributs** et un **cycle de vie**
- Quelques exemples d'assets :
  - Un équipement réseau
  - Un disque dur
  - Un nom de domaine
  - Une licence Minecraft
  - ***Un employé ?***
  - ***Un conteneur Docker ?***

# La CMDB, le cœur du SI

- **CMDB : Configuration Management Database**
- **Base de données** fondamentale d'une architecture ITIL unifiant tous les assets d'un système d'informations :
  - **Inventaire** (équipements, licences...)
  - Disponibilité et **utilisation des assets**
  - Attributs et configurations (peut entrer en conflit avec les outils de Configuration Management !)
  - **Liens entre les assets** (câblage, dépendances...)
  - **Historique et suivi** (modifications, pannes...)
- **Peut être composée de plusieurs outils complémentaires (/\!\!)**
- **Pas de CMDB = supervision incomplète !**



# CMDB, DCIM, IPAM...

- **IPAM** : IP Address Management
  - **ITSM** : IT Asset Management
  - **DCIM** : Datacenter Infrastructure Management
- 
- Chaque outil est adapté à un **besoin métier**
  - **Un outil qui couvre tous les aspects d'un SI n'existe pas !**
- 
- Beaucoup d'outils disponibles :
    - GLPI
    - RackTables
    - iTop
    - NetBox
    - ...



# Quelques outils de gestion d'assets

**RackTables**

Hello, RackTables Administrator. This is RackTables 0.17.1. Click [here](#) to logout.

MyCompanyName: Main page: Objects: london router

Search:

View Properties Rackspace Ports IPv4 NATv4 Tags Files

**london router**

**summary**

Common name: london router  
Object type: Router  
Asset tag: net247  
Visible label: bbtr1  
HW type: Cisco 7206VXR  
Explicit tags: London, testing  
Implicit tags: west, Geo

**ports and links**

Local name	Visible label	Port type	L2 address	Rem. Object	Rem. port
fa2/0		RJ-45/100Base-TX	00:00:00:00:A0:01	londonswitch1	g8
fa2/1		RJ-45/100Base-TX	00:00:00:00:A0:02	Reserved:	ISP uplink
sel/0	sync serial		New-York router 1	sel/1	
sel/1	sync serial		moscow router	sel/0	

**IPv4 addresses**

OS interface	IP address	peers
sel/1	10.200.0.1/31	
sel/0	10.200.0.2/31	
fa2/0	10.200.1.62/26 R (default gw)	

**rackspace allocation**

London : L02

Front	Interior	Back
12		
11		
9		
8		
7	londonswitch1	
6	[PDU]	
5	london LB	
4		
3		
2	london-NAS	
1		

**109.72.89.0 /25**

**Public Web Hosting**  
IPv4 leaf network, Operational  
Public farms  
220 (inherited) (HQ) New Orleans, LA (inherited) info@samplecompany.com, +1 234 567 890

Child subnetworks: 0  
Child nodes: 52 (41% Free)  
Utilization: 240  
Enabled TCP services: Manage

Allocation scheme for 52 child nodes

**IP Ranges**

Range	Utilization	Type	Name	Description
109.72.89.1 - 109.72.89.10	80%	Generic	Network Equipment	Static IP's
109.72.89.20 - 109.72.89.39	20%	Generic	Legacy group	To be migrated
109.72.89.100 - 109.72.89.126	63%	DHCP	Dynamic server farms	

**IP Nodes**

Address	Name	Type	Status	Last response	TCP Services	Description	Contact
109.72.89.0	Network address						
109.72.89.1	router03.2tc1.nl	Router (virtual)	Operational	17 ms	0	Auto discovered	
109.72.89.2	router04.2tc1.nl	Router	Allocated	15 ms	0	Auto discovered	
109.72.89.3	gateway03.2tc1.nl	Gateway	Operational	16 ms	0	Auto discovered	
109.72.89.4	gateway04.2tc1.nl	Gateway	Temporary	16 ms	0	Auto discovered	
109.72.89.5	pdu01.2tc1.nl			18 ms	3	Auto discovered	
109.72.89.9	fw01.2tc1.nl	Firewall	Operational	16 ms	1	Auto discovered	
109.72.89.15	hosted.by.huizinga.nl			23 ms	7	Auto discovered	
109.72.89.16	pdu03.2tc1.nl			17 ms	4	Auto discovered	
109.72.89.17	pdu04.2tc1.nl	Server	Pending	15 ms	0		
109.72.89.20	server02.huizinga.nl	Server (virtual)	Legacy	15 ms	8	Auto discovered	
109.72.89.21	hosted.by.huizinga.nl	Server (virtual)	Legacy	15 ms	7	Auto discovered	
109.72.89.23	hosted.by.huizinga.nl	Server (virtual)	Legacy	15 ms	8	Auto discovered	
109.72.89.24	rmedia01.2tc1.nl	Server (virtual)	Legacy	14 ms	7	Auto discovered	
109.72.89.40	vps02.huizinga.nl			15 ms	4	Auto discovered	

# Quelques outils de gestion d'assets

The screenshot shows the GLPI (General Linux Infrastructure Planner) web interface. The top navigation bar includes links for Inventory, Assistance, Management, Tools, Plugins, Administration, and Setup, along with a search bar and a logout link for the 'admin' user.

The main content area displays a list of 'Computers' under the 'Inventory > Computers' path. The list includes columns for Name, Entity, Status, Manufacturer, Serial Number, Type, Model, OS, Location, Last update, and Contact. The data shows various Dell workstations and servers, mostly running Red Hat Enterprise Linux Client release 5.3 (Tikanga), with some exceptions like Mandriva Linux Corporate Server and PowerEdge models.

Name	Entity	Status	Manufacturer	Serial Number	Type	Model	OS	Location	Last update	Contact
planetx	CS	Dell	7ZS7Z91	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:05		
pluto	CS	Dell	GXS7Z91	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41		
populous	CS	Dell	10J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	niranjan	
quake	CS	Dell	B1J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	jim	
railroadtycoon	CS	Dell	C0J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	bobo	
rainbowsix	CS	Dell	20J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41		
rook	CS	Dell	1FVBVB1	Workstation	PowerEdge 850	Red Hat Enterprise Linux Server release 5.4 (Tikanga)	NA	2009-11-12 17:41	root	
safe	CS	Dell	GDVBVB1		PowerEdge 850	Red Hat Enterprise Linux Server release 5.3 (Tikanga)	NA	2009-11-12 17:47	root	
secondlife	CS	Dell	51J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41		
simcity	CS	Dell	G0J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	Inguyen	
snowstorm	CS	Dell	HK17481		PowerEdge 1850	Mandriva Linux Corporate Server release 2006.0 (Official) for i586	CS	2009-11-11 15:27	root	
starcraft	CS	Dell	7ZH4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	sykim	
surf-umans	CS	Dell	H1STM11	Workstation	Precision WorkStation 340	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	niranjan	
tsunami	CS	Dell	FBD5281		PowerEdge 2850	Mandriva Linux Corporate Server release 2006.0 (Official) for i586	NA	2009-11-10 18:33	root	
ultima	CS	Dell	60J4481	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	yo2seol	
uranus	CS	Dell	3ZS7Z91	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	swittman	
venus	CS	Dell	FYS7Z91	Workstation	OptiPlex GX620	Red Hat Enterprise Linux Client release 5.3 (Tikanga)	NA	2009-11-12 17:41	Itsungju	

... et de protocoles



# Supervision et protocoles : SNMP

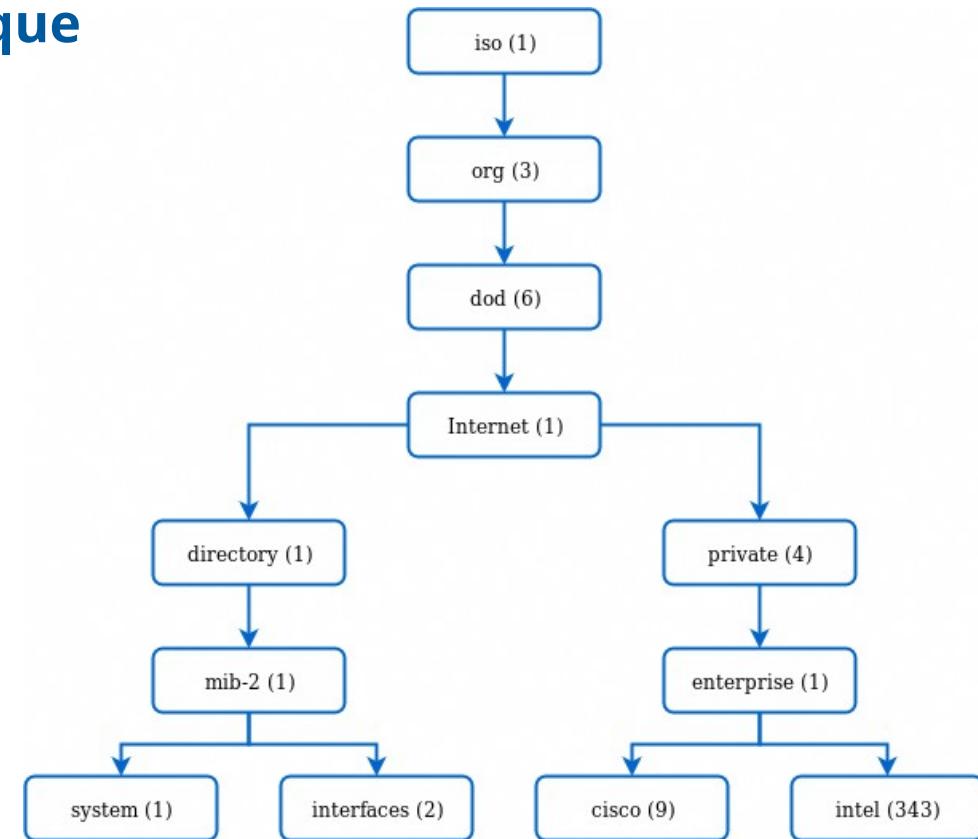
« Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de **gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.** »

Source : Wikipédia

- Crée en 1988
- RFC 1067 et 1157
- Ports UDP 161 et 162 

# OID (Object Identifier)

- Structure d'identification **hiérarchique**
- Standard de l'ITU-T et de l'ISO
- **Un « OID » = un nœud de l'arbre**
- Chaque nœud est contrôlé par un organisme ou une entreprise
- Exemples :
  - 1 : ISO
  - 1.3.6 : Department of Defense
  - 1.3.6.1.4.1.343 : Intel Corporation



# ASN.1 et SMI

- ASN.1 : Abstract Syntax Notation One
  - Standard pour décrire la structure des données
- **SMI : Structure of Management Information**
  - Adaptation d'ASN.1 pour définir les objets d'une MIB
- 3 exemples d'attributs standardisés :
  - **Objects Identifiers** (forme numérique ou littérale)
    - 1.3.6.1.2.1 ou *iso.org.dod.internet.mgmt.mib-2*
  - **Objects Types** : integer, string, IP address...
  - **Object Encoding Method** (comment transmettre cette donnée)

# MIB (Management Information Base)

- **Structure de données hiérarchique**
- Chaque entrée est associée à un OID
- Souvent définie sous forme de « **modules** »
  - Plus de 300 MIBs standardisées (SNMPv2-MIB, IP-MIB...)
  - Et les autres sont créées et maintenues par les fabricants
- Accessible via un agent côté client
- Pour trouver l'OID qui nous intéresse, il est parfois nécessaire d'utiliser un « **MIB Browser** »



# Une MIB en image

Screenshot of OidView Professional interface showing the MIB Tree and LiveGrid for the object ipNetToMediaEntry.

**MIB Tree:**

- (15) ipReasmOKs
- (16) ipReasmFails
- (17) ipFragOKs
- (18) ipFragFails
- (19) ipFragCreates
- (20) ipAddrTable
- (21) ipRouteTable
- (22) ipNetToMediaTable
  - (01) ipNetToMediaEntry
    - (01) ipNetToMediaIndex
    - (02) ipNetToMediaPhysAddress
    - (03) ipNetToMediaNetAddress
    - (04) ipNetToMediaType
  - (23) ipRoutingDiscards
  - (24) ipForward
- (005) icmp
- (006) tcp
- (007) udp
- (008) egp
- (010) transmission

**LiveGrid:**

Object	ipNetToMediaIndex	Type	Value
ipNetToMediaNetAddress: 192.168.1.2	3	INTEGER	3
ipNetToMediaPhysAddress	3	OCTET-STRING	00:60:97:A1:D1:21
ipNetToMediaNetAddress	3	IPADDRESS	192.168.1.2
ipNetToMediaType	3	INTEGER	dynamic(3)
ipNetToMediaNetAddress: 192.168.1.20	3	INTEGER	3
ipNetToMediaPhysAddress	3	OCTET-STRING	00:50:0F:05:CE:4A
ipNetToMediaNetAddress	3	IPADDRESS	192.168.1.20
ipNetToMediaType	3	INTEGER	other(1)

The dropdown menu for ipNetToMediaType shows options: other(1), invalid(2), dynamic(3), static(4).

**Variable Grid:**

Object	OID	Module	Object Type
ipNetToMediaEntry	1.3.6.1.2.1.4.22.1	IP-MIB	OBJECT-TYPE
ipNetToMediaIndex	1.3.6.1.2.1.4.22.1.1	IP-MIB	OBJECT-TYPE
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3	IP-MIB	OBJECT-TYPE
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2	IP-MIB	OBJECT-TYPE
ipNetToMediaTable	1.3.6.1.2.1.4.22	IP-MIB	OBJECT-TYPE
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4	IP-MIB	OBJECT-TYPE
ipOutDiscards	1.3.6.1.2.1.4.11	IP-MIB	OBJECT-TYPE
ipOutNoRoutes	1.3.6.1.2.1.4.12	IP-MIB	OBJECT-TYPE
ipOutRequests	1.3.6.1.2.1.4.10	IP-MIB	OBJECT-TYPE
ipReasmFails	1.3.6.1.2.1.4.16	IP-MIB	OBJECT-TYPE

**MIB Info:**

**ipNetToMediaType**  
SMIv2 OBJECT-TYPE

**Syntax Enumeration:**

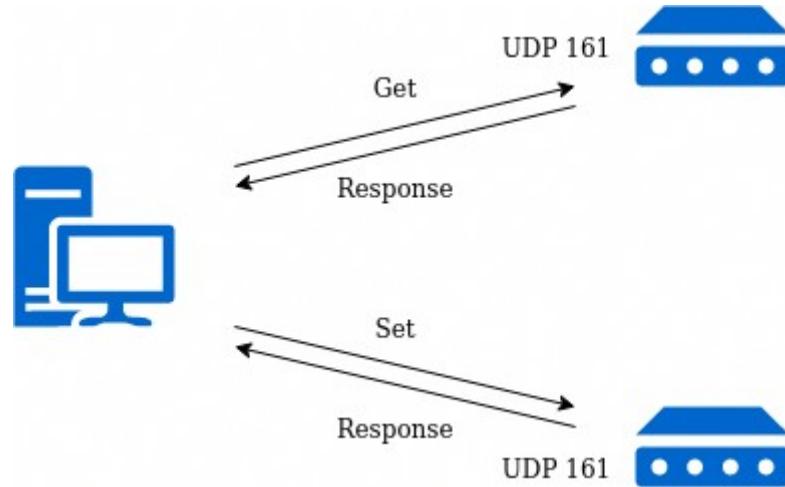
- other(1)
- invalid(2)
- dynamic(3)
- static(4)

**MAX-ACCESS:** READ-CREATE  
**STATUS:** current  
**DESCRIPTION:** The type of mapping.

**OID PATH:** iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4).ipNetToMediaTable(22).ipNetToMediaEntry(1)

POLL FILE SNMP ICMP

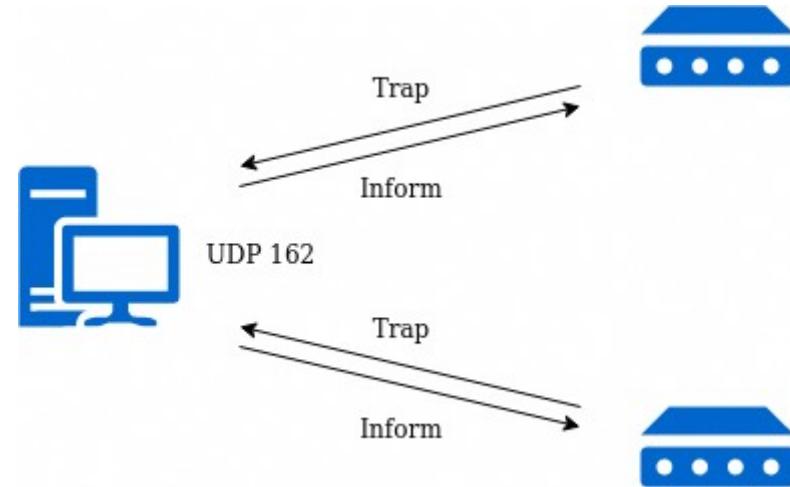
# SNMP : architecture client-serveur



- Schéma d'une PDU :

Version	Community	PDU Type	Request ID	Error Status	Error Index	Variable Binding List
---------	-----------	----------	------------	--------------	-------------	-----------------------

# SNMP : traps



- Schéma d'une PDU de type « trap » :

Version	Community	PDU Type	Enterprise Object Identifier	Network Address	Trap Type	Specific Trap Type	Timestamp	Variable Binding List
---------	-----------	----------	------------------------------	-----------------	-----------	--------------------	-----------	-----------------------

# SNMP v1

- **Compteurs 32 bits**
- **Echanges en clair (PDUs et communautés)**
- 5 PDUs :
  - *GetRequest* : demande une variable au client
  - *SetRequest* : définit une variable (obtient automatiquement une *Response* en retour)
  - *Response* : envoie une variable au serveur
  - *GetNextRequest* : demande la variable suivante au client
  - *Trap* : envoie spontanément une variable et l'OID correspondant au server

# SNMP v2(c)

- **Compteurs 64 bits**
- **Echanges en clair (PDUs et communautés)**
- 2 nouvelles PDUs :
  - *GetBulkRequest* : demande une série de variables au client
  - *InformRequest* : informe le client de la réception de son *Trap*
- ***Attention : format incompatible avec SNMPv1, nécessite une dual-stack ou un proxy***

# SNMP v3

- Focus sur la sécurité (authentification, confidentialité et intégrité), 3 modes d'utilisation :
  - *NoAuthNoPriv*
  - *AuthNoPriv*
  - *AuthPriv*
- MD5 et SHA pour l'authentification, CBC\_DES and CFB\_AES\_128 pour le chiffrement
- 1 nouvelle PDU :
  - *Report* : utilisée comme message « d'erreur »
- Reconnu comme standard par l'IETF depuis 2004

# SNMPwalk en image

```
librenms@librenms:~$ snmpwalk -v 2c -c toto 127.0.0.1
iso.3.6.1.2.1.1.1.0 = STRING: "Linux librenms 5.3.13-1-pve #1 SMP PVE 5.3.13-1 (Thu, 05 Dec 2019 07:18:14 +0100) x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (602) 0:00:06.02
iso.3.6.1.2.1.1.4.0 = STRING: "admin@toto.fr"
iso.3.6.1.2.1.1.5.0 = STRING: "librenms"
iso.3.6.1.2.1.1.6.0 = STRING: "OVH"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.32 = INTEGER: 32
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
iso.3.6.1.2.1.2.2.1.2.32 = STRING: "eth0"
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.3.32 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 65536
iso.3.6.1.2.1.2.2.1.4.32 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 10000000
iso.3.6.1.2.1.2.2.1.5.32 = Gauge32: 4294967295
iso.3.6.1.2.1.2.2.1.6.1 = ""
iso.3.6.1.2.1.2.2.1.6.32 = Hex-STRING: FE C3 74 F7 DC 5C
```

# Supervision et protocoles : WMI

- **WMI : Windows Management Instrumentation**
  - Apparu avec Windows NT 4.0 (1996)
  - Permet de récupérer des informations sur des composants du système, des applications...
  - ... et permet de les configurer (CLI, scripts VBScript ou PowerShell, consoles GUI...)
- Permet aux développeurs d'exposer un « **modèle** » (**objets et relations**) à travers un « **provider** » WMI

# WMI en image

WMI Explorer 2.0

File Launch Help

Computer TIGZY-PC Connect Mode Asynchronous Synchronous Class Enumeration Options Filter: % Include System Classes Include Perf Classes Include CIM Classes Include MSFT Classes Refresh Classes

Namespaces \\\TIGZY-PC\ROOT

- ROOT\aspnet
- ROOT\CIMV2
  - ROOT\CIMV2\Applications
  - ROOT\CIMV2\ms\_409
  - ROOT\CIMV2\ms\_40c
  - ROOT\CIMV2\power
  - ROOT\CIMV2\Security
  - ROOT\CIMV2\TerminalServices
- ROOT\Cli
- ROOT\DEFAULT
- ROOT\directory
- ROOT\Interop
- ROOT\Microsoft
- ROOT\nap
- ROOT\Policy
- ROOT\RSSOP
- ROOT\SECURITY
- ROOT\SecurityCenter
- ROOT\SecurityCenter2
- ROOT\ServiceModel
- ROOT\subscription
- ROOT\WMI
  - ROOT\WMI\ms\_409
  - ROOT\WMI\ms\_40c

Classes (378) Search Quick Filter: Classes

Name	Lazy ...	Description
Win32_PortableBattery	False	La classe
Win32_PortConnector	False	La classe
Win32_PortResource	False	La classe
Win32_POTSModem	False	La classe
Win32_POTSModemToSeri...	False	La classe
Win32_PowerManagement...	False	La classe
Win32_Printer	False	Fonctionn
Win32_PrinterConfiguration	False	La classe
Win32_PrinterController	False	La relation
Win32_PrinterDriver	False	CIM_Serv
Win32_PrinterDriverDLL	False	Associati
Win32_PrinterSetting	False	La classe
Win32_PrinterShare	False	Associati
Win32_PrintJob	False	CIM_Job
Win32_PrivilegesStatus	False	La classe
Win32_Process	False	La classe
Win32_Processor	False	La classe
Win32_ProcessStartTrace	False	La classe
Win32_ProcessStartup	False	La classe
Win32_ProcessStopTrace	False	La classe
Win32_ProcessTrace	False	Cet événé

Instances (54) Properties (45) Methods (6) Query Script Logging Instance Options Quick Filter: Show Null Values Show System Properties Refresh Instances Refresh Objects

Instances
Win32_Process.Handle="0"
Win32_Process.Handle="1060"
Win32_Process.Handle="1124"
Win32_Process.Handle="1176"
Win32_Process.Handle="1348"
Win32_Process.Handle="1392"
Win32_Process.Handle="1536"
Win32_Process.Handle="1656"
Win32_Process.Handle="1736"
Win32_Process.Handle="1748"
Win32_Process.Handle="1896"
Win32_Process.Handle="2076"
Win32_Process.Handle="2144"
Win32_Process.Handle="2172"
Win32_Process.Handle="2404"
Win32_Process.Handle="2448"
Win32_Process.Handle="2480"
Win32_Process.Handle="2572"
Win32_Process.Handle="276"

Properties

*Handle	1348
Caption	svchost.exe
CreationClassName	Win32_Process
CreationDate	20160919080545.138
CSCreationClassName	Win32_ComputerSystem
CSName	TIGZY-PC
Description	svchost.exe
HandleCount	311
KernelModeTime	15781250
Name	svchost.exe
OSCreationClassName	Win32_OperatingSystem
OSName	Microsoft Windows 7
OtherOperationCount	14312
OtherTransferCount	700610

Name Type - String  
La propriété Name définit le nom par lequel l'objet est connu. Lorsqu'elle est mise sous forme de sous-classe, la propriété Name peut être ignorée pour être une propriété Key.

WQL Query (Selected Object)

Query SELECT \* FROM Win32\_Process WHERE Handle='1348' Execute

Retrieved 378 classes from ROOT\CIMV2 that match specified criteria. Retrieved 54 instances from Win32\_Process Time to Enumerate Instances: 00:00.034

# Supervision et protocoles : IPMI

- **IPMI : Intelligent Platform Management Interface**
  - Introduit par Intel en 1998, utilisé par plus de 200 fabricants aujourd'hui
  - Fournit des interfaces pour **superviser et configurer « out-of-band » des éléments indépendants du système d'exploitation** (BIOS, cartes-filles, firmwares...)
  - Un module IPMI est organisé autour d'un Baseboard Management Controller (BMC), ainsi que de capteurs (températures, vitesses de rotation des ventilateurs...) et de microcontrôleurs
- Exemples d'interfaces exploitant IPMI :
  - **iDRAC** (Integrated Dell Remote Access Controller) chez Dell
  - **iLO** (Integrated Lights-Out) chez HPE

# Un exemple de console utilisant IPMI

Integrated Dell Remote Access Controller 7 Enterprise Support | About | Logout

System PowerEdge R920 root, Admin

Overview Server Logs Power / Thermal Virtual Console Alerts Setup Troubleshooting Licenses Intrusion iDRAC Settings Hardware Storage

Power Monitoring Voltages Temperatures

## Temperatures

Fresh Air

Not a Fresh Air Compliant Configuration

### Temperature Probes

Status	Probe Name	Reading	Warning Threshold		Critical Threshold	
			Min	Max	Min	Max
✓	CPU1 Temp	37 °C (98.6 °F)	8 °C (46.4 °F)	78 °C (172.4 °F)	3 °C (37.4 °F)	83 °C (181.4 °F)
✓	CPU2 Temp	38 °C (100.4 °F)	8 °C (46.4 °F)	78 °C (172.4 °F)	3 °C (37.4 °F)	83 °C (181.4 °F)
✓	CPU3 Temp	41 °C (105.8 °F)	8 °C (46.4 °F)	78 °C (172.4 °F)	3 °C (37.4 °F)	83 °C (181.4 °F)
✓	CPU4 Temp	37 °C (98.6 °F)	8 °C (46.4 °F)	78 °C (172.4 °F)	3 °C (37.4 °F)	83 °C (181.4 °F)
✓	System Board Exhaust Temp	37 °C (98.6 °F)	8 °C (46.4 °F)	70 °C (158.0 °F)	3 °C (37.4 °F)	75 °C (167.0 °F)
✓	System Board Inlet Temp	23 °C (73.4 °F)	3 °C (37.4 °F)	42 °C (107.6 °F)	-7 °C (19.4 °F)	47 °C (116.6 °F)

### System Board Temperature Historical Data

CSV Export

Total Operation Time	Time Spent in Warning Threshold Range	Time Spent in Critical Threshold Range
72 Days	0%	0%



# Supervision et protocoles : les API

- **API : Application Programming Interface**
  - Couche d'abstraction pour simplifier l'administration d'une application ou d'un équipement
  - De plus en plus d'éditeurs et de fabricants proposent une API, mais la standardisation reste compliquée (SOAP, **REST**...)
- Permettent de manipuler des données plus complexes
  - Retours en **XML**, ou en **JSON**, ou autre
- Permettent une gestion plus fine de la **sécurité** (authentification, chiffrement...)

# Utiliser une API : GET/POST HTTP

NX-API Developer Sandbox

Quick Start Logout

show ver

Message format: json-rpc  
xml json

Command type: cli  
cli\_ascii

POST Reset

REQUEST:

```
{  
    "jsonrpc": "2.0",  
    "method": "cli",  
    "params": {  
        "cmd": "show ver",  
        "version": 1  
    },  
    "id": 1  
}
```

Copy Python

RESPONSE:

```
{  
    "jsonrpc": "2.0",  
    "result": {  
        "body": {  
            "header_str": "Cisco Nexus Operating System (NX-OS) Software\\nTAC support: http://www.cisco.com/  
tac\\nCopyright (C) 2002-2014, Cisco and/or its affiliates.\\nAll rights reserved.\\nThe copyrights to ce  
rtain works contained in this software are\\nowned by other third parties and used and distributed unde  
r their own\\nllicenses, such as open source. This software is provided \"as is,\" and unless\\nothervis  
e stated, there is no warranty, express or implied, including but not\\unlimited to warranties of mercha  
ntability and fitness for a particular purpose.\\nCertain components of this software are licensed unde  
r\\nthe GNU General Public License (GPL) version 2.0 or \\nGNU General Public License (GPL) version 3.0  
or the GNU\\nLesser General Public License (LGPL) Version 2.1 or \\nLesser General Public License (LGPL  
Version 2.0. \\nA copy of each such license is available at\\nhttp://www.opensource.org/licenses/gpl-2  
.0.php and\\nhttp://opensource.org/licenses/gpl-3.0.html and\\nhttp://www.opensource.org/licenses/lgpl-2  
.1.php and\\nhttp://www.gnu.org/licenses/old-licenses/library.txt.\\n",  
            "bios_ver_str": "07.06",  
            "kickstart_ver_str": "6.1(2)I2(2a)",  
            "bios_cmpl_time": "03/01/2014",  
            "kick_file_name": "bootflash:///n9000-dk9.6.1.2.I2.2a.bin",  
            "kick_cmpl_time": " 6/3/2014 13:00:00",  
        }  
    }  
}
```

Copy

# Utiliser une API : Ansible et Cisco

```
- name: Nexus - Configuring spanning tree to pvst
  nxos_config:
    save_when: modified
    provider: "{{ provider }}"
    lines:
      - spanning-tree mode rapid-pvst
    match: line
  when: ('telnet' not in group_names) and
        ('nexus' in group_names)

- name: Catalyst - Pushing bpdufilter, bpduguard and recovery configuration
  ios_config:
    save_when: never
    authorize: yes
    provider: "{{ provider }}"
    lines:
      - spanning-tree portfast bpdufilter default
      - spanning-tree portfast bpduguard default
      - errdisable recovery interval 30
      - errdisable recovery cause bpduguard
    match: line
  when: ('telnet' not in group_names) and
        ('nexus' not in group_names)
  notify: save

- name: Nexus - Configuring default port to edge port
  nxos_config:
    save_when: modified
    provider: "{{ provider }}"
    lines:
      - spanning-tree port type edge default
    match: line
  when: ('telnet' not in group_names) and
        ('nexus' in group_names)

- name: Nexus - Pushing bpdufilter, bpduguard and recovery configuration
  nxos_config:
    save_when: modified
    provider: "{{ provider }}"
    lines:
      - spanning-tree port type edge bpdufilter default
      - spanning-tree port type edge bpduguard default
      - errdisable recovery interval 30
      - errdisable recovery cause bpduguard
    match: line
  when: ('telnet' not in group_names) and
        ('nexus' in group_names)
```



- API disponible **suivant le modèle...**
- ... et **la licence !**
- Dans le cas d'Ansible, certains modules utilisent l'API, sinon il faut se rabattre sur des modules qui exploitent la CLI...



# Supervision : petite conclusion

- **Le protocole à utiliser dépend du besoin et du contexte !**
- **Le plus répandu : SNMP**
  - **SNMPv3 encore très rare**, SNMPv1 toujours standard chez beaucoup d'équipementiers...
  - Sur certains équipements (ex : Ubiquiti ?), pourrait commencer à disparaître (pour forcer l'achat de licences pour utiliser les API ?)
  - Nécessite d'avoir les modules adéquats (ex : supervision d'un onduleur industriel)
- **Les API sont prometteuses**
  - Permettent de transmettre **plus de données**, et de **façon structurée** (JSON)
  - Permettent de mieux gérer **l'authentification et le chiffrement**
  - Encore peu disponibles, et nécessitent un serveur Web côté client

# Supervision : quelques outils du marché

# Commençons par du simple

- **Ping**

```
librenms@librenms:~$ ping 10.0.0.6
PING 10.0.0.6 (10.0.0.6) 56(84) bytes of data.
64 bytes from 10.0.0.6: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 10.0.0.6: icmp_seq=2 ttl=64 time=0.076 ms
^C
--- 10.0.0.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.053/0.064/0.076/0.014 ms
```

- **Telnet**

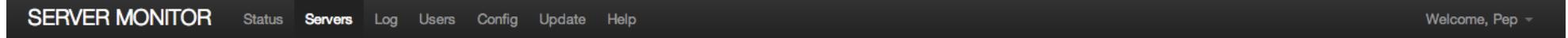
```
librenms@librenms:~$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
```

- **Curl**

```
librenms@librenms:~$ curl 127.0.0.1 80
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="refresh" content="0;url='http://127.0.0.1/login'" />

    <title>Redirecting to http://127.0.0.1/login</title>
  </head>
  <body>
    Redirecting to <a href="http://127.0.0.1/login">http://127.0.0.1/login</a>.
  </body>
</html>^C
```

# Un outil basique : PHP Server Monitor



## Servers

SERVERS

+ Add new

Update

	Label	Domain/IP	Port	Type	Latency	Last online	Monitoring	Send Email	Send SMS	Action
off	Example FTP	ftp.example.org	21	Service	0.0005 s	6 hours ago	Yes	Yes	Yes	
on	Gmail SMTP	smtp.gmail.com	465	Service	0.0129 s	about a minute ago	Yes	Yes	Yes	
on	Google	http://www.google.com	80	Website	0.115 s	about a minute ago	Yes	No	No	
on	PHP Server Monitor	http://www.phpservermonitor.org	80	Website	0.4881 s	about a minute ago	Yes	Yes	Yes	
on	SourceForge	http://sourceforge.net/	0	Website	0.3945 s	about a minute ago	Yes	Yes	Yes	

Powered by [PHP Server Monitor v3.0.0](#).

[Back to top](#)

The screenshot shows the 'Status' tab selected in the top navigation bar. The page displays five status cards:

- Example FTP** (Red card): Last online: 6 hours ago, Last check: 10 seconds ago.
- Gmail SMTP** (Green card): Last online: 10 seconds ago, Latency: 0.0128851s.
- Google** (Green card): Last online: 9 seconds ago, Latency: 0.1150210s.
- PHP Server Monitor** (Green card): Last online: 10 seconds ago, Latency: 0.4881301s.
- SourceForge** (Green card): Last online: 9 seconds ago, Latency: 0.3944931s.

# Nagios

- Créé en 2002 (GPLv2)
- S'articule autour :
  - D'un moteur de collecte et d'ordonnancement
  - D'une interface Web
  - De **fichiers de configuration** à plat
  - De **plugins**, pouvant être développés **dans n'importe quel langage** (Bash, Ruby, Python...) et devant juste respecter la norme suivante :
    - **0 : OK** (tout va bien)
    - **1 : WARNING** (le seuil d'alerte est dépassé)
    - **2 : CRITICAL** (le service a un problème)
    - **3 : UNKNOWN** (impossible de connaître l'état du service)
- Souvent utilisé avec des extensions comme **NagVis** (créé en 2004) pour avoir un rendu plus visuel



# Nagios et son environnement

- **NDOUtils : Nagios Data Output Utilities**
  - Permet d'exporter les données de Nagios dans une base MySQL
- **RRDtool : Round-Robin Database Tool**
  - Issu du projet MRTG (Multi Router Traffic Grapher)
  - Permet la gestion de données sous forme de **séries temporelles** (représentant l'évolution d'une donnée dans le temps)
  - Permet la représentation de ces données sous forme graphique
  - Utilisé dans de **très nombreux** outils de supervision
- **NRPE : Nagios Remote Plugin Executor**
  - Permet l'exécution de scripts directement sur les clients
  - Permet l'exécution de scripts vers des clients injoignables (utilisé alors en tant que proxy)

# Nagios par l'image

**Nagios®**

General

Home Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
- Unhandled
- Host Problems
- Unhandled
- Network Outages

Show Host:

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Reporting

Trends

Availability

Alert Histogram

Alert History

Alert Summary

Notifications

Event Log

Configuration

View Config

**Current Network Status**  
Last Updated: Tue Aug 11 10:04:02 PDT 2009  
Updated every 90 seconds  
Nagios® 3.0b5 - www.nagios.org  
Logged in as *nagiosadmin*

[View History For All hosts](#)  
[View Notifications For All Hosts](#)  
[View Host Status Detail For All Hosts](#)

Host Status Totals			
Up	Down	Unreachable	Pending
3	1	0	0
<a href="#">All Problems</a>		<a href="#">All Types</a>	
1		4	

Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
7	2	4	8	0
<a href="#">All Problems</a>		<a href="#">All Types</a>		
14		21		

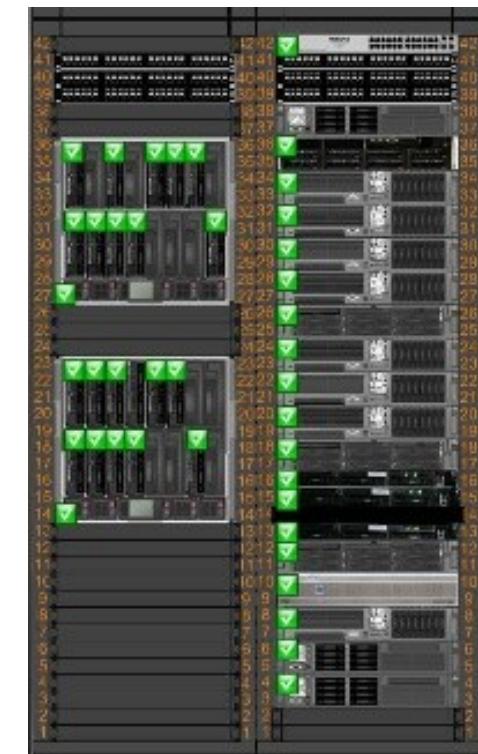
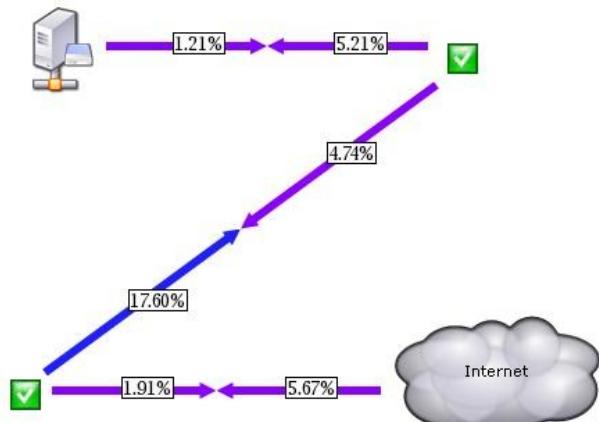
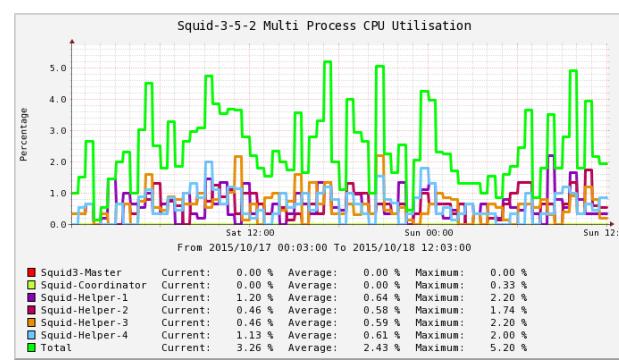
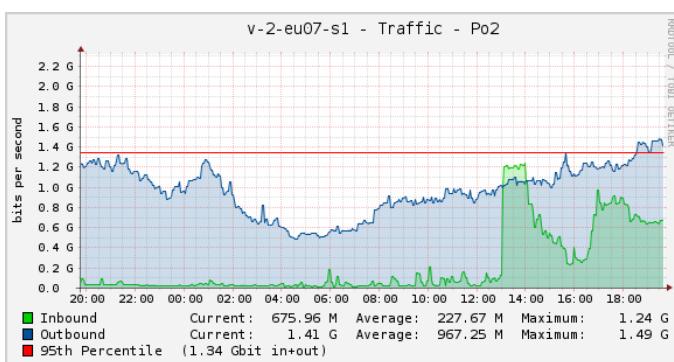
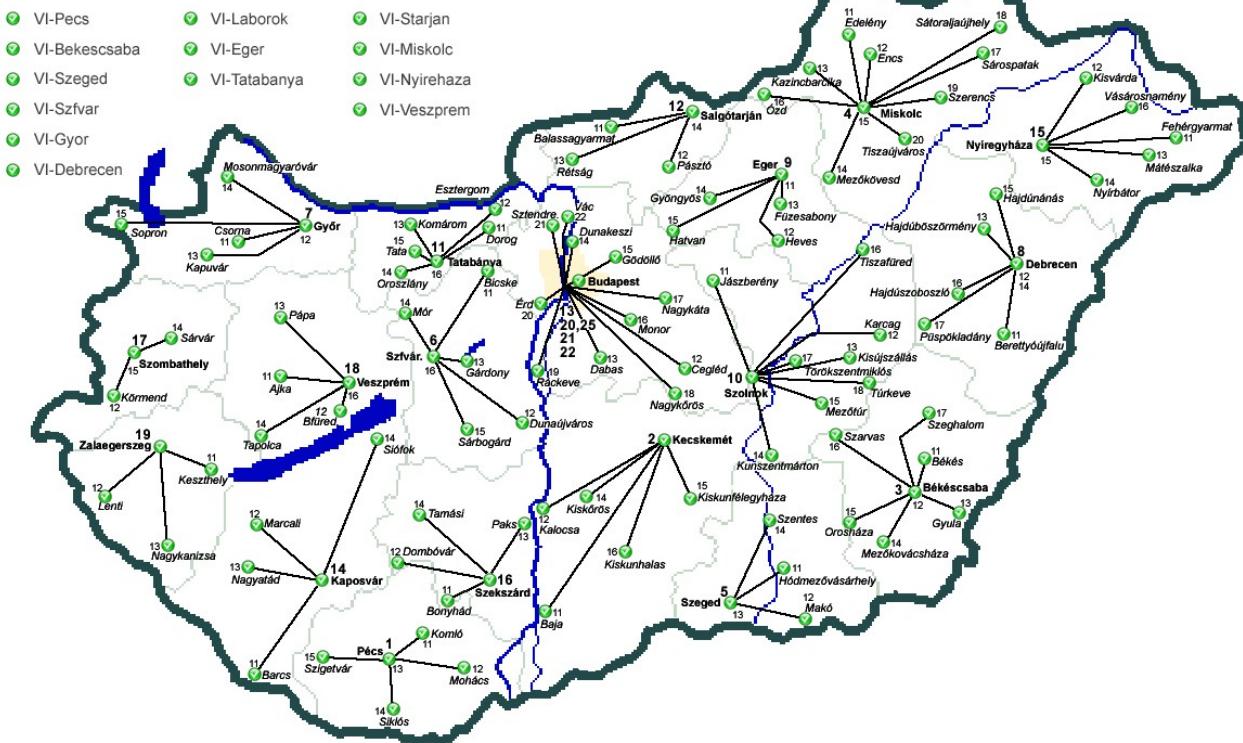
## Service Status Details For All Hosts

Entries sorted by **service status** (descending)

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
cisco2690	<a href="#">PING</a>	CRITICAL	08-11-2009 10:00:32	657d 16h 59m 56s	1/3	CRITICAL - Host Unreachable (10.2.0.2)
kparikh-t60	<a href="#">C:\ Drive Space</a>	CRITICAL	08-11-2009 09:59:10	586d 21h 15m 4s	3/3	Connection refused
	<a href="#">CPU Load</a>	CRITICAL	08-11-2009 09:57:54	586d 17h 4m 7s	3/3	Connection refused
	<a href="#">Explorer</a>	CRITICAL	08-11-2009 09:59:17	586d 17h 3m 6s	3/3	Connection refused
	<a href="#">Memory Usage</a>	CRITICAL	08-11-2009 09:59:10	586d 17h 2m 7s	3/3	Connection refused
	<a href="#">NSClient++ Version</a>	CRITICAL	08-11-2009 09:59:16	586d 17h 3m 7s	3/3	Connection refused
	<a href="#">Uptime</a>	CRITICAL	08-11-2009 09:59:11	586d 17h 2m 7s	3/3	Connection refused
	<a href="#">W3SVC</a>	CRITICAL	08-11-2009 09:59:12	586d 17h 7m 4s	3/3	Connection refused
cisco2690	<a href="#">Port 1 Link Status</a>	UNKNOWN	08-11-2009 10:00:50	657d 16h 58m 41s	1/3	SNMP problem - No data received from host
	<a href="#">Uptime</a>	UNKNOWN	08-11-2009 10:02:54	657d 16h 57m 26s	1/3	SNMP problem - No data received from host
netgearAtColo	<a href="#">Port 161 Link Status</a>	UNKNOWN	08-11-2009 10:01:53	241d 14h 23m 10s	3/3	SNMP problem - No data received from host
	<a href="#">Uptime</a>	UNKNOWN	08-11-2009 09:53:54	241d 14h 25m 36s	3/3	SNMP problem - No data received from host
localhost	<a href="#">Root Partition</a>	WARNING	08-11-2009 09:58:51	25d 16h 13m 23s	4/4	DISK WARNING - free space: / 1750 MB (18% inode=74%)
	<a href="#">Total Processes</a>	WARNING	08-11-2009 10:00:37	13d 3h 3m 26s	4/4	PROCS WARNING: 345 processes with STATE = RSZDT
	<a href="#">Current Load</a>	OK	08-11-2009 10:00:58	26d 5h 53m 10s	1/4	OK - load average: 0.13, 0.11, 0.09
	<a href="#">Current Users</a>	OK	08-11-2009 10:03:02	675d 18h 16m 18s	1/4	USERS OK - 1 users currently logged in
	<a href="#">HTTP</a>	OK	08-11-2009 10:03:20	17d 5h 45m 42s	1/4	HTTP OK HTTP/1.1 200 OK - 681 bytes in 0.001 seconds
	<a href="#">PING</a>	OK	08-11-2009 10:01:00	675d 18h 15m 18s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	<a href="#">SSH</a>	OK	08-11-2009 10:00:31	657d 20h 27m 26s	1/4	SSH OK - OpenSSH_3.4p1 (protocol 1.99)
	<a href="#">Swap Usage</a>	OK	08-11-2009 10:01:00	657d 20h 26m 49s	1/4	SWAP OK - 72% free (2937 MB out of 4094 MB)
netgearAtColo	<a href="#">PING</a>	OK	08-11-2009 10:01:00	242d 3h 51m 8s	1/3	PING OK - Packet loss = 0%, RTA = 0.63 ms

# NagVis et RRDtool par l'image

Bérelt vonalak az országban



# Centreon

- Au début, une **surcouche Web à Nagios** :
  - Meilleure lisibilité des alertes
  - Gestion des configurations plus accessible (directement via la GUI Web)
  - Graphiques de performances
- En 2012, introduction du **centreon-engine** pour s'émanciper complètement de Nagios
- Aujourd'hui, solution complète proposant :
  - Une solution de supervision distribuée : **Centreon Engine** (moteur de collecte), **Centreon Broker** (gestionnaire d'événements) et **Centreon Web**
  - Des **packs de plugins** payants et gratuits
  - Des outils d'analyses et de reporting (dont des suites payantes)

# Centreon par l'image

The screenshot shows the Centreon monitoring interface. The top navigation bar includes links for Home, Monitoring, Status Details, Services, Pollers, Databases, and a search bar. On the right, it displays system statistics: 0 hosts, 3 services (1 red, 0 yellow, 0 green), and 38 pollers. The date and time are shown as October 24, 2018, 11:50 AM.

The main content area is titled "Monitoring > Status Details > Services". It features several filter dropdowns: Service Status (All), Status (OK), Poller (All), Hostgroup (All), Servicegroup (All), and Output (All). Below these filters is a "More actions..." button and a set of icons for refresh, search, and other operations.

The central part of the screen is a table titled "Services Grid" showing the status of various services. The columns include Hosts, Services, Status, Duration, Last Check, Tries, and Status information. A legend indicates that green means OK, yellow means warning, and red means critical. The table lists numerous services, such as Broker-Retention, Connection-Time, Cpu, Database-Size, Load, Memory, Myisam-Keycache, Open-Files, Partitioning, Ping, proc-broker-rrd, proc-broker-sql, proc-centcore, proc-centengine, proc-cron, proc-htpd, proc-ntpd, proc-sshd, Queries, Slowqueries, and Swap. The "proc-ntpd" service is highlighted in red, indicating a CRITICAL status.

On the left side, there is a sidebar with links for Home, Monitoring, Status Details, Services, Hosts, Services Grid, Services by Hostgroup, Services by Servicegroup, Hostgroups Summary, Performances, Business Activity, Downtimes, Event Logs, Reporting (which is currently selected), Configuration, and Administration.

# Icinga

- Fork de Nagios créé en 2009 (GPLv2)
- Né de la volonté de **moderniser** Nagios :
  - **Cycle de développement plus rapide**
  - Interface Web moderne
  - Support des bases de données Oracle et PostgreSQL
  - API REST
- **Maintien de la compatibilité** des configurations et des plugins avec Nagios (attention : Icinga2 ne garantie plus cette compatibilité !)

# Icinga par l'image

Icinga Web Interface screenshot showing current incidents and service/host problems.

**Current Incidents**

**Service Problems**

Severity	Timestamp	Description	Status
CRITICAL	09:49	Webserver Testing (DOWN): SSH CRITICAL - Socket timeout after 10 seconds	✓
CRITICAL	09:49	Icinga Exchange: HTTP HTTP CRITICAL: HTTP/1.1 200 OK - string 'welcome to Icinga Exchange' not found on 'https://accounts icinga.com:443/' - 5830 bytes in 0.168 second response time	✓
CRITICAL	09:49	localhost: SSH connect to address 127.0.0.2 and port 22: Connection refused	✓
WARNING	09:49	localhost: Disk DISK WARNING - free space: / 18420 MB (83% inode=91%): /etc/re- solv.conf 18420 MB (83% inode=91%): /etc/hostname 18420 MB (83% inode=91%): /etc/hosts 18420 MB (83% inode=91%):	● ● ● ●

**Host Problems**

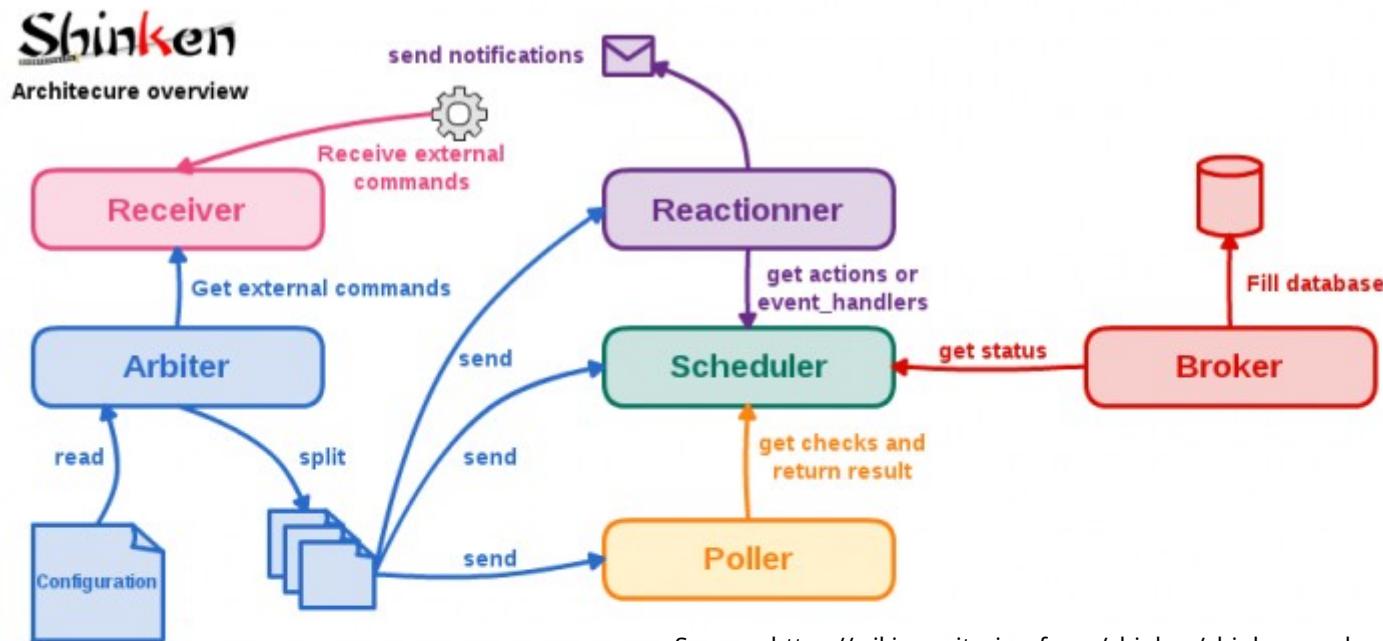
Status	Timestamp	Description
DOWN	09:49	Webserver Development PING CRITICAL - Packet loss = 100%
DOWN	09:49	Webserver Testing PING CRITICAL - Packet loss = 100%

**Cube**

Environment	Location	Count
development (2) ▾	berlin ▾	1
	new-york ▾	1
production (5) ▾	berlin ▾	1
	london ▾	1
	new-york ▾	3
testing (2) ▾	berlin ▾	1

# Shinken

- Projet Libre (AGPL) issu d'un POC de refonte de Nagios, publié en 2009
- Développé en **Python**
- Découpe les rôles de Nagios



Source : <https://wiki.monitoring-fr.org/shinken/shinken-work>

# Shinken par l'image

The screenshot shows the Shinken 2.4 Web User Interface. The left sidebar contains navigation links: Dashboard, Problems, Groups and tags, Tactical views, System, Configuration, Add a comment, Recheck, Submit check result, and Schedule a downtime. The main content area shows the host 'Fred's testing server' with a status of 'host is UP'. It displays 13 services: 12 up (92.31%), 1 down (7.69%), and 0 others. The 'Information' tab is selected. The 'Availability' section shows the host has been up for 1m 24s. The 'Last check' section shows the last check was 9s ago, output was PING OK - Packet loss = 0%, RTA = 0.00 ms, and performance data was rta=0.00000ms;1000.000000;3000.000000;0.000000... The 'Flapping detection' section has 'ON' enabled with options o, d, u, low threshold 25, and high threshold 50. The 'Notifications' section has 'ON' enabled with notification period Always, options Down, Flapping, Recovery, and notification options None, Downtimes, Unreachable. The footer includes the Shinken logo, version Shinken 2.4 — Web User Interface 2.0.1, and copyright ©2011-2015.

# Zabbix

- Projet créé en 1998 et devenu Libre (GPLv2) en 2001
- Peut de faire de l'auto-discovery
- Pensé pour la performance, théoriquement capable de superviser des centaines de milliers d'assets
- S'articule autour des composants :
  - **Zabbix Server** : collecte les données et gère les alertes
  - **Zabbix Agent** : collecte locale des données d'un système
  - **Zabbix Frontend** : l'interface Web centralisée
  - **Zabbix Proxy** : permet d'atteindre des systèmes éloignés

# Zabbix par l'image

**ZABBIX** Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

## Dashboard

Favourite maps

Local network

Maps

Favourite graphs

New host: CPU load

Graphs

Favourite screens

Zabbix server

Screens Slide shows

### Last 20 issues

HOST	ISSUE	LAST CHANGE	AGE	INFO	ACK	ACTIONS
Zabbix server 1	Version of zabbix-agent(d) was changed on Zabbix server 1	2016-01-11 22:36:06	1m 39s	No	1	
Zabbix server 1	Lack of free swap space on Zabbix server 1	2015-08-11 23:29:28	5m 3d	Yes	4	

2 of 2 issues are shown Updated: 22:37:45

### System status

HOST GROUP	DISASTER	HIGH	AVERAGE	WARNING	INFORMATION	NOT CLASSIFIED
Discovered hosts	0	0	0	1	1	0
Network devices	0	0	0	0	0	0
SNMP hosts	0	0	0	0	0	0
Zabbix servers	0	0	0	1	1	0

Updated: 22:37:45

### Host status

HOST GROUP	WITHOUT PROBLEMS	WITH PROBLEMS	TOTAL
Discovered hosts	7	1	8
Network devices	1	0	1
SNMP hosts	2	0	2

### Status of Zabbix

PARAMETER	VALUE	DETAILS
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled /templates)	54	10 / 1 / 43
Number of items (enabled/disabled/not supported)	356	350 / 0 / 6
Number of triggers (enabled/disabled [problem/ok])	95	94 / 1 [2 / 92]
Number of users (online)	3	2
Required server performance, new values per second	4.79	

Updated: 22:37:45

### Web monitoring

HOST GROUP	OK	FAILED	UNKNOWN
Discovered hosts	1	0	0
Zabbix servers	1	0	0

Updated: 22:37:44

# Dell OpenManage Essentials

- Console d'administration et de supervision d'un parc matériel (Dell et autres vendeurs)
- S'interface avec les équipements via **IPMI, SNMP, WS-MAN** (Web-Services Management)...
- Permet de :
  - Déployer des **templates de configuration** sur les serveurs (BIOS, iDRAC...)
  - Gérer les **mises à jours de firmwares**
  - Surveiller **l'état des composants** et **lever des alertes** (tickets automatiques au support Dell)
- Peut faire de l'auto-discovery



# Dell OME par l'image

**DELL OPENMANAGE ESSENTIALS**

Dell TechCenter | Support | Help | About | Administrator  
2 1 1 1

Home Manage Reports Preferences Logs Tutorials Extensions  
Dashboard Schedule View Map View

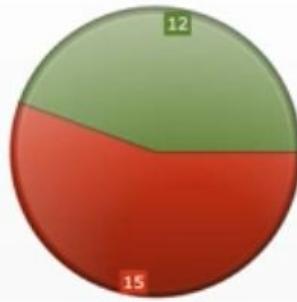
cmc-27B0012

Home Portal Filter by: All Devices

Devices by Status



Alerts by Severity



Alerts

Filter by: All Alerts Viewing 27 Filtered Alerts  Continuous Updates

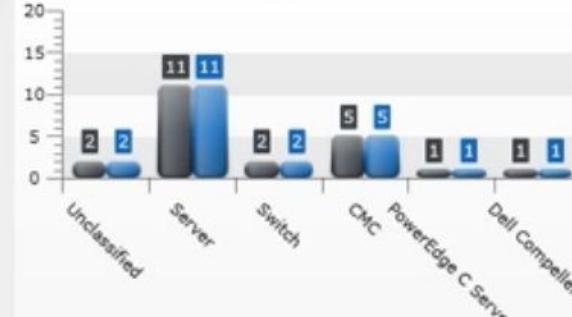
Severity	Acknowledged	Time	Device	Details	Category
Normal	Yes	6/29/2013 11:52:24 PM	cmc-servicetag	System is up: cmc-servicetag	System
Critical	No	6/29/2013 10:52:07 PM	cmc-servicetag	System is down: cmc-servicetag	System
Normal	Yes	6/29/2013 8:51:23 AM	cmc-servicetag	System is up: cmc-servicetag	System
Critical	No	6/29/2013 8:51:06 AM	10.35.155.240	System is down: 10.35.155.240	System
Critical	No	6/29/2013 4:51:05 AM	cmc-PLSC034	System is down: cmc-PLSC034	System
Critical	No	6/29/2013 4:51:05 AM	cmc-BDC1234	System is down: cmc-BDC1234	System

Discovered vs. Inventory Devices

Filter by: All

Devices in Range: 22

Discovered: 20  
Inventory: 11



Task Status

Task Name	Task State	% Completed	Start Time	End Time
Scheduled Status Poll	Complete	100%	7/1/2013 11:52:01 PM	7/1/2013 11:52:23 PM
Discovery of 10.94.173.128 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:32:20 AM
Discovery of 10.94.169.67 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:32:05 AM
Discovery of 10.94.168.97 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:31:44 AM
Scheduled Inventory	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:31:37 AM
Discovery of 10.36.0.138 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:31:24 AM
Discovery of 10.36.0.253 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:31:00 AM
Discovery of 10.35.155.199 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:30:55 AM
Discovery of 10.94.173.164 (Scheduled)	Complete	100%	7/1/2013 5:30:01 AM	7/1/2013 5:30:46 AM

# La supervision-as-a-service

- Aujourd'hui, plusieurs solutions « Cloud » existent : 
  - Des offres issues des éditeurs historiques (comme Centreon)
  - Des nouveaux arrivants, par exemple Datadog (fondée en 2010 par 2 français)
- Avantages :
  - Un déploiement **simplifié** et une **rationalisation** des solutions de supervision et de métrologie
  - Un tarif adapté à la quantité de sondes mises en place
  - Une offre de **support** adaptée
- Inconvénients :
  - Un risque de **sécurité** important à prendre en compte
  - Un **risque financier** si l'évolution de

# Datadog par l'image

Application + infrastructure overview ▾

Add Template Variables ?

1h The Past Hour

ESC /

## Metrics

Active users

ELB requests per second

us-east-1a us-east-1d us-east-1c us-central-1a

Updated < 1 min ago

CPU %

Disk space available

System load

Memory

Lambda invocations by function

Lambda execution duration by function

Postgres committed transactions

Postgres DB connections

## Traces

Latency SLO

Over 7 days 99.50% Error Budget 50m

Month-to-date 99.51% Error Budget 2h 23m

App performance

Total Requests 74/s Total Errors 1.75%

Latency 791 ms avg

Total time spent by service

Name Hits Avg Latency Total time Errors Error rate

Name	Hits	Avg Latency	Total time	Errors	Error rate
GET /coffeehouse	98.7k	2.14 s	2.4 d	0	0%
GET /orders/muffin	9.39k	1.29 ms	12.2 s	0	0%
GET /orders/milk	9.39k	1.25 ms	11.7 s	0	0%
GET /orders/bacon	9.39k	1.24 ms	11.7 s	0	0%
GET /orders/crepe	9.39k	1.24 ms	11.6 s	0	0%

Service dependencies

```
graph TD; coffee-house --- dotnet-coffe...; coffee-house --- sql-server; coffee-house --- redis; coffee-house --- dotnet-coffe...
```

## Logs

2xx/3xx responses 19.3K rps 325.42 rps 240.05 rps

4xx errors

5xx errors

Service logs

DATE	HOST	SERVICE
Aug 07 13:59:31.000	[coffeehouse-staging-12.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:31	INFO CoffeeHouse:157 - 407832065508908283 5861134944696466449 GET /api/auth/ (10.8.4.7) - 200 OK - Authentication successful	
Aug 07 13:59:30.606	[coffeehouse-production.c.fetch-171516.internal]	coffee-house
17:59:30	INFO Executing ObjectResult, writing value of type System.Collections.Generic.List`1[[DataDog.Coffeehouse.Core.Models.User, DataDog.Coffeehouse.Core, Version=1.0.0, Culture=neutral, PublicKeyToken=null]]	
Aug 07 13:59:30.414	[coffeehouse-production.c.fetch-171516.internal]	coffee-house
17:59:30	INFO Route matched with action = Get , controller = Users . Executing controller action with signature:	
System.Web.Mvc.ActionResult`1 System.Collections.Generic.IEnumerable`1[[DataDog.Coffeehouse.Core...		
Aug 07 13:59:30.412	[coffeehouse-production.c.fetch-171516.internal]	coffee-house
17:59:30	INFO Executing endpoint DataDog.Coffeehouse.Api.Controllers.UsersController.Get	
Aug 07 13:59:30.220	[coffeehouse-production.c.fetch-171516.internal]	coffee-house
17:59:30	INFO Executing ObjectResult, writing value of type System.Collections.Generic.List`1[[DataDog.Coffeehouse.Core.Models.User, DataDog.Coffeehouse.Core, Version=1.0.0, Culture=neutral, PublicKeyToken=null]]	
Aug 07 13:59:30.083	[coffeehouse-staging-11.c.fetch-171516.internal]	coffee-house

Error logs by endpoint

DATE	HOST	SERVICE
6.20k	/api/v1/email	
83.00	/send/notice	
595.00	/bad	
238.00	/ingest	
23.00	/request	
23.00	/rate	
23.00	/auth	
23.00	/metric-base	
23.00	/order	
23.00	/search	

4xx/5xx errors

Error logs

DATE	HOST	SERVICE
Aug 07 13:59:30.000	[coffeehouse-staging-8.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:30	ERROR CoffeeHouse:248 - 29543750619787226 5095176791500978196 - Java.lang.InterruptedException: Thread interrupted for external calls timeout 500	
Aug 07 13:59:29.000	[coffeehouse-staging-10.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:29	ERROR CoffeeHouse:248 - 153509530855943104 408423362523346143 - Java.lang.InterruptedException: Thread interrupted for external calls timeout 500	
Aug 07 13:59:29.000	[coffeehouse-staging-12.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:29	ERROR CoffeeHouse:248 - 887348413354659775 575808366010536435 - Java.lang.InterruptedException: Thread interrupted for external calls timeout 500	
Aug 07 13:59:29.000	[coffeehouse-staging-7.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:29	ERROR CoffeeHouse:248 - 3444519610640237538 7261088733274925398 - Java.lang.InterruptedException: Thread interrupted for external calls timeout 500	
Aug 07 13:59:28.000	[coffeehouse-staging-10.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:28	ERROR CoffeeHouse:248 - 7279434490078407886 506263352378300119 - Java.lang.InterruptedException: Thread interrupted for external calls timeout 500	
Aug 07 13:59:28.000	[coffeehouse-staging-11.c.fetch-171516.internal]	coffee-house
2019-08-07 17:59:28	ERROR CoffeeHouse:248 - 7487178679219360982 3405959682017114916 - Java.lang.InterruptedException: Thread interrupted for external calls timeout 500	
Aug 07 13:59:28.000	[coffeehouse-staging-11.c.fetch-171516.internal]	coffee-house

# Les outils : petite conclusion

- Une **très grande** variété d'outils disponibles
- Quelques exemples de critères de sélection :
  - **Le cahier des charges !**
  - Le **type d'assets** à superviser
  - L'environnement existant
  - La pérennité de l'outil (communauté, stabilité, support...)
- Quelques exemples de **mauvais** critères de sélection : 
  - Les **affinités** (ou non) avec le socle technique
  - Le **coût**
  - Les compétences actuelles des équipes

# La métrologie

---

# La métrologie : pourquoi ?

# Définition

« *La métrologie est la science de la mesure.*



On peut la découper en trois composantes :

- *La définition des unités de mesures*
- *La réalisation des mesures*
- *La traçabilité et l'exploitation des mesures dans le temps* »

Source : Wikipédia

# Pourquoi relever des métriques ?

- Pour faire des **statistiques** :
  - Mesure des **taux de disponibilité** (SLA)
  - Surveiller les **performances** d'un environnement dans le temps
  - **Comparer** des environnements (ex : avant/après mise à jour)
  - **Étalonner** son infrastructure
  - **Anticiper** les besoins d'évolutions
- Pour **identifier des problèmes** :
  - **Incidents récurrents = problème sous-jacent !** 
  - Pertes de performances difficilement perceptibles pour la supervision
  - Tentatives d'intrusion ou d'attaques dissimulées
  - Fuites de données

# La métrologie : comment ?

# Comment relever des métriques ?

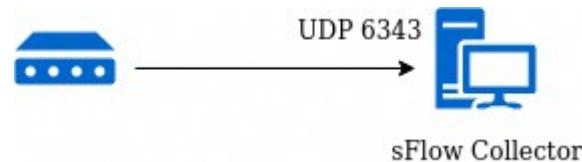
- Processus simplifié :
  - 1 : Définir ce qu'on souhaite mesurer et **pourquoi**
  - 2 : Sélectionner l'outil **adéquat** (faire des POC !), penser « **scalabilité** »
  - 3 : Commencer à injecter les métriques, suivre le dimensionnement de l'infrastructure
  - 4 : Commencer à exploiter les métriques, créer les premiers dashboards
- **Pas nécessairement besoin de « temps réel »**, on pourra opérer des collectes régulières (dépend du contexte)
- 2 approches opposées qui reviennent souvent :
  - Collecter **trop de données** (mais ne pas savoir quoi en faire)
  - Collecter **juste le minimum vital** (mais risquer d'en manquer)

# Les protocoles 2 : le retour 😕



# sFlow

- Protocole industriel standard
- Fonctionne sur la base d'**échantillons**, centré sur la **couche 2 OSI**
- **Pas de notion de flux** au sens « suite de packets »
- 3 notions :
  - **flow** : échantillon de 1/n packets
  - **counter** : compteur d'interface
  - **sFlow datagram** : échantillons et compteurs envoyés en UDP à un **sFlow Collector**



# NetFlow

- Protocole développé par Cisco (supporté par d'autres fabricants, mais souvent sous un autre nom...)
- Fonctionne sur la base de **flux réseaux (couches 4 et 5 OSI)**
- 3 notions :
  - **NetFlow Exporter** : agrège les flux
  - **NetFlow Collector** : collecte et met en forme les flux
  - **Analysis Application** : analyse les flux selon des filtres définis (détection d'attaques par déni de service, de tentatives d'intrusion...)
- Un flux  $\approx$  une suite unidirectionnelle de paquets entrant sur la même interface, possédant les mêmes IP et ports sources et destination

# RMON et SNMP (encore lui !)

- **RMON : Remote Network Monitoring**
- Protocole industriel standard
- S'appuie sur **SNMP** et un modèle client-serveur
- 2 versions :
  - **RMON 1** : centré sur la **couche 2 OSI**
  - **RMON 2** : prend en charge les **couches 4 et 5 OSI**
- Une **sonde** ou agent RMON
  - **collecte** et applique un pré-traitement aux données
  - peut être intégrée dans un équipement réseau, installée sur un serveur ou déployée sous forme d'appliance physique

# Exemples de statistiques RMON

- En RMON 1 :
  - Quantité de paquets reçus sur un segment
  - Quantité de paquets de broadcast
  - Quantité de paquets échangés entre deux addresses MAC
  - Addresses MAC les plus bavardes
- En RMON 2 :
  - Quantité de paquets émis ou reçus par une adresse IP
  - Quantité de paquets reçus pour une adresse IP et un port TCP particuliers
  - ...

# De nouvelles approches applicatives

- Les infrastructures évoluent : **Cloud Public, conteneurs, Continuous Delivery...**
- Les approches traditionnelles côté supervision/métrologie sont **trop « statiques »**, il est nécessaire d'être beaucoup **plus souple et réactif**
- Apparition d'outils spécifiques, qui peu à peu s'imposent comme une nouvelle norme :
  - Un agent très léger et sans dépendances est déployé avec les VM/conteneurs et envoie (ou met à disposition) ses métriques
  - Un serveur central trie ces métriques par type, tag, provenance...

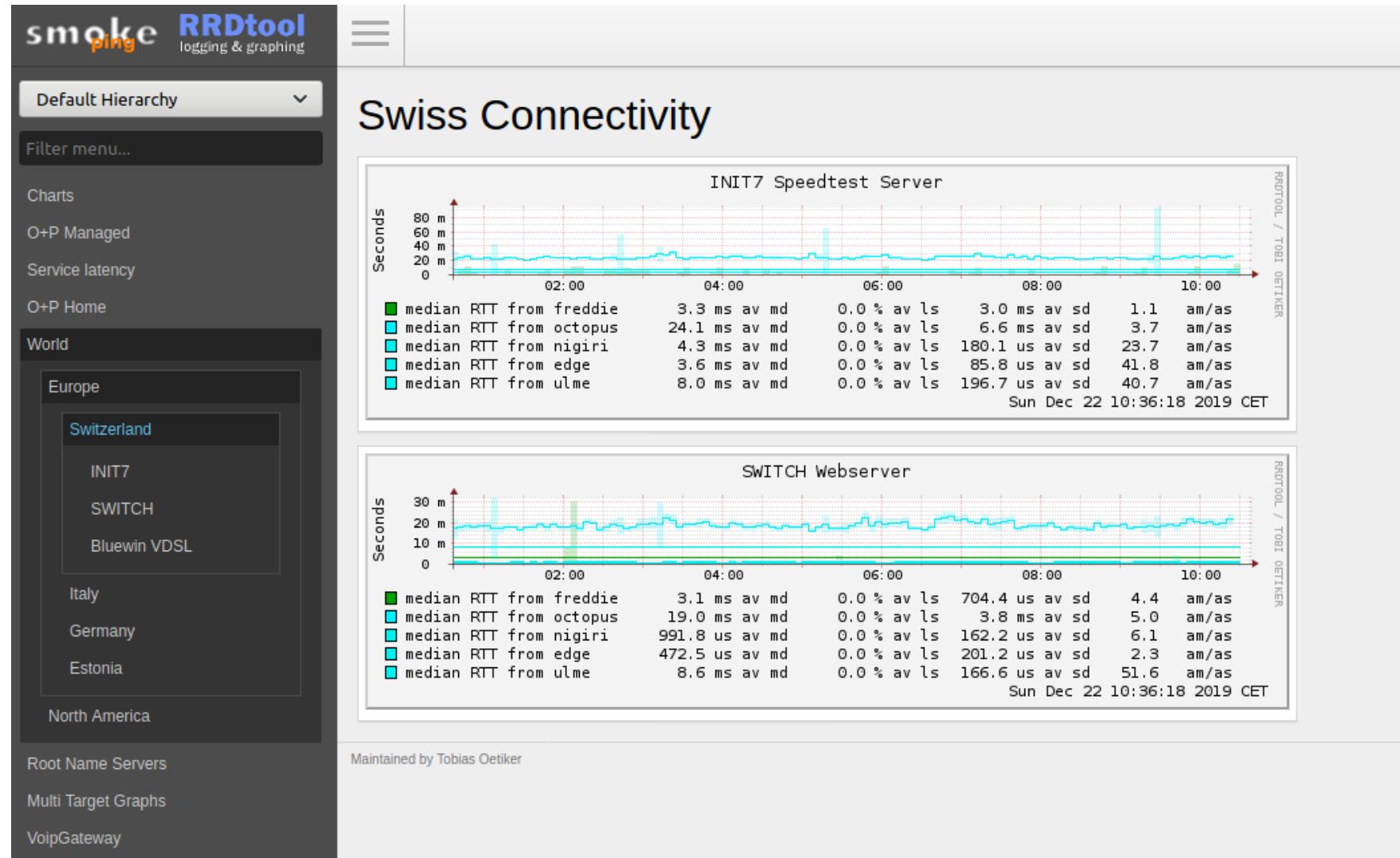


# Métrologie : quelques outils du marché

# SmokePing

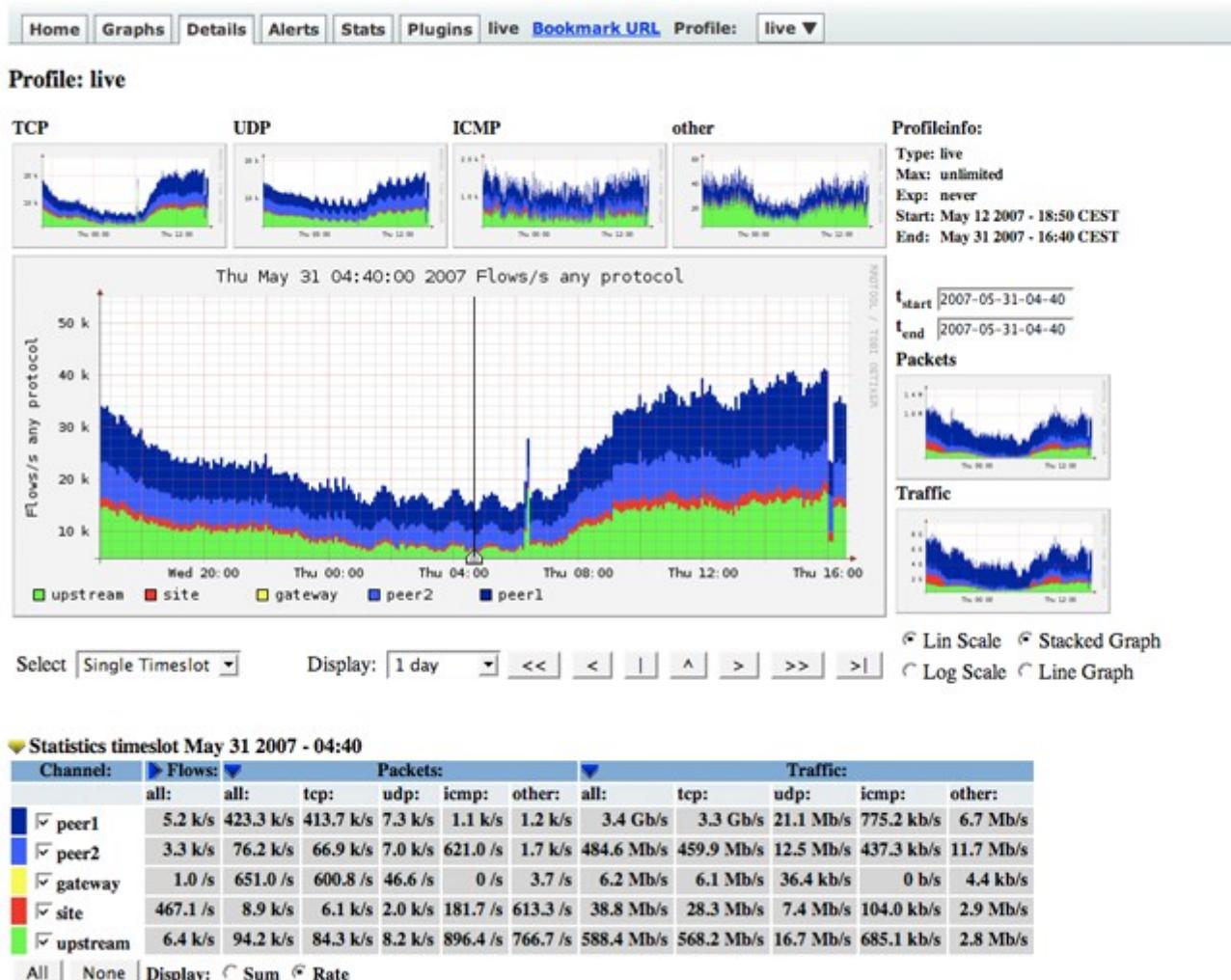
- Outil d'analyse de **latences**
- Dispose de nombreuses sondes :
  - ICMP
  - DNS
  - SSH
  - LDAP
  - Radius...
- Permet de définir des seuils d'alerte

# SmokePing par l'image



- NfDump collecte les datas NetFlow, mais leur exploitation se fait en CLI
- NfSen est une GUI Web permettant de générer des graphs RRD à partir de ces datas
- Travaille par défaut sur des périodes de 5 min (**=/temps réel !**)
- Permet de travailler en modes :
  - **Flows** (quantité de flux par seconde)
  - **Packets** (quantité de packets par seconde)
  - **Bytes** (quantité d'octets par seconde)
- Permet de définir des seuils d'alerte

# NfSen par l'image



# Cacti

- Pensé comme une interface Web pour **RRDtool**
- Capable de découvrir toutes les interfaces à surveiller sur un équipement réseau
- Capable de collecter d'autres type de métriques (espace disque, CPU...)
- Facilement scalable
- S'appuie sur **SNMP**
- Permet d'analyser des comportements sur des **périodes de temps données**

# Cacti par l'image



# Observium / LibreNMS

- LibreNMS est un fork d'Observium, davantage tourné vers la communauté
- Permet de faire de l'**auto-discovery**, identifie les métriques à collecter
- **Compatible avec des dizaines d'équipementiers !**
- Dispose d'un système de plugins pour collecter des données « internes » : tables ARP, routes BGP, VLANs configurés...
- Permet de faire du « **billing** » (par quota ou 95th percentile)
- Peut s'interfacer avec des outils de NetFlow/sFlow, de sauvegarde des équipements (Rancid, Oxidized), de syslog...
- Permet de définir des seuils d'alerte



# LibreNMS par l'image

**Synology** [muffinstation.naschenweng.info](http://muffinstation.naschenweng.info) Unknown

Storage Usage      Memory Usage      Processor Usage

Overview Graphs Health Ports Map Inventory Logs Alerts Alert Stats Performance Notes

**Linux MuffinStation 3.10.35 #5967 SMP Tue Apr 26 16:28:37 CST 2016 x86\_64**

System Name	muffinstation
Resolved IP	192.168.1.97
Operating System	Synology DSM "DSM 5.2-5967"
Object ID	enterprises.8072.3.2.10
Contact	admin@diskstation
Location	Unknown
Lat / Lng	[35.220505,-80.857536]
Uptime	14 days, 20h 1m 2s

**Overall Traffic**

58    49    1    8

lo, sit0, **eth1**, eth0, docker0, dockerc12df77, dockerc312b8f, docker3e68c2f, docker6711f9a, docker9822b09, docker06e6b56, docker85566d0

**Processors**

Intel Atom K510 @ 1.66GHz x4 25%

**Memory Pools**

Physical memory	83%
Virtual memory	51%
Swap space	5%

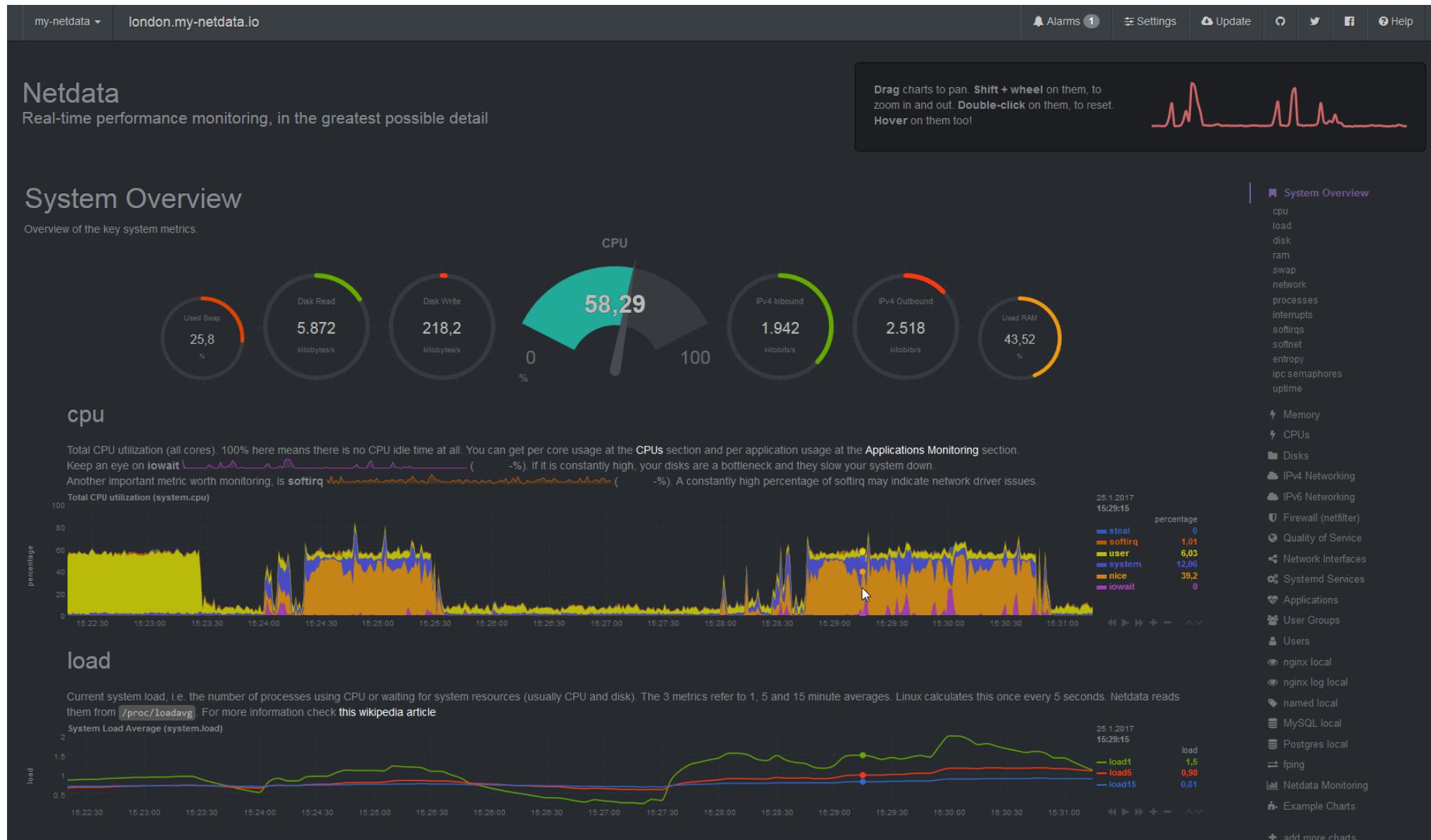
**Storage**

/	45%
/dev/shm	0%
/run	0%
/sys/fs/cgroup	0%
/tmp	0%
/volume1	44%

# Netdata

- Outil de collecte de données installé en local
- **Analyse l'environnement** pour déterminer les métriques à collecter (système, applicatifs...)
- Pensé pour être **léger**, collecte les données de façon **non-intrusive** :
  - Utilise les cycles CPU libres
  - Lit le maximum d'informations dans **/proc**
  - Écrit dans ses logs uniquement à l'arrêt
  - **Aucune dépendance**
- Fournit une interface Web (**à protéger !**)
- **Pas de centralisation** des données collectées, même si l'interface Web permet d'agréger les visualisations de plusieurs machines

# Netdata par l'image

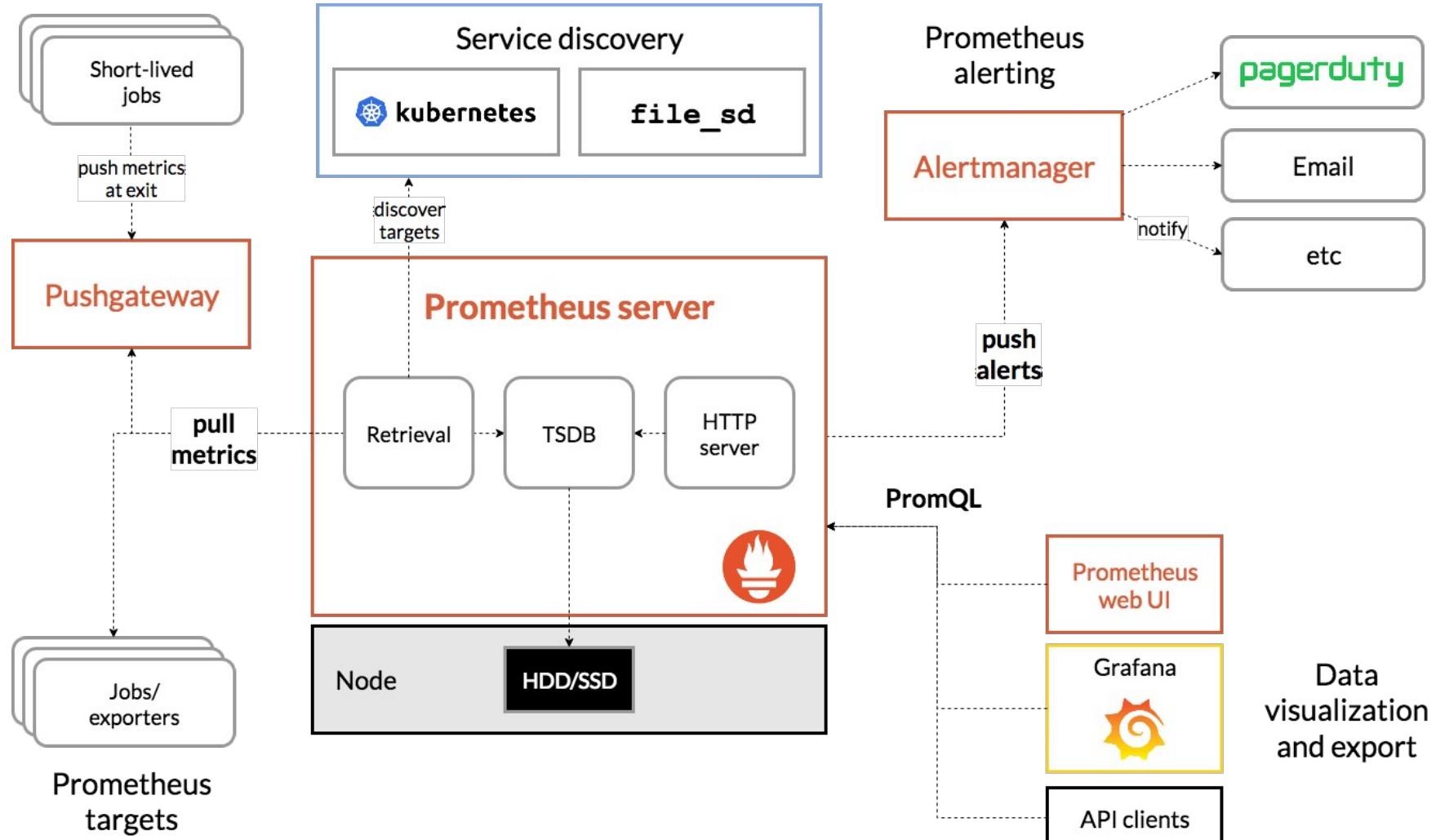


# Prometheus

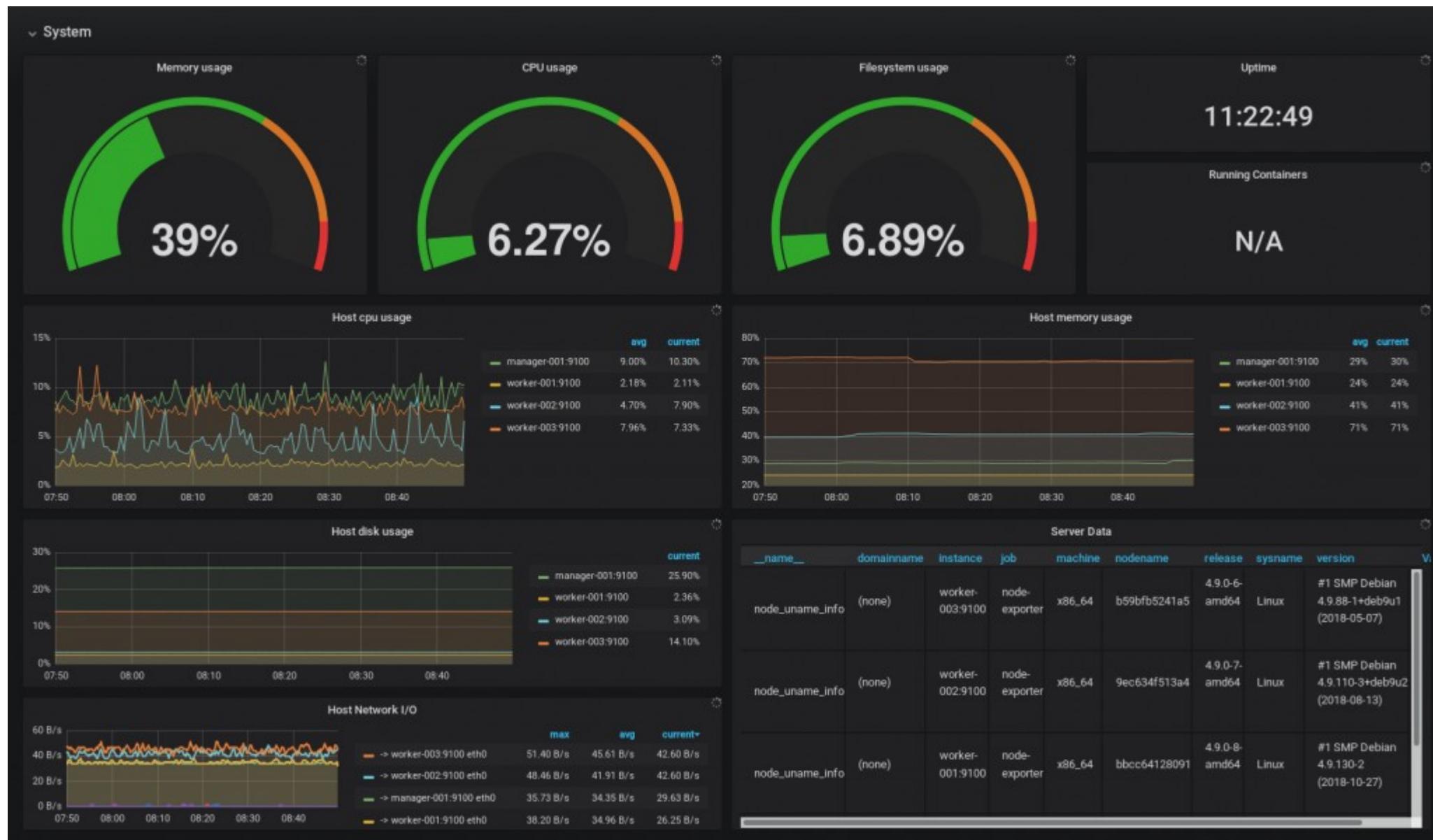
- Projet open-source apparu en 2012
- Développé en Go, **aucune dépendance**
- Modèle de données multidimensionnel : **timeseries et clé/valeur**
- Propose un langage de requête puissant
- Repose sur un modèle **client-serveur** :
  - Les clients mettent les données à disposition via des **exporteurs**, chaque application possédant son propre exporter
  - Le serveur Prometheus vient collecter les données en HTTP régulièrement
- Principalement utilisé en combinaison avec **Grafana** pour visualiser les données



# Fonctionnement de Prometheus



# Prometheus et Grafana par l'image



## **Annexe 1 : la supervision des logs**

---

# Pourquoi ? Comment ?

- **Pourquoi ?**
  - Pour des raisons de **sécurité**
    - **tentatives d'intrusions**
    - authentifications échouées
    - tentatives d'accès à des pages normalement inaccessibles
  - Pour détecter des **comportements anormaux** dans les services
    - pages ou scripts en **erreur**
    - **temps d'accès** trop importants...
- **Comment ?**
  - **Centralisation et archivage** (raisons légales ou pratiques)
  - Puis **analyse** (expressions régulières, indexation...)

# Exemple d'outil 1 : Graylog

- Outil de centralisation et d'analyse des logs créé en 2009
- S'appuie sur **Elasticsearch** (moteur de stockage, de recherche et d'analyse full-text puissant, multi-tenant et distribué)
- Permet de créer des dashboards pour suivre les logs de son infrastructure
- Permet de définir des seuils d'alerte

# Graylog par l'image

graylog Search Streams Dashboards Sources System 1 In 21 / Out 22 msg/s Help Lennart Koopmann

Search in the last 8 hours Saved searches Type your search query here and press enter. ("not found" AND http) OR http\_response\_code:[400 TO 404]

Search result Found 360,614 messages in 14 ms, searched in 1 index. Add count to dashboard Save search criteria More actions

Fields Default All None Filter fields

- child\_pid
- client\_ip
- cluster\_id
- connect\_time\_ms
- connection\_status
- controller
- current\_check\_attempt
- db\_duration Statistics Quick values Generate chart
- drain\_id
- duration
- dyno
- facility
- file

List fields of [current page](#) or [all fields](#).

### Field Statistics

Field	Total	Mean	Minimum	Maximum	Std. deviation	Variance	Sum	Cardinality
connect_time_ms	48,475	0.85	0	84	1.96	3.84	41,064	39
connection_status	2,550	NaN	NaN	NaN	NaN	NaN	NaN	2
db_duration	2,416	19.96	0	201.62	34.5	1,190.45	48,223.99	1,095

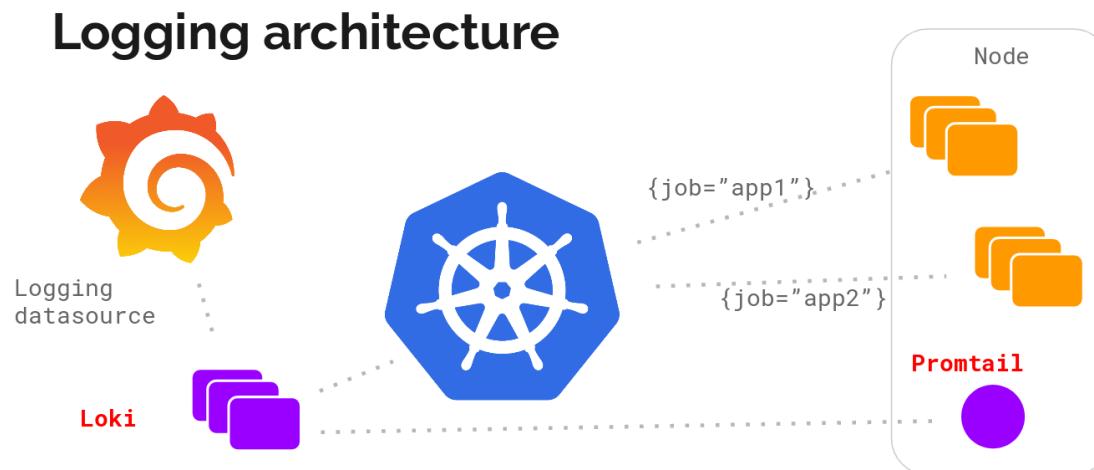
### Quick Values for http\_status

Found 48,472 messages with this field, and 312,135 messages without it.

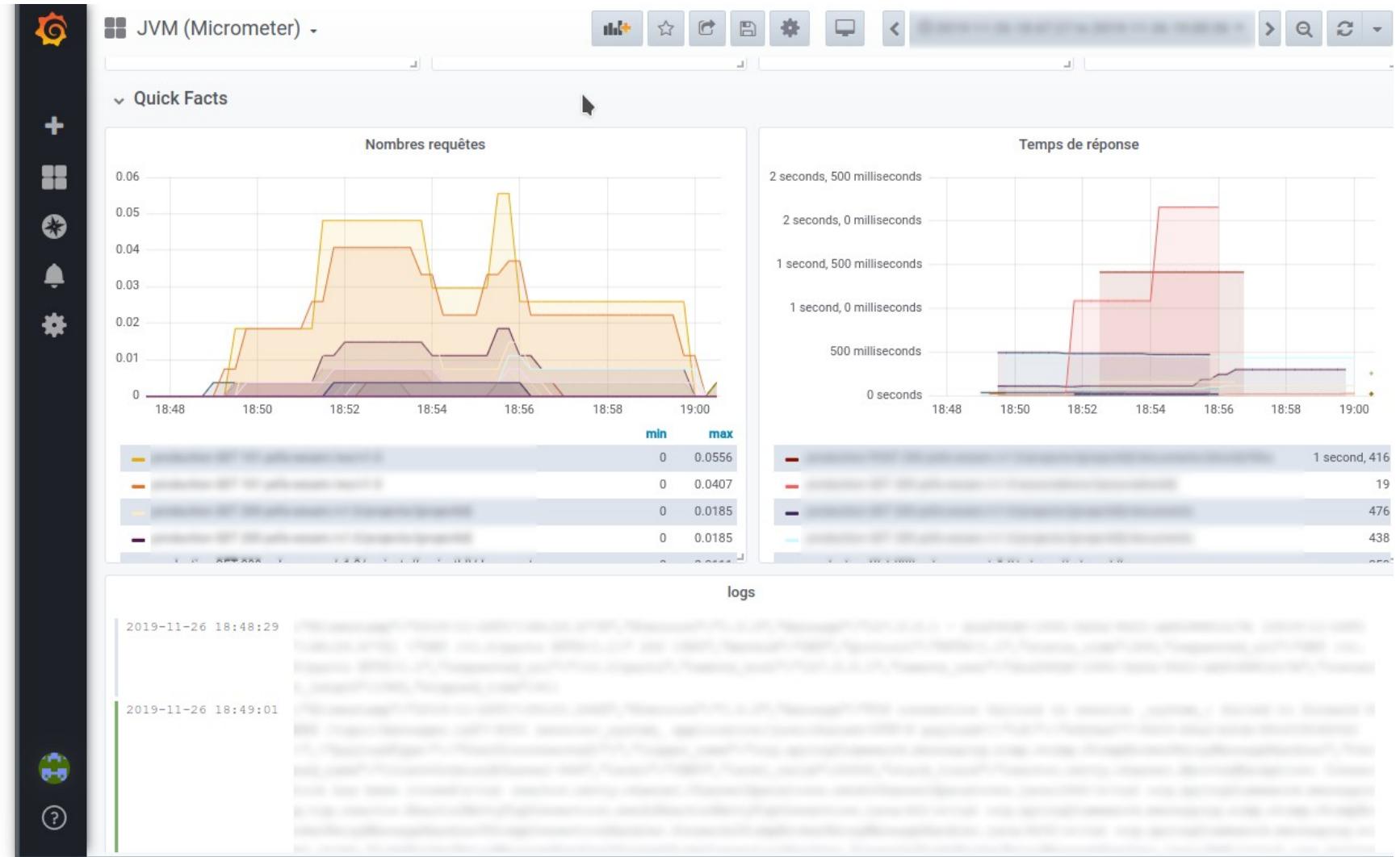
Value	%	Count
404	66.24%	32,107
302	31.02%	15,035
200	2.74%	1,329
500	0.00%	1

# Exemple d'outil 2 : Loki

- Loki = Prometheus, mais pour les logs
- Pour le stockage des données, on reprend l'idée de **timeseries** auxquelles on ajoute des **labels** (pas d'indexation et de structuration des logs, juste des metadata)
- On s'appuie une fois encore sur **Grafana** pour réaliser des dashboards



# Loki et Grafana par l'image



## **Annexe 2 : aux frontières de la sécurité**

---

# Les firewalls

- Un firewall n'a pas qu'un rôle de filtrage : il doit aussi être surveillé
- Plusieurs informations peuvent avoir de l'importance :
  - Les **règles qui ont bloqué des flux** : un « match » n'est pas significatif, mais une série importante dans un cours laps de temps peut indiquer une anomalie
  - Le nombre de « **stateful connections** » actuellement ouvertes : un firewall a des capacités limitées, si on s'approche trop du seuil on prend le risque d'avoir des connexions interrompues ou coupées, ou des dégradations de performances
  - Dans le cas de règles de **QOS**, de « **queuing** »/« **shaping** », on peut vouloir alerter le client qu'il atteint les limites prévues contractuellement

# Le cas des IDS (et IPS)

- **IDS : Intrusion Detection System**
- **IPS : Intrusion Prevention System**
- Peuvent nécessiter des **ressources importantes** (analyse du trafic en temps réel)
- **A ne pas confondre avec des pare-feux**, même si ces derniers incluent parfois des IDS/IPS
- Permettent d'avoir un aperçu du type de trafic reçu (ou émis !) pour :
  - **Réagir en cas d'anomalie**
  - **Adapter et faire évoluer l'infrastructure** en cas de besoin

# Exemple d'outil 1 : Snort

- IDS et IPS créé en 1998, édité par Sourcefire, aujourd'hui détenu par Cisco
- Diffusé sous licence GPL
- S'appuie sur des règles écrites par la communauté ou l'éditeur
- Peut détecter :
  - Des **scans de ports**
  - Des **dépassements de buffers**
  - Des tentatives d'**injections SQL**
  - Des **requêtes DNS** mal formées ou suspectes
  - Des **requêtes HTTP** mal formées ou suspectes
  - ...

# Snort par l'image

Services / Snort / Alerts ?

Snort Interfaces Global Settings Updates **Alerts** Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

[Clear all interface log files](#)

**Alert Log View Settings**

Interface to Inspect: WAN   Auto-refresh view   Choose interface.. Alert lines to display.

**Alert Log Actions**

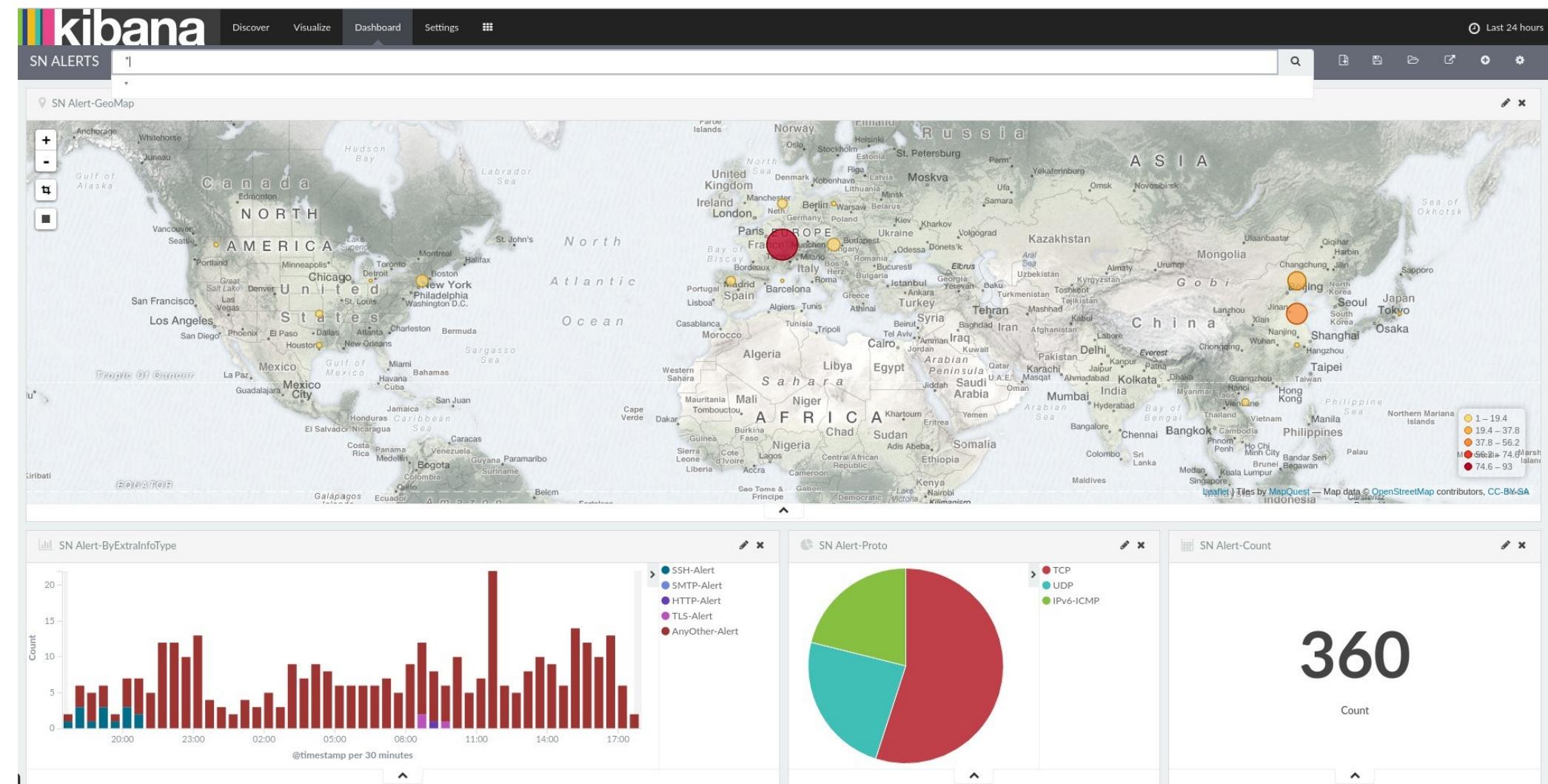
**Alert Log View Filter** +

Last 1000 Alert Log Entries									
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-07-23 20:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066	<input type="button" value="Q"/> <input type="button" value="⊕"/>	16464	<input type="button" value="⊕"/> <input type="button" value="X"/>	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465	<input type="button" value="Q"/> <input type="button" value="⊕"/>	5060	<input type="button" value="⊕"/> <input type="button" value="X"/>	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428	<input type="button" value="Q"/> <input type="button" value="⊕"/>	5060	<input type="button" value="⊕"/> <input type="button" value="X"/>	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834	<input type="button" value="Q"/> <input type="button" value="⊕"/>	5060	<input type="button" value="⊕"/> <input type="button" value="X"/>	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788	<input type="button" value="Q"/> <input type="button" value="⊕"/>	5060	<input type="button" value="⊕"/> <input type="button" value="X"/>	(spp_sip) Method is unknown
2017-07-20 08:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571	<input type="button" value="Q"/> <input type="button" value="⊕"/>	5060	<input type="button" value="⊕"/> <input type="button" value="X"/>	(spp_sip) Method is unknown

# Exemple d'outil 2 : SELKS

- Distribution tout-en-un comprenant basée sur :
  - **Suricata** (IDS/IPS multi-thread, concurrent et compatible avec Snort, apportant de nouvelles fonctionnalités comme la réputation d'IP)
  - Une stack **ELK** :
    - **Elasticsearch** : stockage, recherche et analyse des logs
    - **Logstash** : collecte et formatage des logs pour les injecter dans Elasticsearch
    - **Kibana** : création de requêtes et de dashboards
  - Une interface Web spécifique
- Édité par Stamus Networks et distribué sous licence GPLv3

# SELKS par l'image



# L'état des mises à jour du parc

- Pourquoi mettre à jour ?
  - Patcher des **failles de sécurité**
  - Patcher des **bugs**
  - Améliorer les performances
- La complexité de la gestion des mises à jour augmente en fonction :
  - Du **nombre** d'équipements/systèmes
  - De la **variété** des équipements/systèmes
  - Des **contraintes de production** (application ou système critique, plages de maintenances...)
  - De la **sévérité** des failles (CVE !)

# Exemple d'outil 1 : à la main ?...

- Peu d'outils disponibles dans le monde Linux :(
- Il existe des plugins pour **Nagios/Centreon/etc** s'appuyant sur **apt/yum/pkg\_add/zypper** pour vérifier la quantité de mises à jour disponibles
- **SUSE Manager** : outil de gestion d'infrastructure, permet le déploiement de machines et de configurations ainsi que le suivi des mises à jour du parc

# Exemple d'outil 2 : WSUS

- **WSUS : Windows Server Update Services**
- Disponible dans **Windows Server**
- Permet la gestion des mises à jour du parc :
  - Récupère les mises à jour depuis Windows Update
  - Peut permettre la mise à jour de **machines isolées**
  - Affiche un **état du parc** (mises à jour en attente, mises à jour critiques en attente...)
  - Permet aux administrateurs de **filtrer** les mises à jour
  - Permet de **déployer** les mises à jour ou de les **planifier**

# WSUS par l'image

Screenshot of the Windows Server Update Services (WSUS) interface showing the 'Updates' view.

The left sidebar shows the navigation tree:

- Update Services
- 2K12R2EVAL
  - Updates
    - All Updates
    - Critical Updates
    - Security Updates
    - WSUS Updates
  - Computers
    - All Computers
    - Unassigned Computers
  - Downstream Servers
  - Synchronizations
  - Reports
  - Options

The main content area displays the 'Updates' summary:

This view shows a summary of the status of your updates by update view.

**Overview**

Category	Status	Count
All Updates	Updates with errors	0
	Updates needed by computers	49
	Updates installed/not applicable	102
	Updates with no status	0
Critical Updates	Updates with errors	0
	Updates needed by computers	14
	Updates installed/not applicable	19
	Updates with no status	0
Security Updates	Updates with errors	0
	Updates needed by computers	35
	Updates installed/not applicable	83
	Updates with no status	0
WSUS Updates	Updates with errors	0
	Updates needed by computers	0
	Updates installed/not applicable	0
	Updates with no status	0

**Actions**

- Updates
  - Search...
  - New Update View...
  - Import Updates...
- View
  - New Window from Here
- Refresh
- Help

# Les failles de sécurité du parc

- Une faille de sécurité peut être due :
  - À une **implémentation logicielle** défectueuse
  - À une **mauvaise configuration**
  - À une négligence ou malveillance humaine
- Bien que souvent côté « Web » (mauvaise configuration Apache2 ou Nginx, version obsolète de PHP qui permet d'exploiter des bugs...), peuvent également se retrouver dans :
  - SSL (ex : Heartbleed)
  - RDP (Remote Desktop Protocol)
  - Des bases de données ouvertes en accès libre...

# Exemple d'outil 1 : Nessus

- Outil créé en 1998, gratuit et Libre à l'époque
- Devenu **propriétaire** en 2005, édité par Tenable
- Permet de **scanner une infrastructure** pour détecter :
  - Des **vulnérabilités** (failles logicielles ou d'implémentation)
  - Des **mauvaises configurations** (SSH, bases de données, Web...)
  - Des **mots de passe par défaut** résiduels (!)
  - Des **URL** permettant d'accéder à des ressources qui ne devraient pas être accessibles/exister (ex : /admin, /test.php...)
- Génère des **rapports** dans différents formats (PDF, HTML) avec des recommandations
- Permet de définir des scans réguliers et des alertes

# Nessus par l'image

SecurityCenter

Dashboard Analysis Scanning Reporting Assets Workflow

Mobile Add Component

Mobile Vulnerabilities

Plugin ID	Name	Severity	Total
65633	Apple iOS 6.1.3 Multiple Vulnerabilities	High	271
64287	Apple iOS 6.1 Multiple Vulnerabilities	High	192
62803	Apple iOS 6.0.1 Multiple Vulnerabilities	High	112
62242	Apple iOS 6.0 Multiple Vulnerabilities	High	70
60027	Apple iOS 5.1.1 Multiple Vulnerabilities	Critical	23
60028	Apple iOS 5.1 Multiple Vulnerabilities	High	20
60025	Apple iOS 5.0.1 Multiple Vulnerabilities	High	12
60026	Apple iOS 5.0 Multiple Vulnerabilities	High	12
62516	Windows Phone7 7.0.7392 Out-of-Date SSL Blacklist	Medium	1
62517	Windows Phone7 7.10.8107 Out-of-Date SSL Certificate Blacklist	Medium	1

Last Updated: 1 hour ago

Mobile Device Types

Device Type	Count
WinPhone	11
iPhone	672
iPad	417
BlackBerry	34
Android	72

Last Updated: 1 minute ago

Vulnerable Users

User	Score	Info	Low	Medium	High	Critical	Total
[REDACTED]	56	2	0	0	12	2	16
[REDACTED]	37	4	0	0	9	1	14
[REDACTED]	37	3	0	0	9	1	13
[REDACTED]	34	3	0	0	8	1	12
[REDACTED]	34	2	0	0	8	1	11
[REDACTED]	31	4	0	0	7	1	12
[REDACTED]	31	1	0	0	7	1	9
[REDACTED]	31	1	0	0	7	1	9
[REDACTED]	31	1	0	0	7	1	9
[REDACTED]	31	3	0	0	7	1	11

Last Updated: 1 hour ago

Mobile Device Types

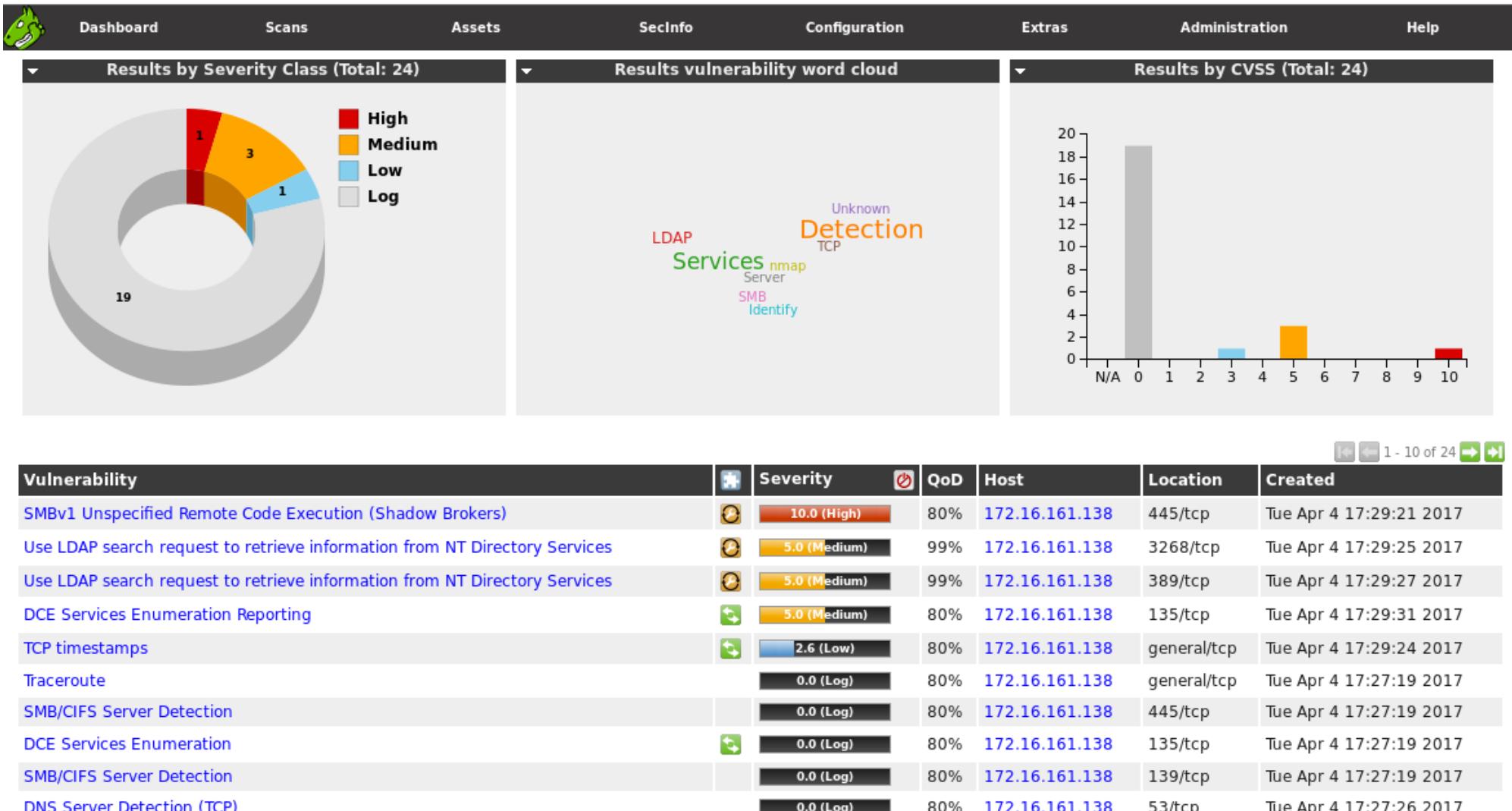
Model	Device Count	Total	High	Critical
WinPhone	11	13	0	0
iPhone	672	1077	389	16
iPad	417	724	300	7
BlackBerry	34	34	0	0
Android	72	72	0	0

Last Updated: 1 hour ago

# Exemple d'outil 2 : OpenVAS

- **OpenVAS : Open Vulnerability Assessment System**
- Fork de Nessus, sous licence GPL
- Les plugins OpenVAS sont écrits en NASL (Nessus Attack Scripting Language)
- Dispose de dizaines de milliers de plugins
- Travaille de la même façon que Nessus :
  - Scan des infrastructures
  - Génération de rapports et de recommandations
  - Peut être automatisé et générer des alertes

# OpenVAS par l'image



# Exemple d'outil 3 : IVRE

- **IVRE : Instrument de veille sur les réseaux extérieurs**
- *Aussi appelé DRUNK (Dynamic Recon of UNKnown networks)*
- Activement soutenu par le **CEA** (Commissariat à l'Energie Atomique)
- S'appuie sur des approches **passives** (NfDump, Argus...) et **actives** (Nmap, ZMap...)
- Permet d'analyser les flux, espaces d'adressage, ports ouverts et systèmes éventuellement mal configurés de son infrastructure
- Accessible en CLI, en Web et via une API Python

# IVRE par l'image

IVRE Web UI    +    localhost/ivre/#80%20skip%3A120

IVRE

7214 RESULTS  
SHOWING 121 TO 130

FILTER  
80 skip:120 Add a criteria

EXPLORE  
product:80

Address space  
IPs & Ports  
Map  
Timeline  
Timeline (24h)

5.11.150.200

Modbus / TR / AS16135 from Linode

UP - syn-ack - 2014-12-13 15:18 - 2014-12-13 15:25

1001 ports **CLOSED** 1001 resets

tcp/21 **OPEN** syn-ack  
ftp: vsftpd, 2.0.8 or later (hostname: DVS)  
banner  
220 Welcome to DVS FTP service.

tcp/23 **OPEN** syn-ack  
tcpwrapped

tcp/53 **OPEN** syn-ack  
domain: dnsmasq, 2.42  
dns-nsid  
bind.version: dnsmasq-2.42

tcp/80 **OPEN** syn-ack  
http: Linksys wireless-G WAP http config (Name H3201 DVS)  
http-auth-finder  
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=5.11.150.200  
url method  
http://5.11.150.200:80/ HTTP: Basic

http-date  
Sat, 13 Dec 2014 17:23:20 GMT; +2h00m43s from local time.

http-headers  
Server: httpd  
Date: Sat, 13 Dec 2014 17:23:26 GMT  
WWW-Authenticate: Basic realm="H3201 DVS"  
Content-Type: text/html  
Connection: close  
(Request type: GET)

tcp/502 **OPEN** syn-ack  
modbus  
modbus-discover  
Positive response for sid = 0x1

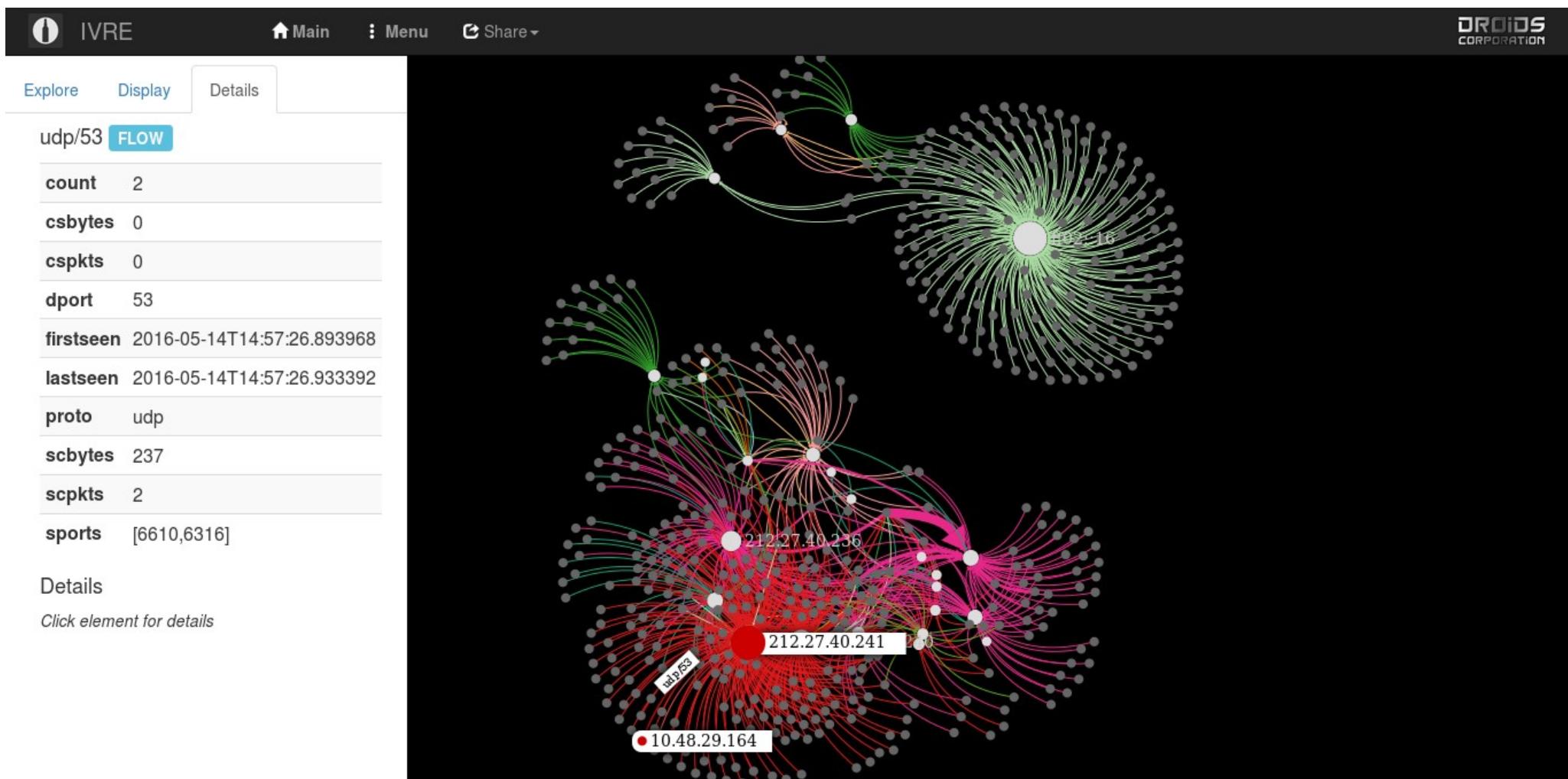
tcp/8888 **OPEN** syn-ack  
Host scripts  
ipidseq  
All zeros

path-mtu

15 most common product:80 values

1387	http / [unknown]
864	tcpwrapped / [unknown]
668	[unknown]
431	httpd
326	Apache httpd
261	Boa HTTPd
239	ioLogik Web Server/1.0
236	lighttpd
235	mini_httpd
208	Microsoft IIS httpd
204	Beck IPC@CHIP embedded httpd
175	eWON
163	Allegro RomPager
103	Schneider-WEB
99	Casi-Rusco camera/Bestelco VoIP phone http config

# IVRE par l'image (une 2<sup>e</sup> pour la route)



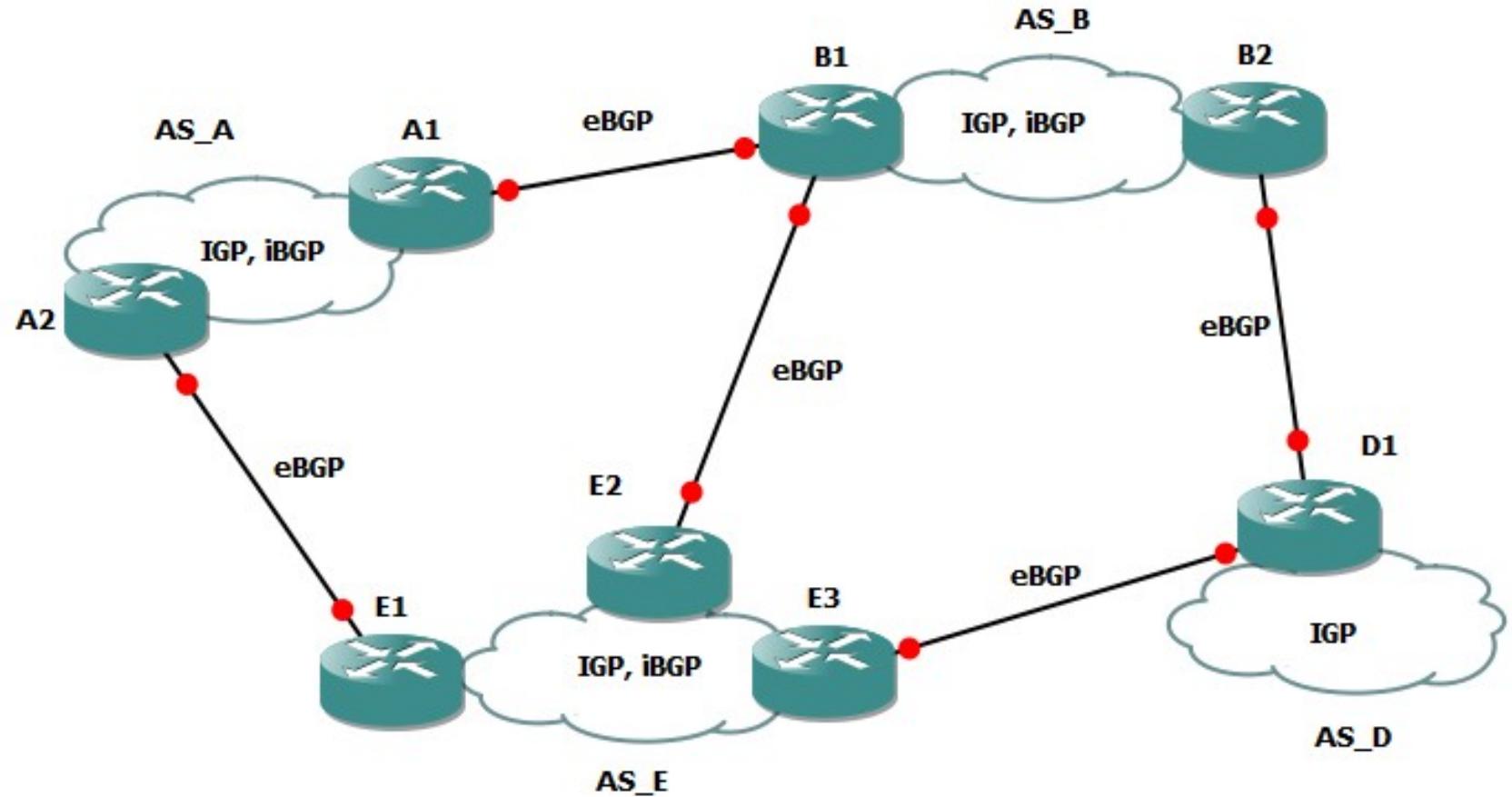
## **Annexe 3 : aux frontières du réseau**

---

# Rappels rapides sur BGP

- **EGP** (Exterior Gateway Protocol), protocole de routage dynamique
- Sert à interconnecter des **AS (Autonomous Systems)**
- Un AS peut être un **opérateur**, une **entreprise**, un **service public**
- Les AS montent des **sessions** entre eux et annoncent des **préfixes** (blocs d'IP publiques), soit en propre, soit au titre de **transitaire**
- **Protocole à vecteur de chemins**, BGP privilégie par défaut l'AS-path le plus court...
- ... mais les règles de routage configurées par chaque AS sont avant tout **politiques** :
  - **Coût du trafic**
  - **Fonctionnalités** (anti-DDOS...)
  - **Affinités** avec telle entreprise, telle plateforme, tel état

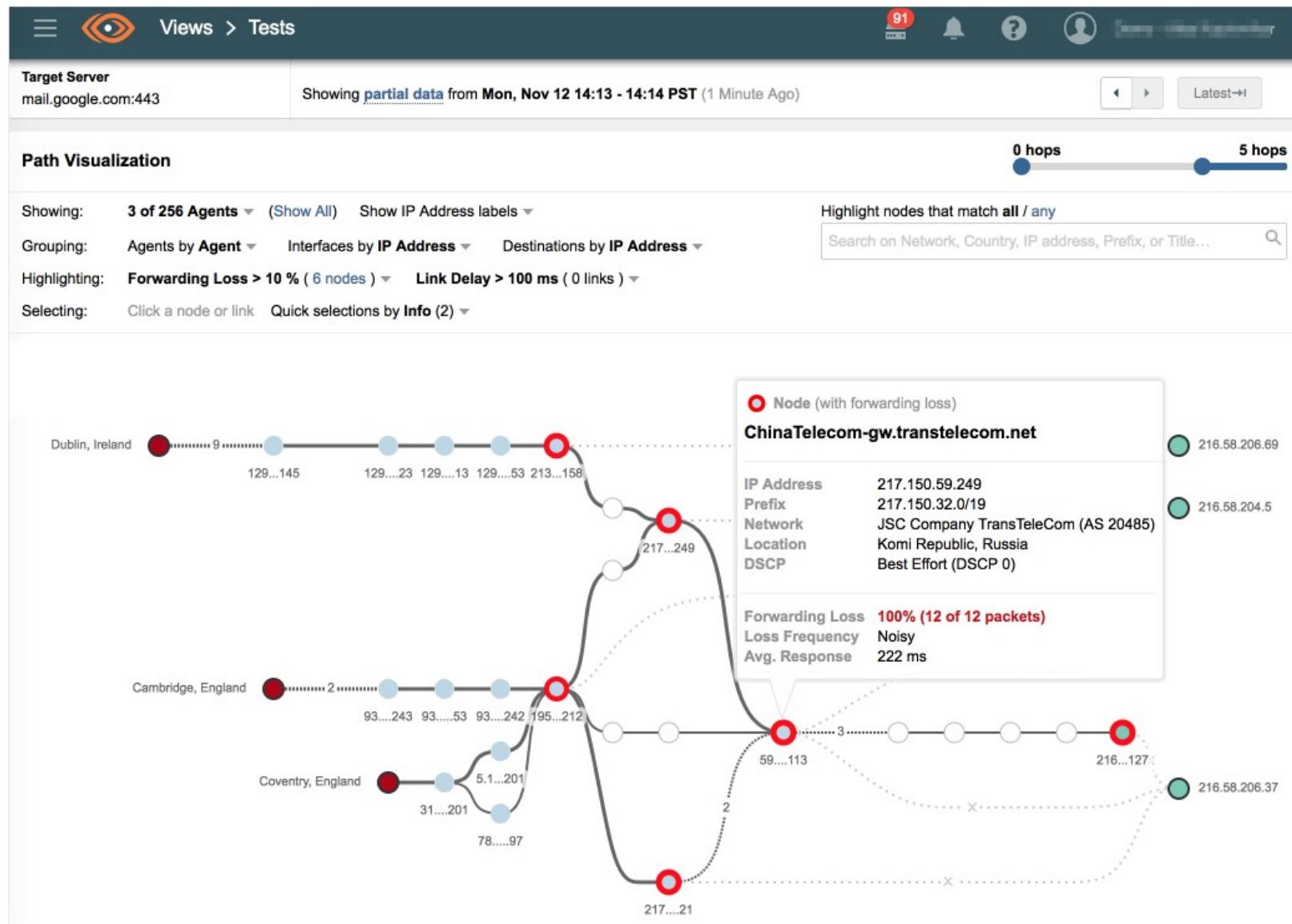
# Rappels rapides sur BGP



# Pourquoi surveiller ses annonces BGP ?

- **Vos annonces BGP = la joignabilité de vos services !**
- Mauvaise configuration dans la chaîne ou **hijack** = trou noir ou instabilités
- Quelques exemples (mais des dizaines par jour !) :
  - En 2008, Pakistan Telecom hijack Youtube au niveau mondial pendant 2h
  - En juin 2015, Telekom Malaysia annonce de nombreuses routes erronées, reprises par Level3... Le trafic mondial est impacté pendant une bonne partie de la journée
  - En avril 2017, l'AS 12389 (PJSC Rostelecom) annonce pendant quelques minutes de nombreux préfixes liés à des banques ou des organismes financiers...
  - En novembre 2018, Google est partiellement injoignable pendant 1h30

# Un exemple de hijack BGP



Source : <https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/>

# Un autre exemple de hijack BGP

<https://www.youtube.com/watch?v=IzLPKuAOe50>

# Exemple d'outil 1 : RIPE Atlas

- Réseau de sondes maintenu par le RIPE
- **Plusieurs milliers de sondes** dans le monde, hébergées gratuitement par des entreprises, des FAI, des particuliers...
- Les sondes fournissent des **métriques** agrégées par le RIPE (joignabilité, latency...) qui permettent de dresser une **cartographie de la qualité et de la performance du réseau IP**
- Chaque entité qui héberge une sonde obtient des crédits
- Chaque entité qui possède des crédits peut effectuer des **requêtes** pour effectuer des **tests** (ping, traceroute, DNS, NTP, HTTP...) depuis les sondes qui l'intéresse
- Disponible via de nombreux outils Web, une API Python, un client CLI...

# RIPE Atlas par l'image

General Information	Probes	Map	LatencyMON	OpenIPMap Prototype	Results	Modification
Probe	ASN (IPv4)	ASN (IPv6)	Time (UTC)	RTT	Hops	
2713	60706	60706	2016-11-18 10:52	33.192	14	
2941	25394		2016-11-18 10:51	50.783	20	
3055	6412		2016-11-18 10:53	150.683	15	
3222	6829		2016-11-18 10:49	36.686	24	
4166	50581		2016-11-18 10:52	39.533	16	
4554	6703		2016-11-18 10:51	82.704	19	
4952	3244		2016-11-18 10:51	35.700	19	
6078	202040	202040	2016-11-18 10:47	9.279	14	
6091	5459	5459	2016-11-18 10:50	9.719	14	
6112	197216	197216	2016-11-18 10:52	33.767	11	
6139	18106	18106	2016-11-18 10:47	216.946	19	
10166	5379		2016-11-18 10:49	60.850	19	
10282	49009	49009	2016-11-18 10:47	32.699	11	
10312	11426		2016-11-18 10:49	116.443	29	



# Exemple d'outil 2 : BGPmon

- Entreprise fournissant un service de supervision des annonces BGP
- Propose les fonctionnalités suivantes :
  - Supervision en temps réel des **annonces de préfixes** avec plusieurs centaines de sondes dans le monde (permet de détecter des anomalies régionales)
    - Qui annonce vos préfixes ?
    - Est-ce que mes politiques de routages sont respectées ?
  - Supervision des **validations ROA** (Route Origin Authorization, permet de valider de manière cryptographique qu'un AS est bien autorisé à annoncer un préfixe)
  - Supervision des préfixes annoncés par votre AS

# BGPmon par l'image



Welcome Andree Toonk | BGPmon API | Help | Configurations &

HOME AUTONOMOUS SYSTEMS

PREFIXES

ALERTS

PEERMON

## My Alerts

### Alerts Details

Tools

On Friday April 22nd 2016 at 17:10 UTC we detected a Origin AS Change event for your prefix (199.16.156.0/23 twitter)  
The detected prefix: 199.16.156.0/24, was announced by AS65021 (-Private Use AS-)

Alert description: Origin AS Change  
Detected Prefix: 199.16.156.0/24  
Detected Origin AS: 65021  
Expected Origin AS: 13414

This alert was detected by 19 unique probes in 12 unique countries

- United States: 4 Peers
- Canada: 3 Peers
- Russian Federation: 2 Peers
- Korea, Republic of: 2 Peers
- Sweden: 1 Peers
- Bulgaria: 1 Peers
- Italy: 1 Peers
- Switzerland: 1 Peers
- Netherlands: 1 Peers
- Czech Republic: 1 Peers
- Germany: 1 Peers
- Slovenia: 1 Peers



UPDATE TIME (UTC)	UPDATE TYPE	PROBE ASN	PROBE LOCATION	PREFIX	AS PATH	CLEARED	DURATION ↓
2016-04-22 17:10:29	Update	AS24482	SE	199.16.156.0/24	24482 43531 200759 65021	2016-04-22 17:30:13	00:19:44
2016-04-22 17:10:16	Update	AS6881	CZ	199.16.156.0/24	6881 15685 6939 200759 65021	2016-04-22 17:20:29	00:10:13
2016-04-22 17:10:17	Update	AS49402	SI	199.16.156.0/24	49402 9119 6939 200759 65021	2016-04-22 17:20:30	00:10:13
2016-04-22 17:10:25	Update	AS395089	CA	199.16.156.0/24	395089 18451 6939 200759 65021	2016-04-22 17:20:25	00:10:00
2016-04-22 17:10:02	Update	AS63297	CA	199.16.156.0/24	63297 6939 200759 65021	2016-04-22 17:19:58	00:09:56
2016-04-22 17:10:15	Update	AS14866	CA	199.16.156.0/24	14866 6939 200759 65021	2016-04-22 17:19:58	00:09:43

# Pilotage, gouvernance et hypervision

---

# La gestion des alertes

# SLA / GTI / GTR...

- **SLA : Service-Level Agreement**
  - **Engagement contractuel sur un niveau de service et de disponibilité**
  - Décrit les attendus du client, les temps de réponse aux incidents, le suivi des processus, les pénalités en cas de non-respect...
  - Exprimé en pourcentages (ex : 99,99 % = 8s / jour, ou 4min 22s / mois)
- **GTI : Garantie de temps d'intervention**
  - Délai contractuel dans lequel un incident doit avoir été **pris en charge**
- **GTR : Garantie de temps de rétablissement**
  - Délai contractuel dans lequel un incident doit avoir été **résolu**

# SLA : une complexité croissante

- La SLA d'un service dépend de celle du **composant le plus faible**
  - Ex fictif :
    - SLA réseau = 99,999 % (26s / mois)
    - SLA stockage = 99,99 % (4min 22s / mois)
    - **SLA VMWare = 99,9 % (43min / mois)**
- **SLA  $\neq$  perception client !**
  - Ex :
    - Un client loue 3 bases de données avec une SLA de 99,99 % / BDD
    - Si chaque BDD a une panne < 2 min dans le mois, SLA ok mais perception client = 3 pannes de son application dans le mois !
- **Le temps de détection et de prise en charge d'une panne est crucial !**

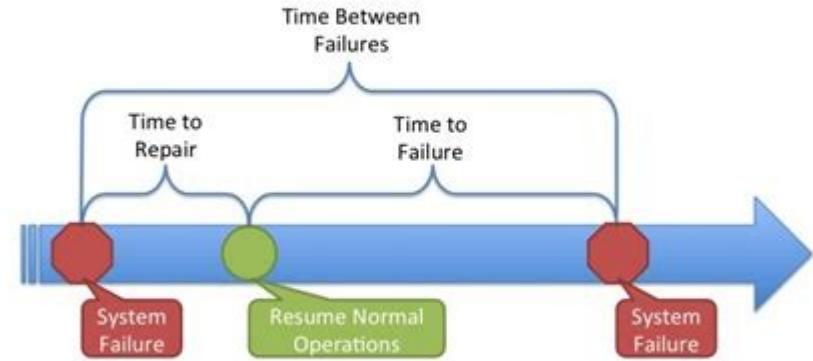
# Différents types de maintenance

- **Maintenance curative :**
  - Consiste à intervenir sur un équipement ou un système après une panne, dans le but de réparer ou corriger.
- **Maintenance préventive :**
  - Consiste à prévoir des actions régulières sur un équipement ou un système afin d'assurer son entretien.
    - Ex : remplacer un disque dur tous les ans.
- **Maintenance prédictive :**
  - Basée sur des modèles d'analyse et des seuils, permet d'anticiper « juste à temps » les interventions nécessaires pour la réparation ou le remplacement d'un équipement ou d'un système.



# MTBF, MTTR, MTTF, FIT...

- **MTTF : Mean Time To Failure**
- **MTTR : Mean Time To Repair**
- **MTBF : Mean Time Between Failure**
- **FIT : Failure In Time**
- **MDT : Mean Down Time**
- ...



MFG	Model	Drive Size	Drive Count	Drive Days	Failures	Annualized Failure Rate
HGST	HMS5C4040ALE640	4TB	2,852	1,048,376	17	0.59%
HGST	HMS5C4040BLE640	4TB	12,746	4,674,986	57	0.45%
HGST	HUH728080ALE600	8TB	1,000	368,454	8	0.79%
HGST	HUH721212ALE600	12TB	1,560	327,080	5	0.56%
HGST	HUH721212ALN604	12TB	10,859	2,848,164	31	0.40%
Seagate	ST4000DM000	4TB	19,211	7,325,582	402	2.00%
Seagate	ST6000DX000	6TB	886	379,894	10	0.96%
Seagate	ST8000DM002	8TB	9,809	3,591,167	125	1.27%
Seagate	ST8000NM0055	8TB	14,447	5,242,891	225	1.57%
Seagate	ST10000NM0086	10TB	1,200	437,259	12	1.00%
Seagate	ST12000NM0007	12TB	37,004	12,721,076	1,156	3.32%
Seagate	ST12000NM0008	12TB	7,215	321,275	10	1.14%
Toshiba	MD04ABA400V	4TB	99	39,788	0	0.00%
Toshiba	MG07ACA14TA	14TB	3,619	564,829	10	0.65%
Totals		122,507	39,890,821	2,068	1.89%	

<https://www.backblaze.com/blog/hard-drive-stats-for-2019/>

# Déterminer des seuils d'alerte

- Déterminer le fonctionnement normal du système (*ne pas se fier aveuglément aux données constructeur ou aux DAT fournis par les prestataires...*) :
  - Benchmarks, tests de résilience...
- Définir des seuils en accord avec :
  - Les résultats des tests et les données constructeurs
  - Les engagements contractuels avec les clients
  - **Les capacités d'interventions des équipes !** (temps d'intervention, outils à disposition...)
- Adapter les seuils d'alerte **au cours de la vie du système :**
  - Evolutions des infrastructures, nouveaux clients, nouvelles SLA...

# Exemples de seuils d'alerte

- **Taux de remplissage d'un espace disque :**

- Tenir compte de l'espace total, du type et de la volatilité des données, des besoins applicatifs et/ou utilisateurs (traitements ponctuels lourds, fichiers temporaires importants...) et de la vitesse de remplissage (nécessite d'avoir des métriques pour adapter dans le temps)
- Exemple classique : **Warning à 80 %, Critical à 90 %**

- **Accessibilité d'un site web :**

- Sur un infrastructure composée de 4 BDD et 20 Frontaux :
  - **Choix 1** : Alerte pour chaque serveur qui tombe
  - **Choix 2** : Alerte uniquement quand le site devient inaccessible
  - **Choix 3** : Mix des deux
    - On détermine à partir de quand le risque de panne totale devient trop important
    - Ou on détermine à partir de quand l'infrastructure ne tient plus la charge

# La gestion des alertes

- Supposons une infrastructure composée d'un serveur de supervision, d'une base de données et d'un poller :
  - *Que se passe-t-il si le poller devient injoignable ?*
    - **Plus aucun check, plus aucune alerte !**
  - **Il est impératif d'avoir une infrastructure distribuée, où les différents composants veillent les uns sur les autres.**
- Supposons une infrastructure distribuée, composée de plusieurs pollers et bases de données réparti·e·s sur 2 datacenters :
  - *Que se passe-t-il en cas de DDOS ou de défaillance du/des transitaires ?*
    - **La supervision peut ne rien détecter, ou ne pas pouvoir alerter !**
  - **Il est vivement recommandé de mettre en place une seconde supervision externe (un VPS chez un hébergeur peut suffire).**



# Envoyer des alertes

- **Une alerte non envoyée = un incident non-traité, voire une situation qui dégénère**
- Il est impératif de prévoir **plusieurs moyens d'envoi** et une bascule automatique en cas d'indisponibilité de l'un deux :
  - SMS via une clé 4G ou un service Web
  - Mail, messagerie instantané...
  - Pager (!)
- Dans un datacenter, la couverture mobile est très mauvaise...
- ... mais en cas d'incident réseau, les mails d'alertes ne passeront pas !
- **Ne pas centraliser l'envoi des alertes sur un seul composant !**



# La gestion des escalades

- Si une alerte ne peut être traitée par le premier niveau de prise en charge, elle doit être « escaladée ».
- Dans beaucoup d'entreprises (type SSII), on parle souvent de :
  - **N1 : gestion des alertes et réponse aux incidents sur procédure simple**
  - **N2 : escalade technique, personnes qualifiées et diagnostique approfondi**
  - **N3 : expertise technique (parfois R&D ou direction technique)**
- L'escalade d'une alerte n'est pertinente que si :
  - Elle est **justifiée** (risque d'engorgement des niveaux supérieurs)
  - Elle est dirigée vers un **service compétent** (nécessite une gestion des compétences et une organisation adaptées)



# La gestion des astreintes

- En dehors des heures ouvrées / horaires de service, la prise en charge des alertes reste **impérative**.
- Il est possible de définir contractuellement :
  - Les **périmètres couverts** par l'astreinte
  - Les **délais d'interventions** si différents
- En astreinte, la gestion des **escalades** reste primordiale :
  - **Escalades techniques** (peuvent nécessiter plusieurs personnes d'astreinte)
  - **Escalades managériales/opérationnelles** (en cas de prise de décisions majeures)
- Une entreprise installée sur plusieurs continents peut ne pas avoir besoin d'astreinte !



# Incidents VS problèmes

- **Incident : évènement ponctuel, avec ou sans impact**
- **Problème : incidents répétés, avec ou sans impact, sur les mêmes composants**
- Incidents et problèmes ne sont **pas uniquement liés à l'infrastructure** : astreinte non prise en charge, procédure erronée..
- Certains outils permettent de remonter les problèmes, mais des **revues régulières** par les responsables de services sont impératives
- **Un incident doit être traité, un problème doit donner lieu à un plan d'action**

# Gouvernance

# Définition

« La gouvernance des technologies de l'information a pour objectif de **mettre en œuvre la stratégie de l'entreprise** et notamment de saisir les différentes opportunités de développement qui s'offrent à l'entreprise. Ainsi **la gouvernance des TI participe à la création de valeur, permet d'optimiser l'utilisation des ressources informatiques et de gérer les risques liés à sa mise en œuvre.** »

Source : Wikipédia

# KPI : définition

- **KPI : Key Performance Indicator**
- **Indicateur mesurable d'aide décisionnelle**, défini **en phase avec la stratégie** de l'entreprise
- Peut être :
  - **Quantitatif** (de façon objective, ex : nombre de tickets résolus par mois)
  - **Qualitatif** (de façon subjective, ex : « bon », « améliorable »...)
- Un succès peut être **l'aboutissement d'un projet** ou le **maintien en conditions opérationnelles** d'un service (incidents traités, tickets suivis...)

# KPI : quelques exemples de métriques

- **Disponibilité :**
  - Temps de résolution des incidents avec impact
  - Quantité de maintenances sur un composant
- **Performances :**
  - Nombre de requêtes par seconde sur une BDD
  - Délais de livraison de nouveaux serveurs
- **Pilotage :**
  - Quantité de tickets ouverts par client
  - Temps de prise en charge et de traitement
- **Sécurité :**
  - Tentatives d'intrusion
  - Failles découvertes et délais avant correction

# Quels outils pour suivre ses KPI ?

- Deux grandes catégories :
  - Les outils d'**extraction**
    - Par « **batchs** » réguliers, sur de grosses volumétries, pouvant effectuer des conversions, des transformations...
    - En « **temps-réel** », en scrutant les échanges inter-applications pour suivre des indicateurs (ex : croiser le stock de serveur disponibles (application de gestion du stock) et le nombre de commandes en cours (« pipe » commercial) pour déterminer la marge disponible et les commandes à prévoir)
  - Les outils de **présentation**
    - **Tableurs**
    - **Tableaux de bord** (spécifiques au métier ou génériques)

# Capacity Planning : définition

« L'objectif de la gestion de la capacité est de garantir que l'infrastructure informatique est fournie **au bon moment, au bon prix et en quantité adéquate** pour tenir la qualité de service en alignement avec **les besoins métiers.** »

Source : Wikipédia

# Gérer un CP : au carrefour des métiers

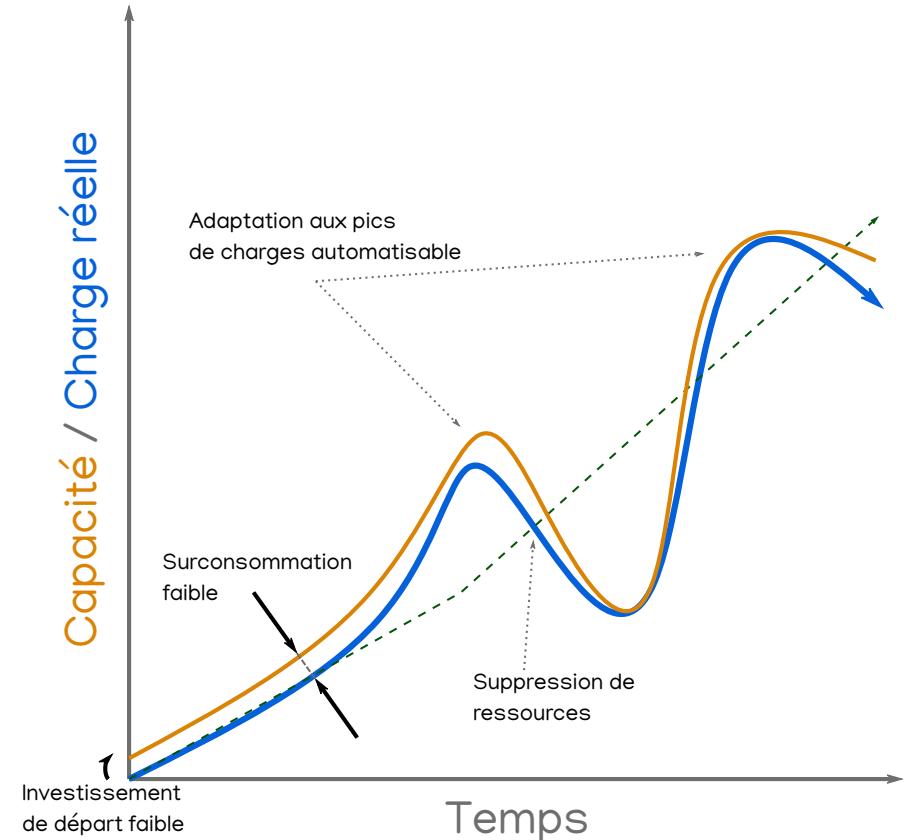
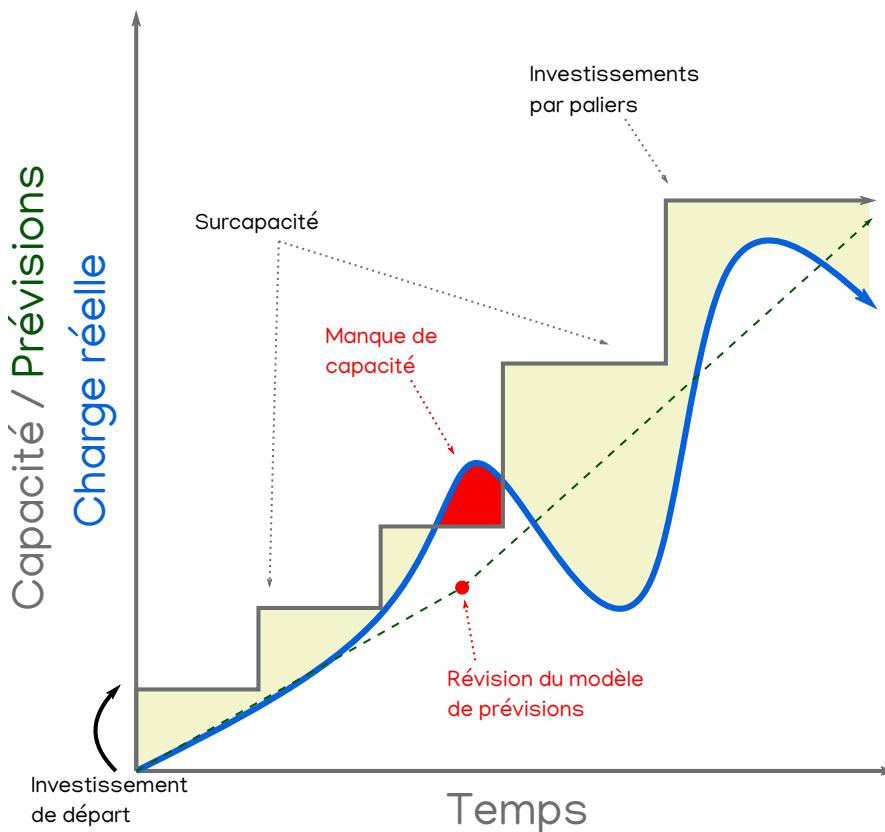
- La gestion de capacité repose sur plusieurs activités :
  - La collecte de **mesures**
  - La production d'**indicateurs** et la définition de **seuils**
  - Le **suivi des demandes** (pour le « run » comme pour le « build »)
  - La **planification**, avec les équipes techniques et la gouvernance
- Elle doit tenir compte :
  - Des **ressources matérielles** (serveurs, licences...)
  - Des **projets** en cours et à venir
  - Des **enveloppes budgétaires** actuelles et à venir
  - Des **équipes** et des **compétences**

# Gérer un CP : au carrefour des équipes

- Un Capacity Planning doit être géré **conjointement par les équipes techniques et la gouvernance** (responsables clients, chefs de projets et direction)
  - Les équipes techniques connaissent les plateformes mais n'ont pas forcément connaissance de la **stratégie** de l'entreprise ou de l'arrivée de nouveaux **projets clients**
  - La gouvernance n'a pas forcément conscience des enjeux de tel ou tel investissement sur la **qualité** ou le **taux de disponibilité** du service
- Un investissement (financier, matériel, humain...) :
  - Trop faible = dégradation des conditions de travail, de la disponibilité et des performances du service, des **capacités de vente**, de la **satisfaction client**...
  - Trop important = une diminution de la **marge** de l'entreprise, des ressources mal exploitées...



# Gérer un CP : CAPEX VS OPEX

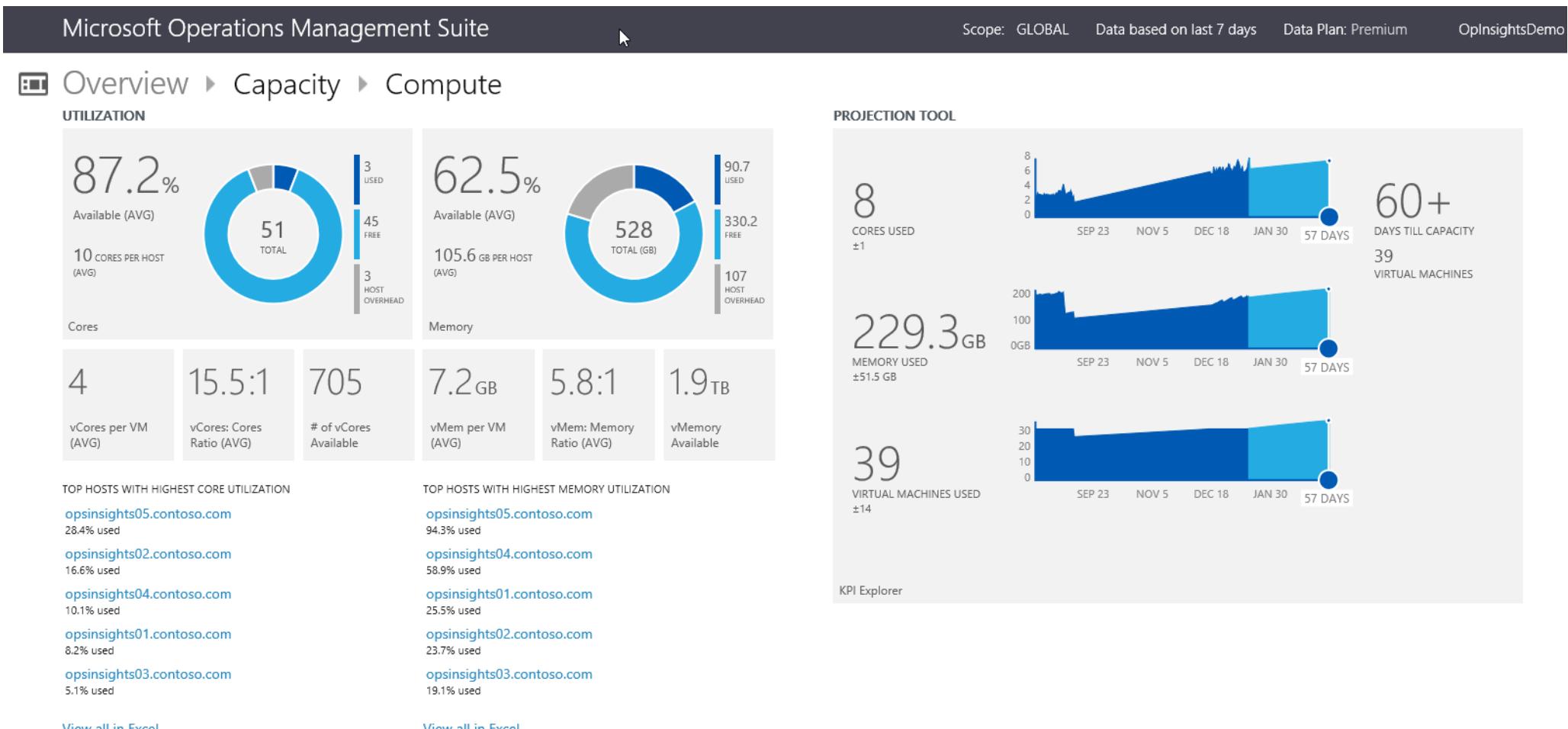


Source : Module de Cloud Computing, par OVH (Crédit : Pierre Gaxatte)

# Quels outils pour gérer son CP ?

- D'un point de vue « **pilotage** » :
  - La définition et la communication de la **stratégie** de l'entreprise
  - Des revues régulières des **projets** et des **commandes** clientes
  - Un suivi des **compétences** des équipes
- D'un point de vue « **technique** » :
  - Des revues régulières des outils de **supervision** et de **métrie**
  - Certains outils de supervision ou de pilotage d'infrastructures permettent de visualiser les tendances d'évolution des infrastructures, et d'anticiper les modifications requises (ex : rajouter une baie de disques dans 2 mois)
  - La création de **dashboards** métiers spécifiques (en s'appuyant par exemple sur Kibana ou Grafana)
  - Une **veille technologique** avancée : nouveaux outils, matériels...

# Quelques exemples d'outils de CP



# Quelques exemples d'outils de CP

**centreon**

pollers 0 hosts 0 services 5 5 4 0 118 118 October 17, 2018 6:18 PM

Home Database F5 Datacenters Tem/Hum Global IT status & current events Network availability & reliability analysis Traffic & Nb connection on Firewall ACME corp. Centreon Website Customer Journey Global Infrastructure Availability HILLMORE Insurance Mail service analysis Mail Service Dashboard Open Tickets Services map Tactical Overview Top 10

**Administration**

- Parameters
- ACL
- Access List
- Access Groups
- Menus Access
- Resources Access
- Actions Access
- Reload ACL
- Centreon MBI
- AOL rules**
- Extensions
- Logs
- Sessions
- Platform Status
- About

**Main MAIL service components' health**

Name	Status	Since	Current Level
Mail-Masters	Not available	28m 14s	0%
Mail-IDF	Not available	34m 2s	0%
Mail - User Experience	Degraded	8m 2s	50%
Mail-Frontends	Degraded	1h 16m	60%
Load-Balancer-Mail-IDF	Available	1h 57m	100%
Mail-Gateways	Available	1h 38m	100%
Mail-Scenarios	Available	8m 2s	100%
Mail-Backends	Available	56m 11s	100%

**Mail service end-user availability - Current month**

**Mail-Scenarios**  
24x7  
Period: Unav. time Warn. SLA SLA: 99.9

**Mail service end-user availability - Last 12 months**

**Mail-Scenarios (24x7)**

**Risky storage spaces evolution on mail servers**

**Resources** Est. saturation Evol. vs yesterday Current usage

mail-jupiter-frontend - disk-/-	29.3 days	-52.64% ↘	19.15%
mail-earth-frontend - disk-/-	31.4 days	88.99% ↗	71.91%
mail-neptune-frontend - disk-/-	44.2 days	81.65% ↗	69.74%
mail-uranus-frontend - disk-/-	60.4 days	-32.37% ↘	26.62%

**Storage space /usr on main mail frontend server - Projection based on the last 30 days**

Indicator : used for service : disk-/usr on mail-earth-frontend It will reach 79.00Go in +3 months (323 days - 2019-09-05)

**Average mail queue on front end servers - Last 31 days**

**24x7**

**Typical 24h mail queue on main mail frontend server vs today's usage**

Indicator : queue. Current value: 497.0 Service : postfix-queue on mail-earth-frontend

Documentation | Centreon Support | Centreon | Github Project | Slack Copyright © 2005 - 2018

# Hypervision

# Définition

« En informatique, l'hypervision est la **centralisation des outils de supervision** d'infrastructure, d'applications et **de référentiels** (par exemple, la base de données configuration management database - CMDB). Il s'agit d'un outil **d'agrégation** ou de console unique. »

Source : Wikipédia

# Principe de l'hypervision

- Un SI complexe devant fournir plusieurs services et composer avec plusieurs équipes et applicatifs/outils = plusieurs outils de supervision, de ticketing...
- **Trop d'interfaces = pertes de temps et d'informations**
- Une console d'hypervision permet généralement de retrouver :
  - Un **bac à évènement** complet (alertes de supervision, logs, tickets en cours...)
  - Une **corrélation des évènements**
  - Des **indicateurs** (statistiques, métriques importantes) permettant d'avoir une **vision globale** de tout le SI

# Les avantages de l'hypervision

- Une **console centralisée** avec des **vues adaptées** à chaque besoin (gouvernance, technique, client...)
- Des **indicateurs** déjà calculés et exploitables pour les KPI
- Des **corrélations d'évènements** permettant d'identifier des problèmes complexes
- Exemple de corrélation possible :
  - 1) Une forte charge réseau In/Out est détectée sur les plateformes (supervision)
  - 2) Une attaque DDOS est identifiée (outils externes + alertes prestataires)
  - 3) Des systèmes de fichiers sont soumis à une forte charge en lecture à une heure inhabituelle (supervision)

➔ ***Tentative d'extraction de données masquée dans le flux ?***

# Les inconvénients de l'hypervision

- Un domaine assez peu connu
- Peu d'outils disponibles
- Une **complexité** de mise en place importante et croissante en fonction de la quantité d'outils à interfaçer
- **Connecter des outils, c'est bien, mais réussir à les exploiter, c'est mieux !**
  - Identifier les informations importantes à mettre en avant est difficile
  - Créer des règles de corrélation d'évènements est complexe, car l'infrastructure évolue sans cesse

# Les outils d'hypervision

- Aujourd'hui, plusieurs éditeurs de solutions de supervision commencent à intégrer des outils d'hypervision : Centreon, Zabbix...
- Des éditeurs proposent des solutions clé-en-main : Canopsis (de Capensis)
- D'autres proposent des solutions sur-mesure intégrées au SI (plus complexes, plus coûteuses mais potentiellement plus efficaces) : BMC, IBM, HP...
- Pour certains besoins ou secteurs industriels, on peut également trouver des outils et consoles spécifiques

# Un exemple de console d'hypervision spécifique



# Un autre exemple de console d'hypervision

The screenshot displays the Canopsis monitoring interface. On the left, a sidebar shows navigation categories: MDS (selected), Bac à alarmes, Contexte, and a gear icon for administration. The main area has a green header bar with the title "Météo des services". Below it is a grid titled "Météo des services" containing 12 service status cards. The cards are arranged in four rows of three. Each card includes a small icon, a name, and a subtitle. The colors of the cards indicate different service states. Below the grid is a section titled "Bac à alarmes" which contains a table of alarm logs.

Search	Filter	Selectionner un filtre							
<input type="checkbox"/>	Connecteur	Nom du connecteur	Composant	Ressource	Output	Détails supplémentaires	État	Status	Actions
<input type="checkbox"/>	periode	contemporaine	Révolution industrielle	Photographie	1899		major	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	canopsis	engine	periode			3 ok, 1 minor, 1 major, 1 critical	critical	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	canopsis	engine	moderne			0 ok, 1 minor, 0 major, 1 critical	critical	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	canopsis	engine	contemporaine			0 ok, 0 minor, 1 major, 0 critical	major	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	periode	Historique	Antiquité	Fondation de Rome	-753		minor	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	periode	Historique	Moyen âge	Séments de Strasbourg	842		major	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	periode	moderne	Renaissance	L'École d'Athènes	1509-1510		minor	En cours	<span>OK</span> <span>✓</span> <span>⋮</span>
<input type="checkbox"/>	periode	moderne	Les lumières	L'Encyclopédie	1747-1765		critical	En cours	<span>OK</span> <span>✗</span> <span>⋮</span>

# Conclusion

---

# In the end...

- Supervision ?
  - **Vérification de l'état d'un composant ou d'un service**
- Métrologie ?
  - **Mesure des performances ou des capacités dans le temps**
- Mettre en place des solutions de supervision :
  - Établir un **cahier des charges** avec toutes les parties prenantes (gouvernance **ET** opérations)
  - Procéder à une **étude technique comparative**
  - Choisir l'**outil adapté** et y mettre les **moyens** (humains et financiers)

# Contact

**Florian Haller-Casagrande**

Mail : [florian@haller-casagrande.fr](mailto:florian@haller-casagrande.fr)

LinkedIn : <https://www.linkedin.com/in/florianhc>