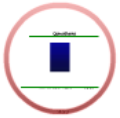


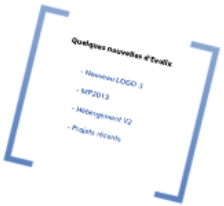
Rdv Techno
Monitoring Open Source

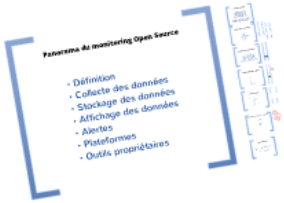
- Quelques nouvelles d'Evolix
- Introduction
- Témoignage CG13 sur le projet NagiosRT
- Retour sur le projet NagiosRT pour le CG13
- Panorama du monitoring Open Source
- Architecture du monitoring Evolix

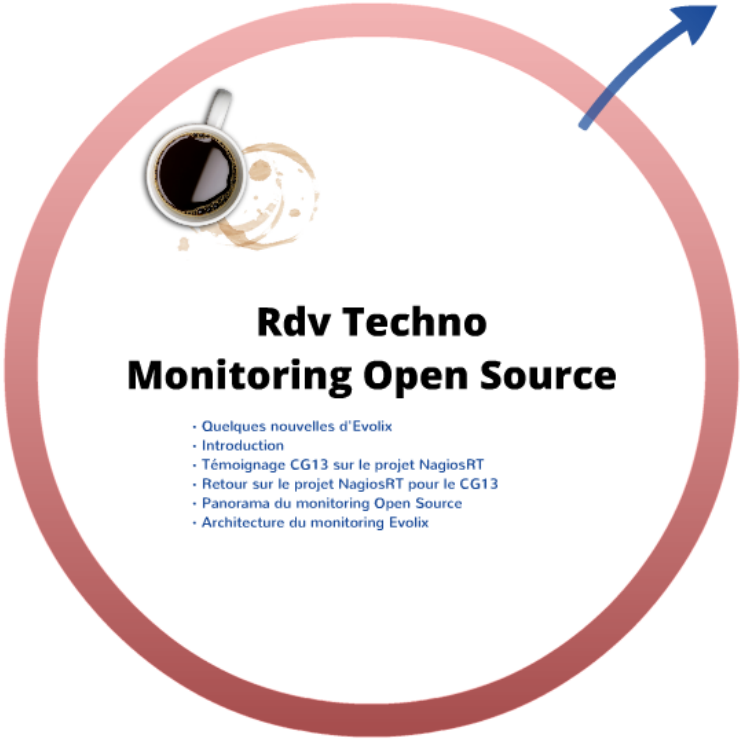
?

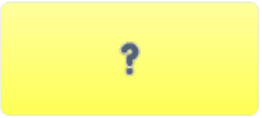
evolix

Hébergement et Infogérance Open Source









evolix

Hébergement et Infogérance Open Source

Quelques nouvelles d'Evolix

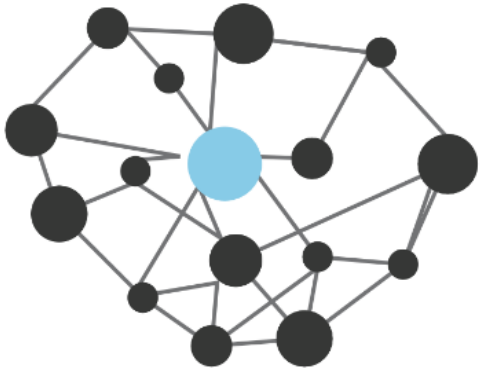
- Nouveau LOGO :)

- MP2013

- Hébergement V2

- Projets récents

evolix



Hébergement et Infogérance Open Source

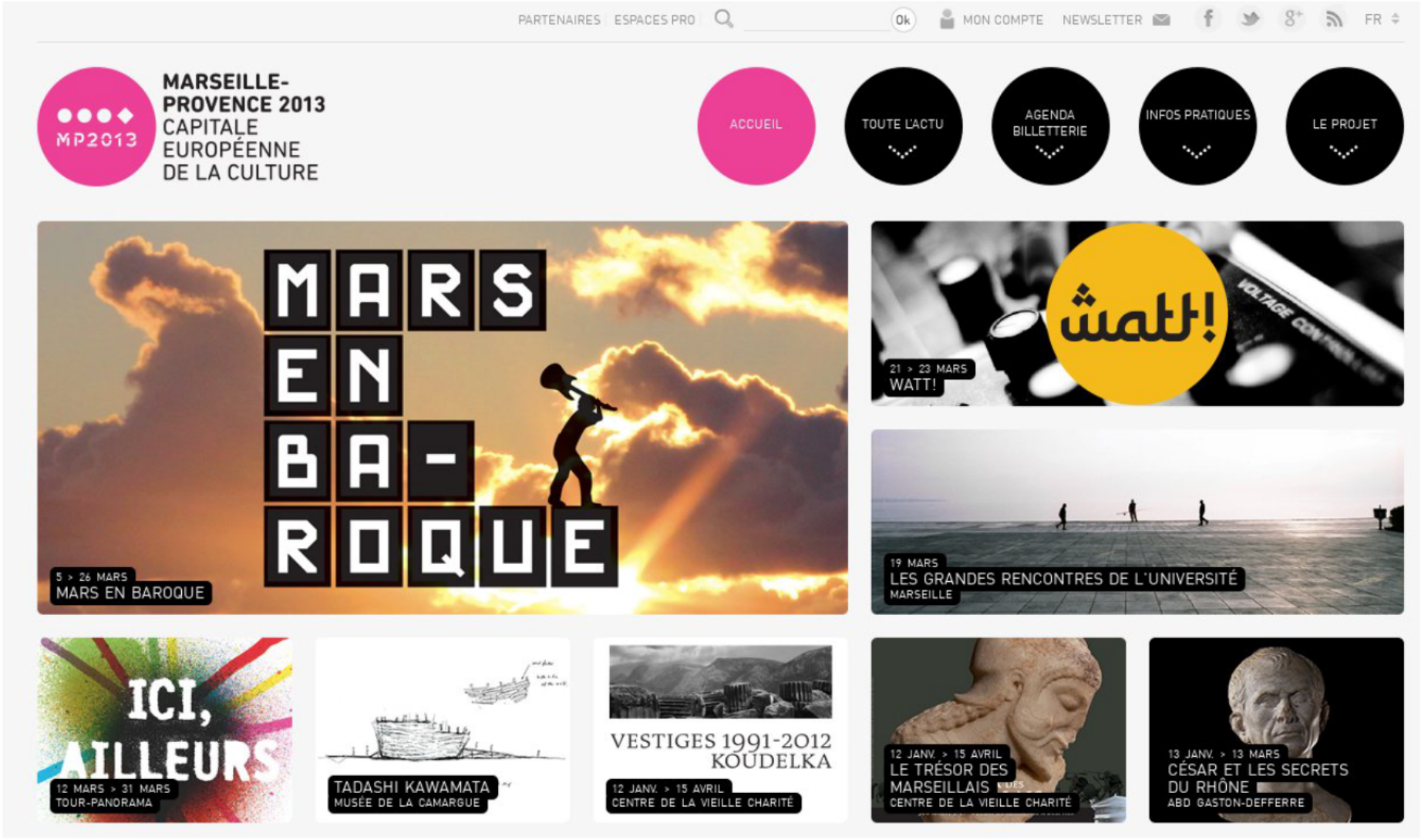
Quelques nouvelles d'Evolix

- Nouveau LOGO :)

- MP2013

- Hébergement V2

- Projets récents



Hébergement Evolix - Serveur dédié loué avec PRA/PCA activable

Quelques nouvelles d'Evolix

- Nouveau LOGO :)

- MP2013

- Hébergement V2

- Projets récents

Hébergement Evolix - Serveur dédié loué avec PRA/PCA activable

Serveur matériel proposé DELL PowerEdge R320 CPU Intel Xeon E5-1410 2.80GHz (4 coeurs) 16 Go de RAM 2 disques hotplug SAS 15K de 300 Go, Raid 1 hardware Carte raid **avec** cache (H700 NV 512 Mo)	

Un serveur dédié de qualité

Serveurs de marque neuf avec taux de panne extrêmement bas.
Serveur personnalisable (CPU, mémoire ECC, disques SATA/SAS (gamme pro))

Hosting très haute qualité

Hébergement dans des datacenters sécurisés (minimum tiers IV).
Equipements réseau redondants
Réseau BGP indépendant
Accès physique possible

PRA/PCA activable

En option mise à disposition d'une machine virtuelle capable de prendre la suite en cas de crash du serveur dédié
Deux fréquences de synchronisation : journalière (PRA) ou permanente (PCA)

Infogérance 24h/24

Monitoring et supervision 24/24 7/7
Sysadmin Evolix joignable directement 24/24 7/7
Mises-à-jour mineures et majeures incluses
Panel Evolix et Sauvegarde

Infrastructure évolutive

Votre serveur a des ressources extensibles (CPU/RAM/Disques)
Evolution possible vers infrastructure multi-serveurs (avec inter-liens Go)

Interlocuteur expert

Installation basée sur plus de 8 ans d'expérience.
Conseils d'optimisation par des sysadmin reconnus (projet Debian, OpenBSD...)

Quelques nouvelles d'Evolix

- Nouveau LOGO :)

- MP2013

- Hébergement V2

- Projets récents

Introduction

- Définition
- Contexte Evolix
- Exemple Client : CG13

Introduction // Définition

Définition de monitoring :
Système de surveillance électronique

- Collecte des données
- Stockage des données
- Affichage des données
- Déclenchement d'alertes

=> monitoring système & réseau
=> solutions Open Source

Introduction // Contexte Evolix

- Evolix infogère environ 350 serveurs pour une 50 clients, répartis dans différents datacenters et chez nos clients.
- Nous nous efforçons d'améliorer continuellement notre monitoring système & réseau.
- Nous mettons en place également du monitoring pour nos clients qui le souhaitent !

Introduction // Exemple Client : CG13

Monitoring pour le service SRT (Service Réseau et Télécom)

- Surveillance principalement switchs / flux réseau
- Existant : vieille version de WhatsUp

Recherche d'une solution standalone

- FAN (Fully Automated Nagios) : distribution Linux basée sur CentOS intégrant Centreon / Nagvis
- EON (EyesOfNetwork) : distribution Linux basée sur CentOS intégrant LILAC/Nagios/Nagvis/Cacti/weathermap.

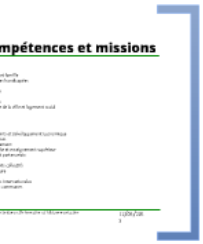
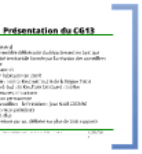
=> FAN jugé pas assez mature, EON correspondant au besoin.

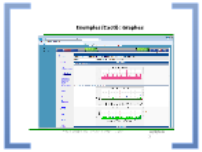
Introduction // Exemple Client : CG13

« audit » EON par Evolix fin 2010

- Basé sur une distribution CentOS avec des paquets modifiés et 3 paquets spécifiques (eonconf,eonweb,ged).
- Sources accessibles mais développement... fermé! Pas de bugtracker, surtout pas de SCM, les sources des paquets accessibles via un .ISO contenant les .SRPM (!)
- On ne sait pas quel paquet est patché, quels sont les patchs appliqués et ils ne sont pas documentés (pas de changelog...)

=> Conclusion : afin d'avoir une solution souple et pérenne, nous sommes donc partis sur l'intégration des logiciels demandés : LILAC/Nagios/Nagvis/Cacti/weathermap
avec une légère surcouche web pour tout centraliser.



Témoignage de la Direction des Systèmes d'Information et Télécommunication du CG13

Monitoring Réseau au CG13

12/03/2013

SOMMAIRE

Présentation du CG13
Ses compétences et missions
Son budget
Son réseau
Le monitoring
Quelques exemples
Questions

Présentation du CG13

Le Conseil Général

C'est l'assemblée délibérante du département en tant que collectivité territoriale formée par la réunion des conseillers généraux

Le département 13

1 979 267 habitants (en 2009)

Superficie : 5 087,5 Km2 soit 16,2 % de la Région PACA

L'axe Nord-Sud : 80 Km, l'axe Est-Ouest : 150 Km

119 communes, 57 cantons

La commission permanente

56 conseillers + le Président : Jean Noël GUERINI

15 vice-présidents

41 élus

11 sessions par an, délibère sur plus de 2000 rapports

Ses compétences et missions

Solidarité
- Enfance et famille
- Personnes handicapées
- Seniors
- Insertion
- Santé
- Jeunesse
- Politique de la ville et logement social

Éducation
- Collèges

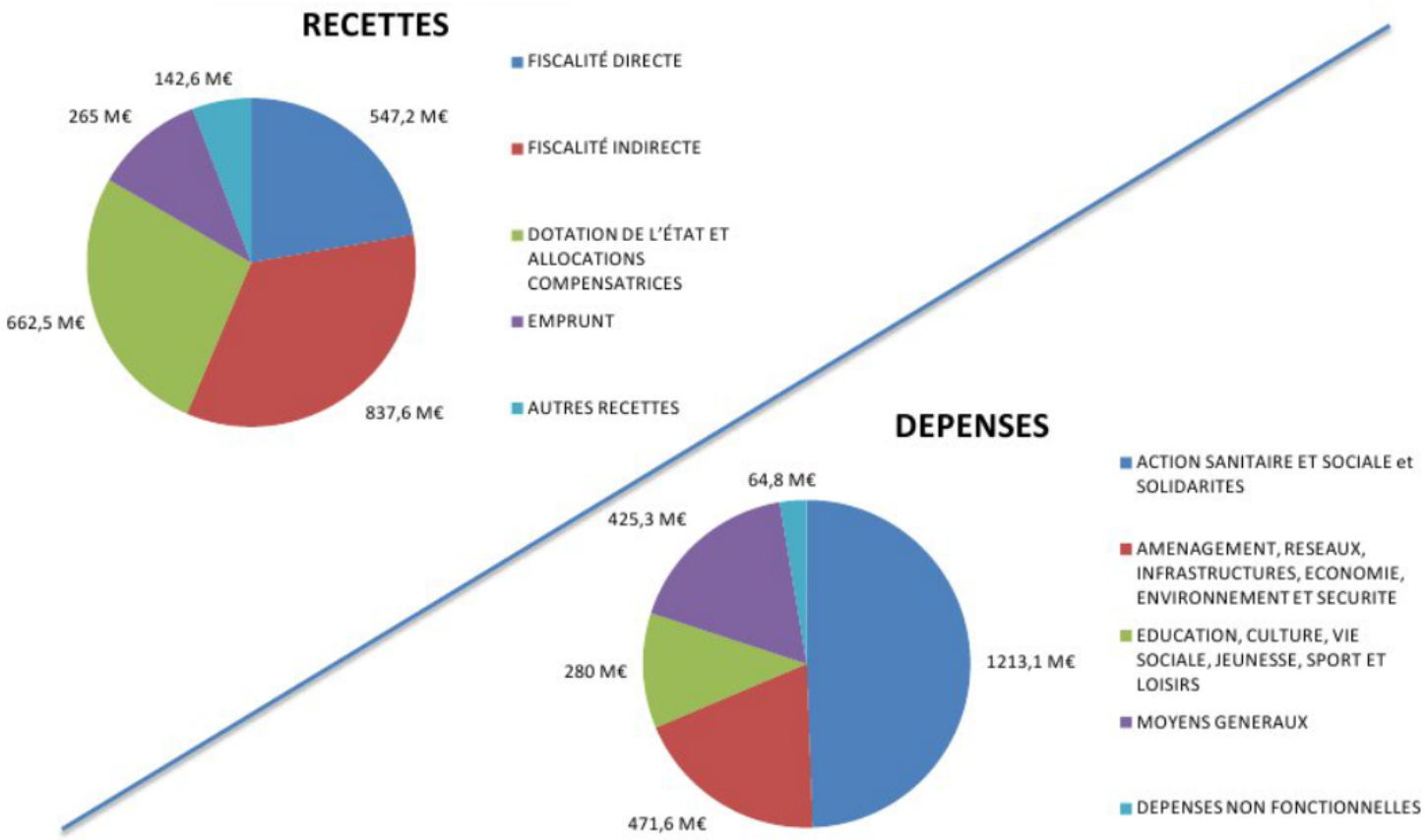
Aménagements et Développement Économique
- Entreprises
- Aménagement
- Recherche et enseignement supérieur
- Etudes et partenariats
- Routes
- Transports collectifs
- Agriculture
- Ports
- Relations internationales
- Aide aux communes

Ses compétences et missions (suite)

Cadre de Vie
- Tourisme
- Environnement
- Culture
- Sports
- Santé
- Vie associative

Le Conseil Départemental De Concertation (CDC)
- Véritable collège d'experts, c'est une instance consultative qui mène des études, réflexions, critiques et propositions sur des thèmes d'actualité

Son budget (2,5 Md €)



Son réseau

Sites CG13

- 2 sites principaux
  - Hd13
  - Arenc
- ~160 sites distants

Collèges (~ 96 000 élèves)

- ~140 publics
- ~50 privés

Equipements LAN

- Réseau CG13 : ~700
- Réseau collège : ~1 500
- Sécurité : ~150

Equipements WAN

- Routeurs CG13 : ~140
- Routeurs collège : ~160

Equipements Wifi

- Bornes CG13 : ~500
- Bornes collèges : ~6000

Equipements ToIP

- Serveurs : ~15
- Téléphones : ~4500

Le monitoring

Une nécessité au CG13

- Un besoin de surveillance du périmètre précédemment listé (excepté les routeurs, certains serveurs ToIP et en grande partie les téléphones et bornes Wifi)

Notre console d'administration actuelle

- 1 plateforme unique : un serveur HP Proliant DL380/G7
- avec l'OS : CentOS version 5.7
- composée de Nagios, Cacti, Nagvis, Weathermaps, Smokeping, NFSen

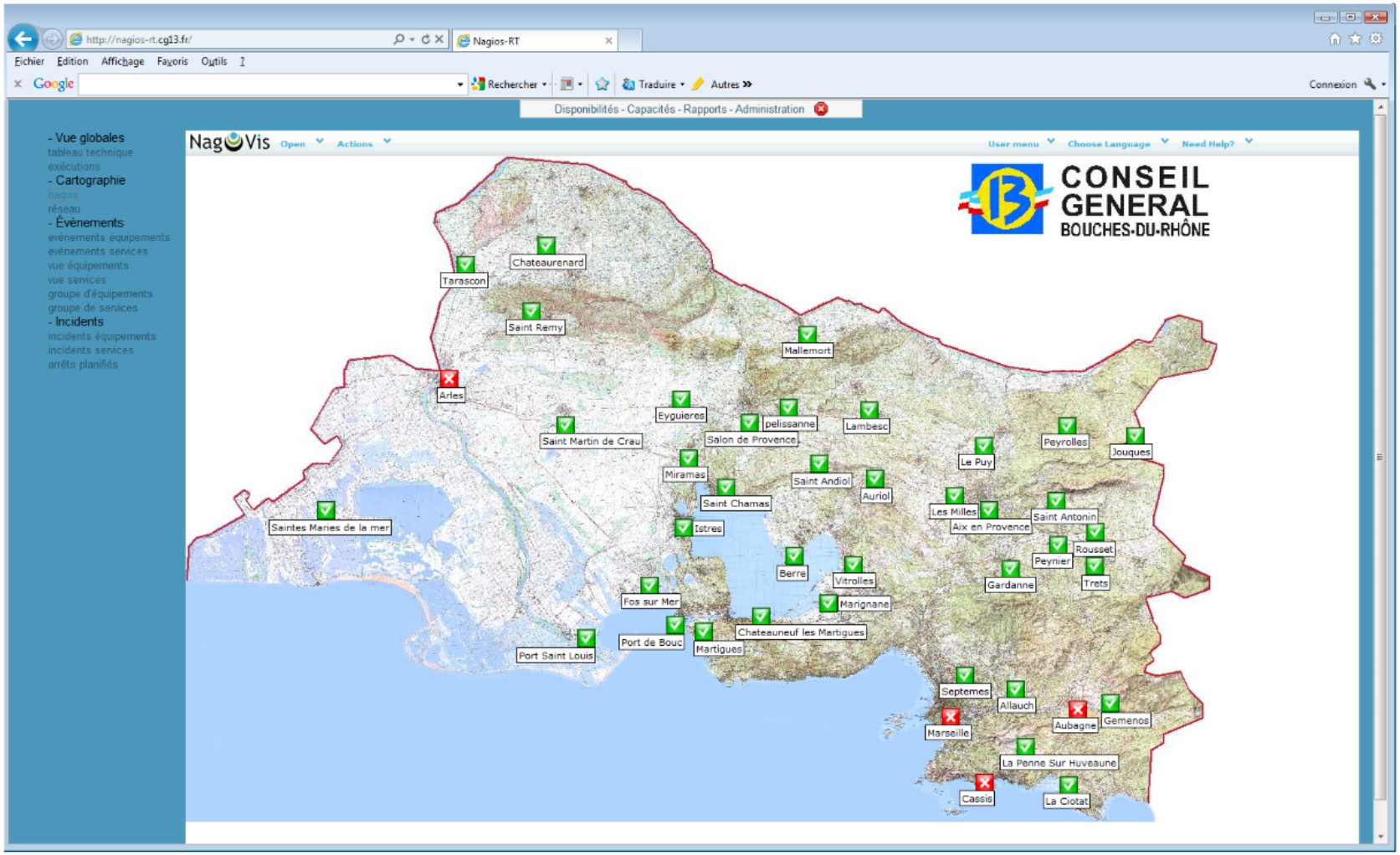
Notre console customisée

- À partir d'Eon (Eye On Network)
- Gestion niveau login : administrateur ou utilisateur
- Remplacement NTOP par NFSen
- Debian privilégié mais contrainte package OS du CG13

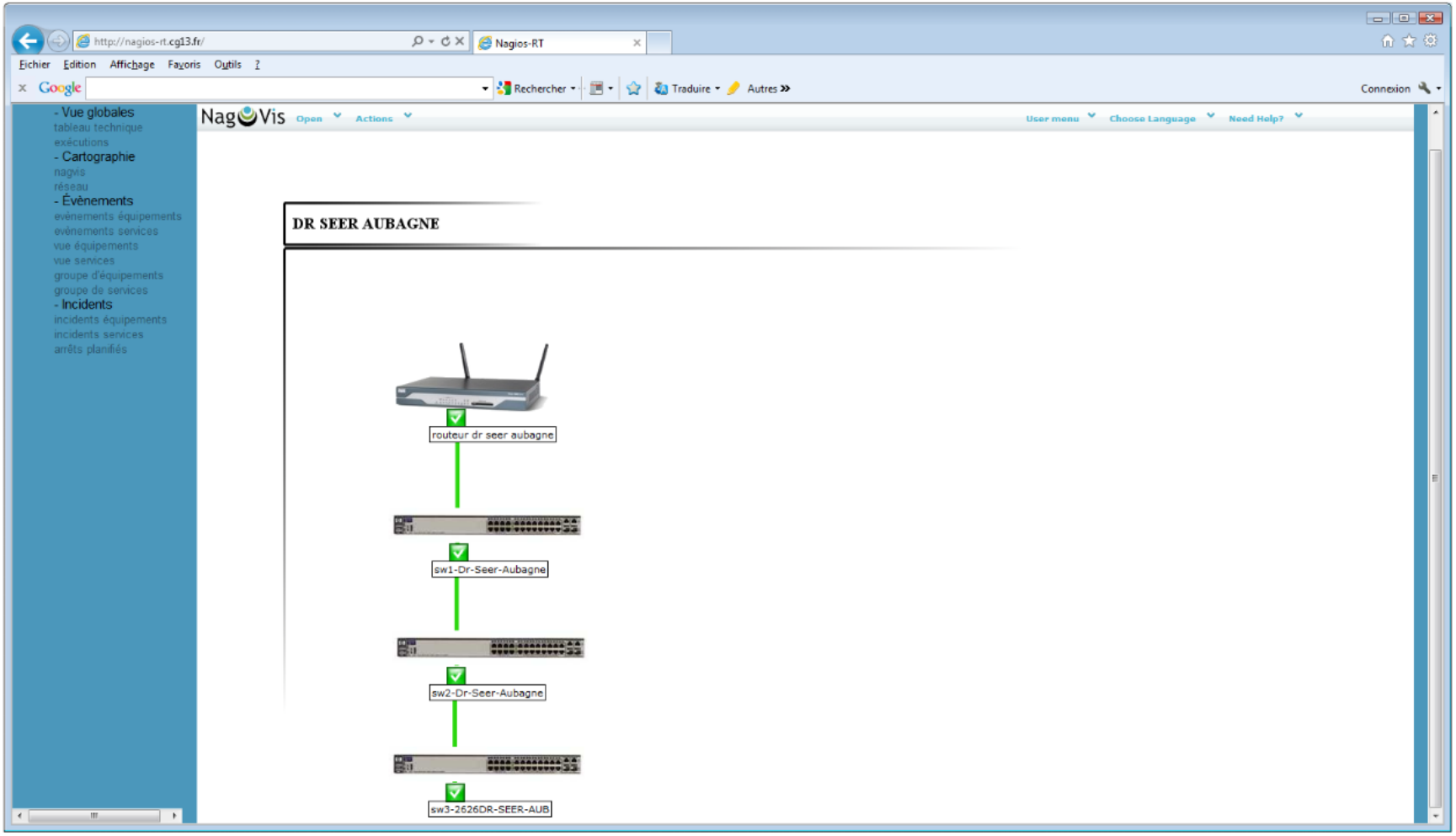
Nos objectifs 2013

- Redondance de la console
- Développement de dashboards

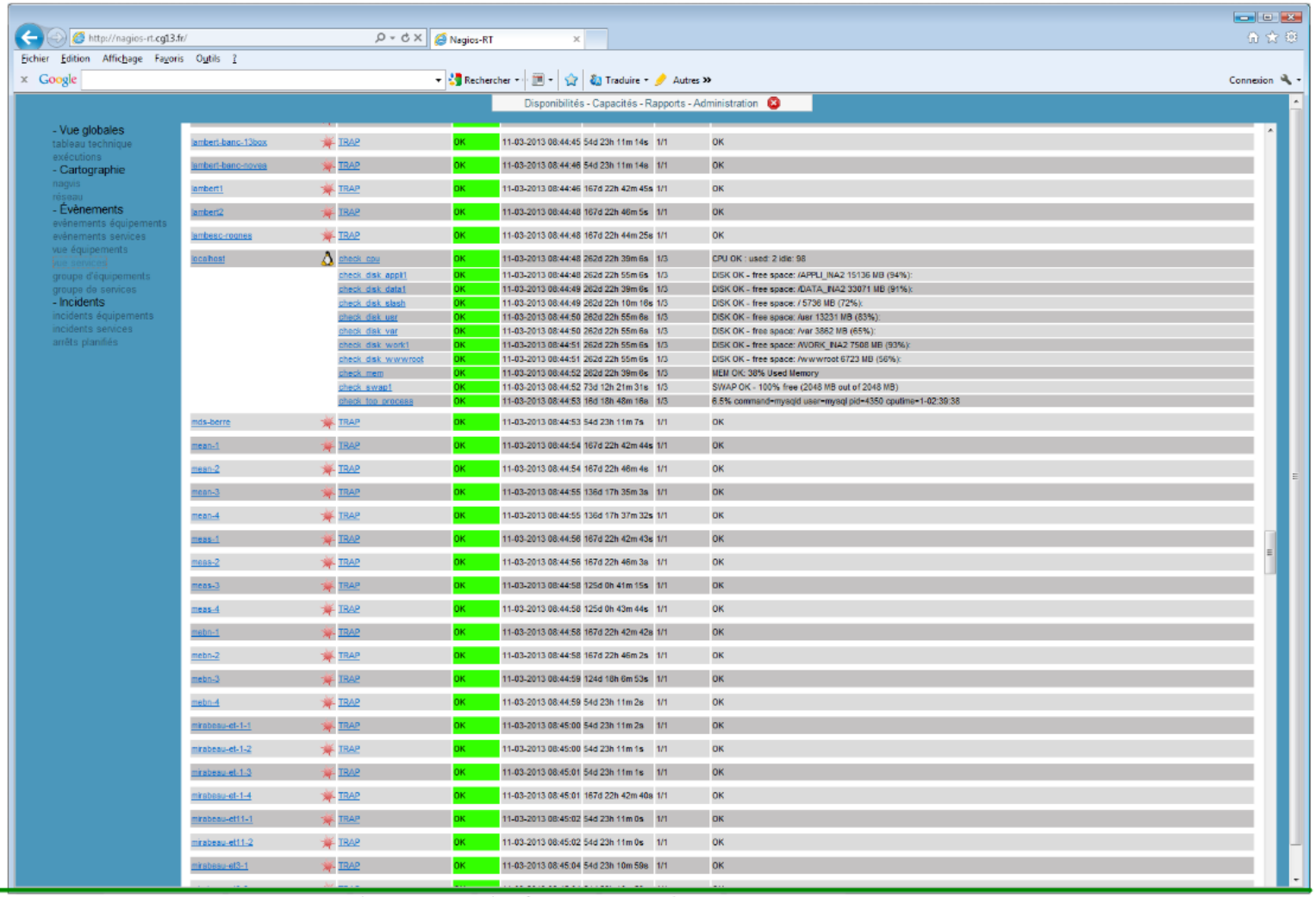
Exemples (Nagvis): Map



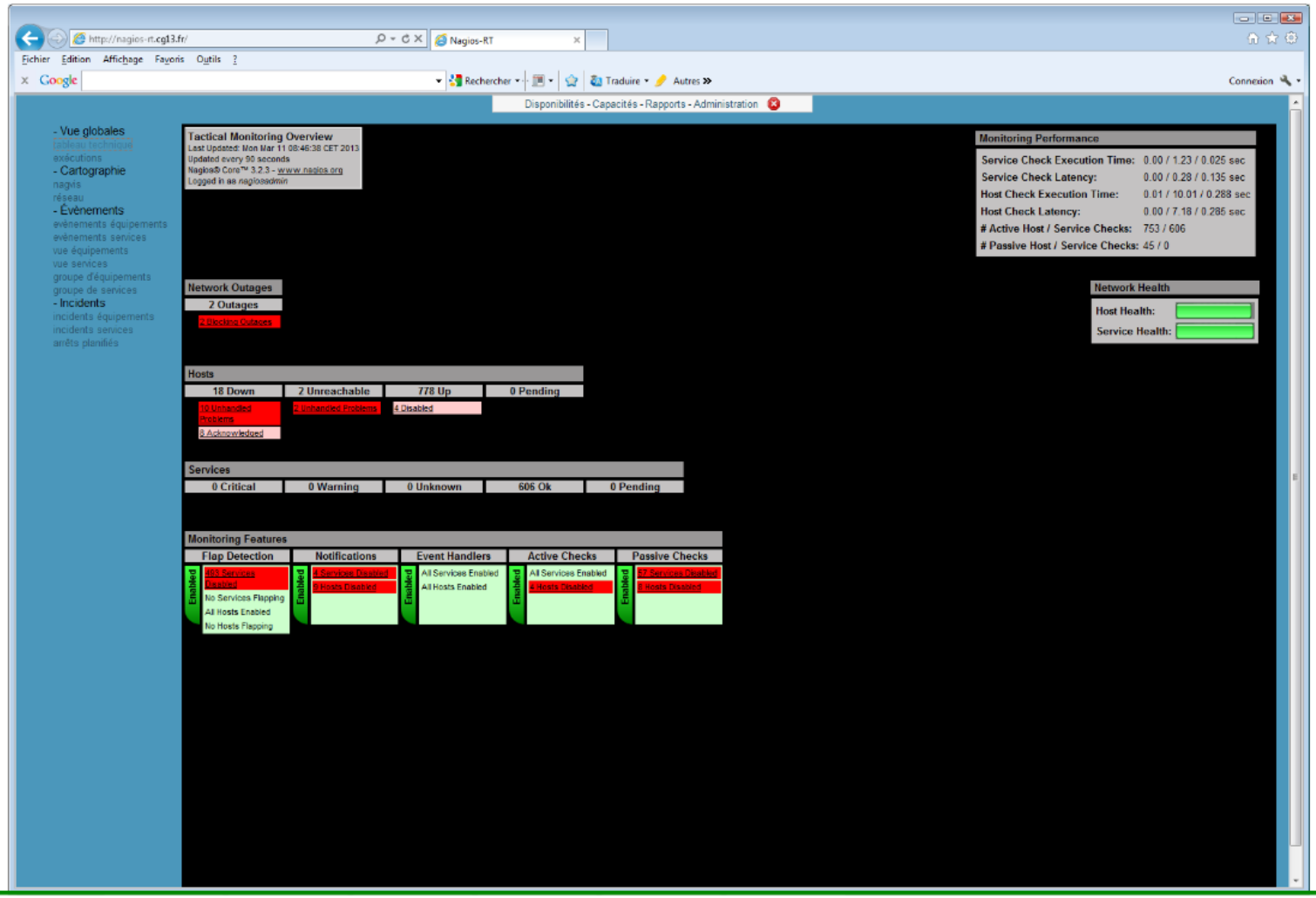
Exemples (Nagvis): Topologie réseau



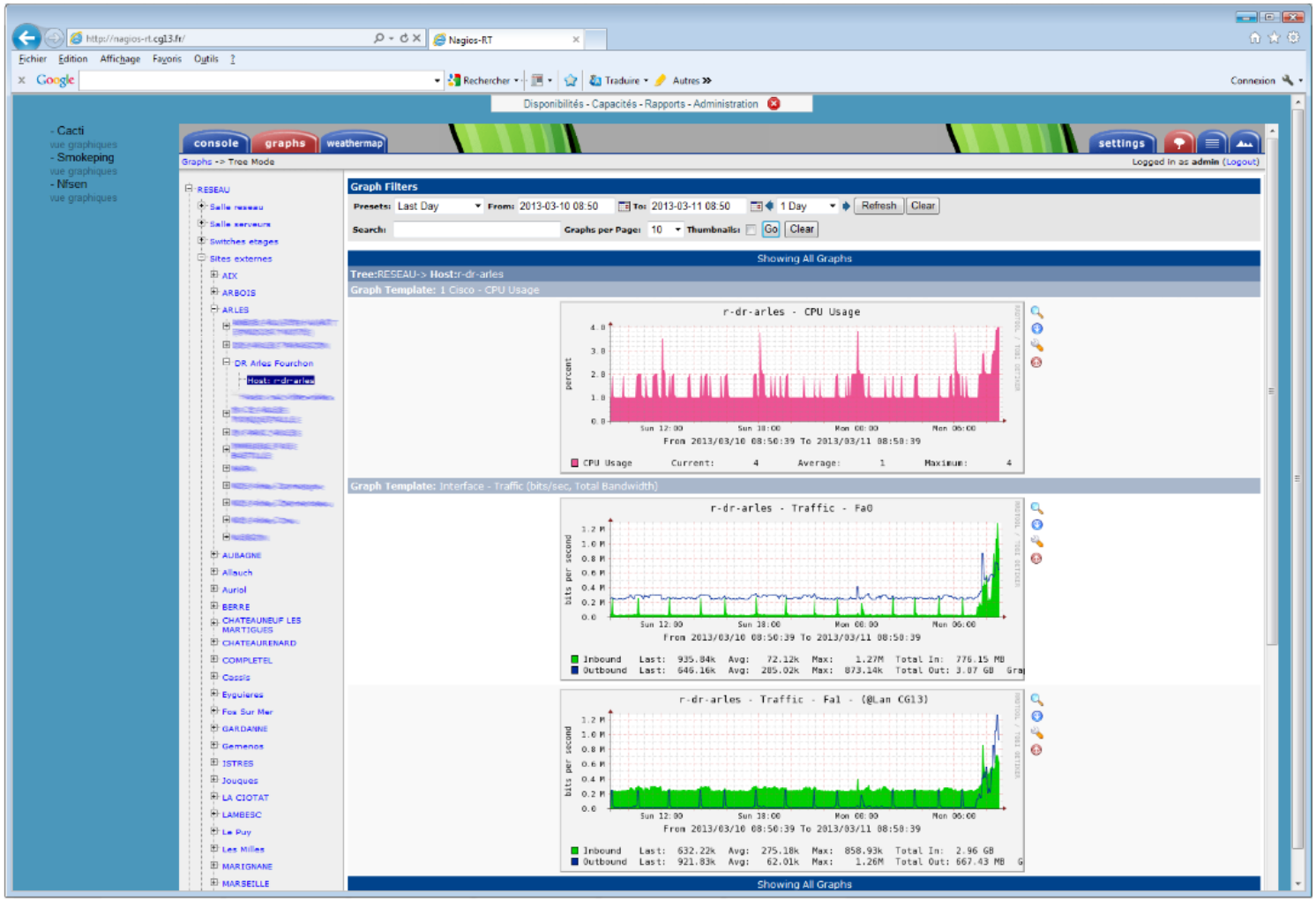
Exemples (Nagvis): Vue des services



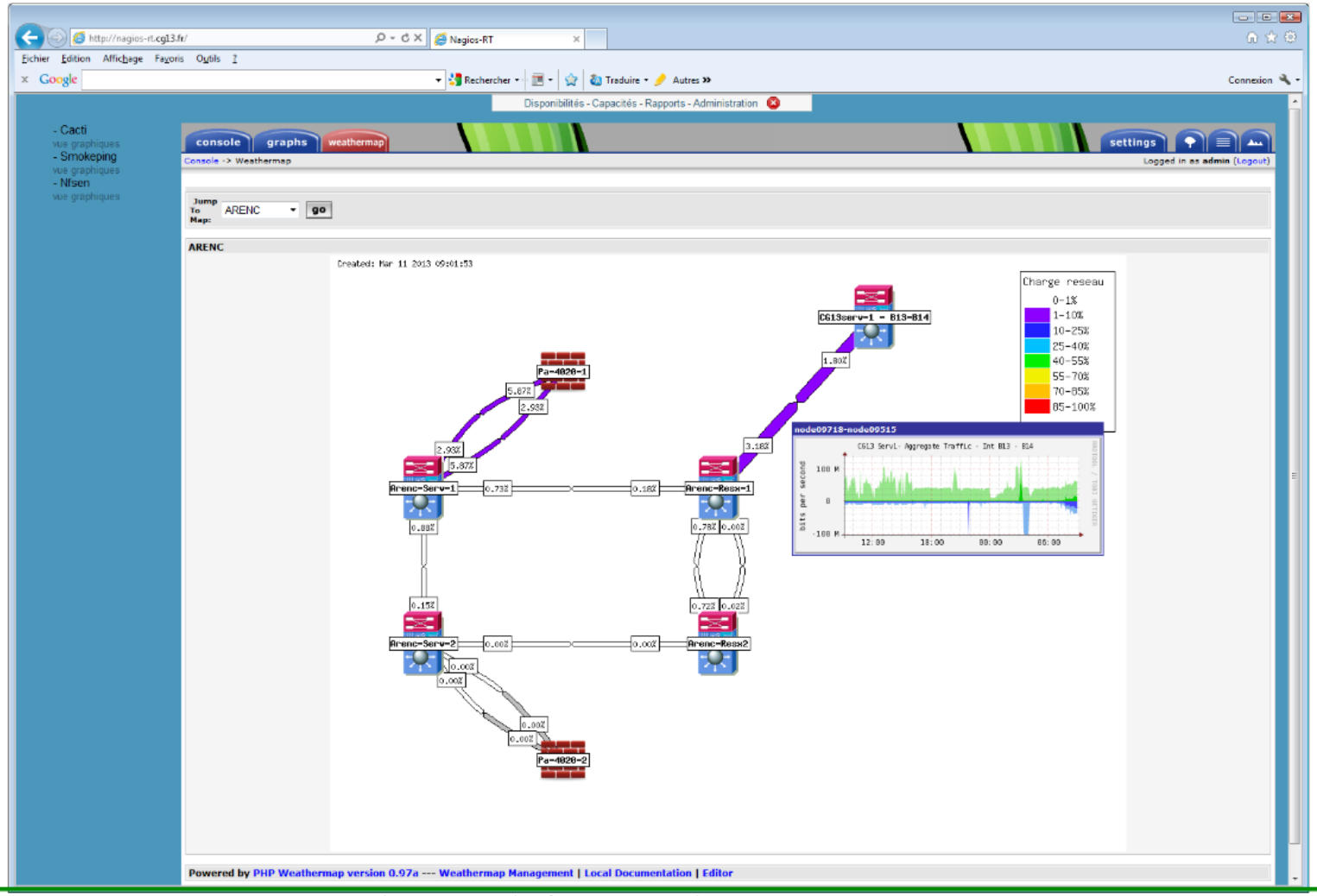
Exemples (Nagios) : Overview



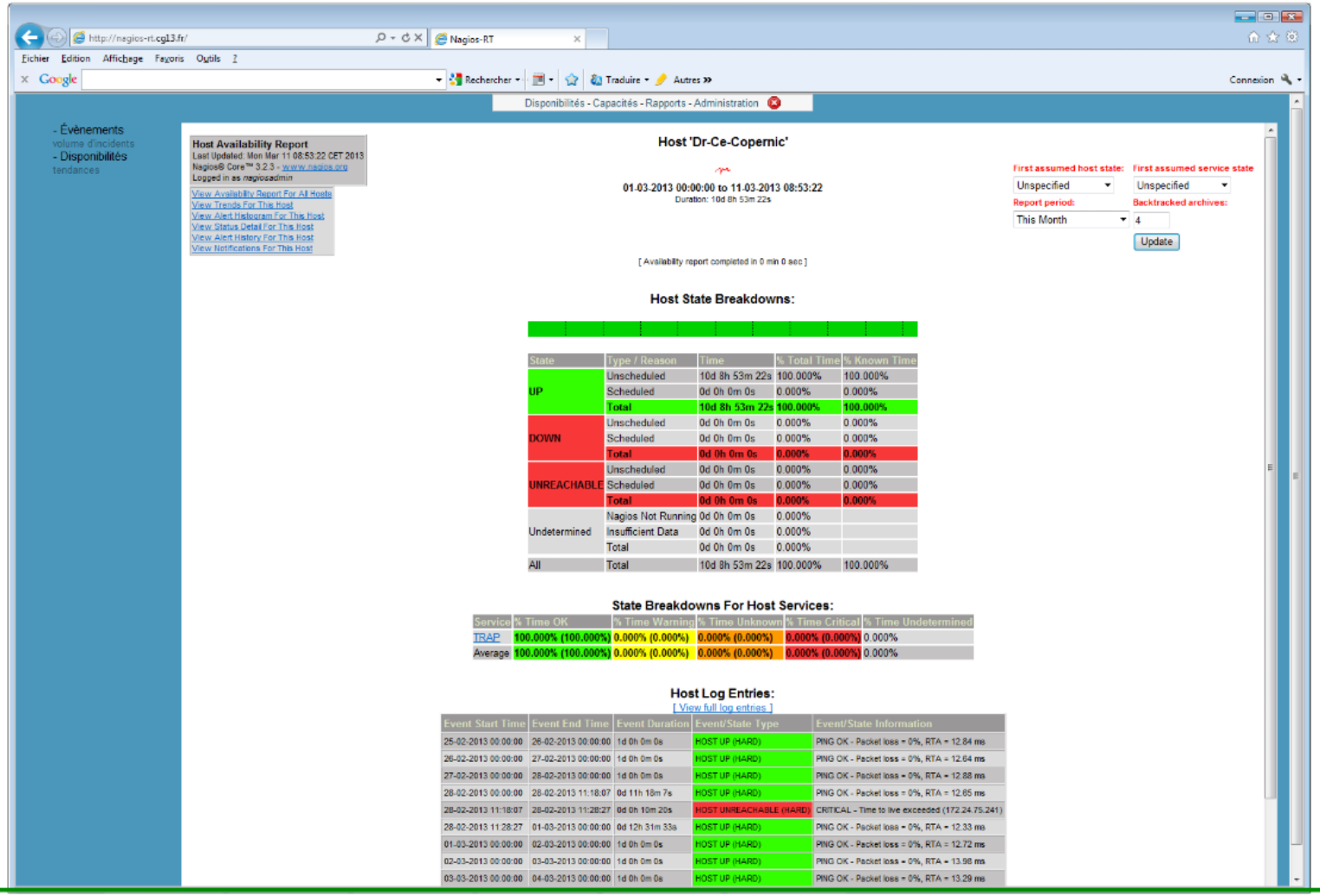
Exemples (Cacti) : Graphes



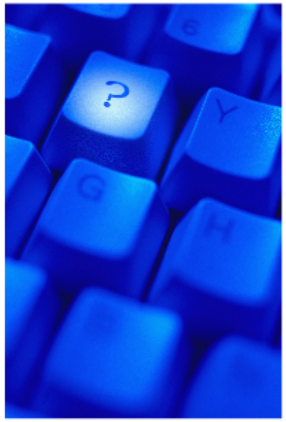
Exemples (weathermap): Charge liens



Exemples (Nagios): Rapport



Questions



Merci

Témoignage de la Direction des Systèmes d'Information et Télécommunication du CG13

Monitoring Réseau au CG13

Retour sur le projet NagiosRT pour le CG13

- Objectifs
- Fonctionnalités
- Logiciels utilisés

NagiosRT // Objectifs

- Disposer d'un outil de supervision permettant de générer des statistiques et des rapports paramétrables sur l'ensemble des équipements et des services réseau fournis par le SRT.
- Obtenir graphiquement et en temps réel l'état de charge du réseau et des ses différents constituants.
- Obtenir une cartographie et un espace référentiel documentaire unique permettant d'accéder aux informations relatives aux équipements sous la responsabilité du SRT.

=> NagiosRT a pour objectif la migration des outils de supervision et de "cartographie documentaire" actuels (resp. WhatsUp et "Map" Vision/HTML) en un seul et même outil.

NagiosRT // Fonctionnalités

Surveillance : Surveillance temps réel / Remonter d'alertes / Gestion des dépendances / Test d'accessibilité de service web / Permet l'accès aux statistiques Netflow/sFlow

Cartographie : Création d'une carte dynamique du réseau / Navigation de façon arborescente / Insertion d'image (container, equipement) / Liens réseau visibles et présentant les informations de ces derniers / Ajout d'informations aux éléments de la carte / Une vue d'ensemble complémentaire sous forme arborescence

Métrologie : Produire des statistiques et historiques relatifs aux données collectées

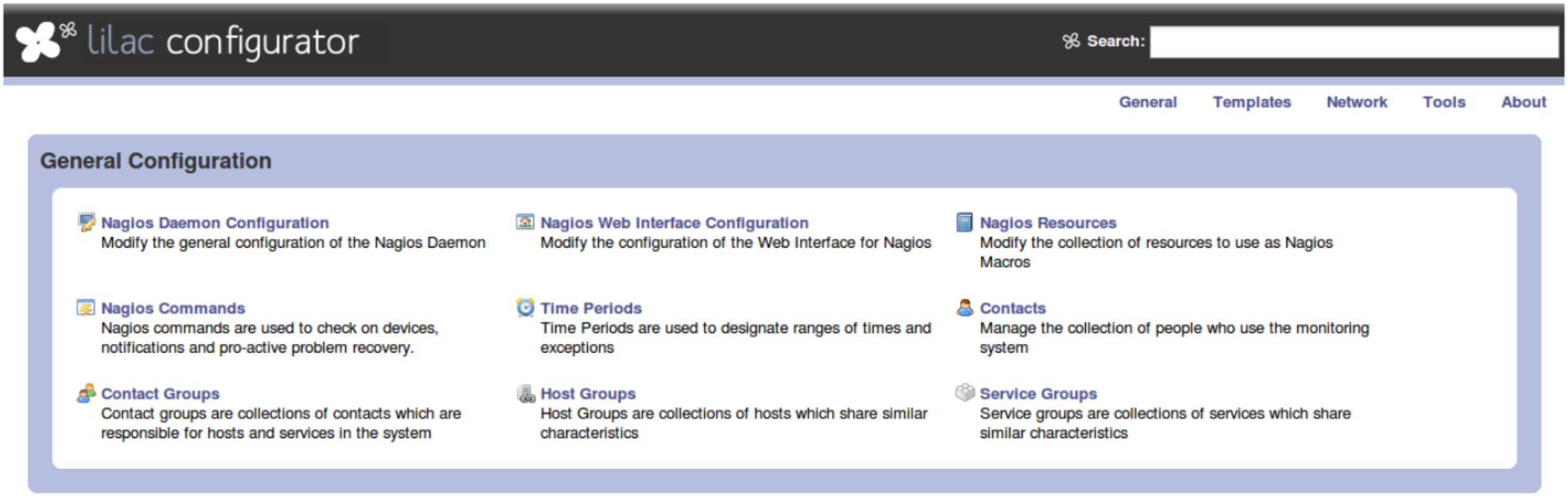
Rapport : Génération de rapports paramétrables selon les besoins (type de matériel, de données, par site, sur un intervalle de temps) et exportables (images, base de données, PDF)

NagiosRT // Logiciels utilisés

Nagios : surveillance machines/services
Nagvis : cartographie personnalisée des éléments Nagios
LILAC : configuration de Nagios depuis une interface web
Cacti : graphes (principalement réseau)
weathermap : cartographie des flux de bande passante
snmptt : gestion des traps SNMP
Smokeping : mesure des latences réseau
NFSEN : stats Netflow

NagiosRT : interface web unifiée de la solution (disponible sur la forge Evolix !)

NagiosRT // Focus sur LILAC



- Interface web pour configuration Nagios
- disponible sur la forge Evolix

Panorama du monitoring Open Source

- Définition
- Collecte des données
- Stockage des données
- Affichage des données
- Alertes
- Plateformes
- Outils propriétaires

Panorama // Définition

- Collecte des données
- Stockage des données
- Affichage des données
- Déclenchement d'alertes

Philosophie Unix (KISS) avec des éléments simples VS Plateformes

Panorama // Collecte des données

- SNMP
- IPMI
- plugins Nagios / NRPE
- collectd
- plugins Munin
- plugins Sensu

Panorama // Collecte // SNMP

- Simple Network Management Protocol
  - Protocole standard (RFC1157)

client/manager <--->>>> agent SNMP (snmpd) ---> exécution de scripts

- Intégré à de nombreux équipements

(switchs, routeurs, LB, SAN, imprimantes, etc.)

- Utilisation de MIB (description des valeurs accessibles en SNMP)

=> Pratique pour récolter des infos sur les équipements "boites noires"

=> Pratique pour récolter des infos réseau et système de base

=> Pas optimum pour récolter des infos système avancés

comme l'état d'une base de données (statut précis, timeout etc.)

Exemple :

```
# aptitude install snmpd
# aptitude install snmp
$ snmpwalk -v 1 -c public 127.0.0.1 iso.3.6.1.2.1.25.1.1.0
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (15606939) 1 day, 19:21:09.39
$ snmpwalk -v 1 -c public 127.0.0.1 .1
```

Panorama // Collecte // IPMI

Intelligent Platform Management Interface

=> Permet de récolter des informations sur la partie hardware d'un serveur (ventilateurs, température...)
=> Intégré à certaines marques de serveurs comme DELL

Exemple :

```
# aptitude install ipmitool
$ ipmitool -I lan -H <IP> -U root shell
ipmitool> sel list
   7 | Pre-Init Time-stamp   | Power Supply #0x65 | Power Supply AC lost | Asserted
   8 | Pre-Init Time-stamp   | Power Supply #0x74 | Redundancy Lost
   9 | 08/17/2007 | 15:46:15 | Power Supply #0x65 | Failure detected | Deasserted
   a | 08/17/2007 | 15:46:16 | Power Supply #0x65 | Power Supply AC lost | Deasserted
   b | 08/17/2007 | 15:46:16 | Power Supply #0x74 | Fully Redundant
   c | 08/17/2007 | 15:46:35 | Memory #0x53 | Correctable ECC | Asserted
   d | 08/17/2007 | 15:46:42 | Temperature #0x30 | Upper Critical going high
   e | 08/17/2007 | 15:46:46 | Temperature #0x30 | Upper Critical going high
   f | 08/17/2007 | 15:46:49 | Voltage #0x60 | Lower Critical going low
```

Panorama // Collecte // Plugins Nagios / NRPE

Plugin Nagios

=> Facilité d'écrire des plugins

=> Scripts shell/Perl/Python/C renvoyant :

- un statut : 0 (OK) 1 (WARNING) ou 2 (CRITICAL)

- un commentaire pouvant contenir des indications, valeurs, etc. (limité à 4 KB)

Exemple d'un plugin en shell :

```
if [ "$STATE" = "$STATE_OK" ]
 then
 echo "TEST OK"
 exit 0
 else
 echo "TEST FAIL"
 exit 2
 fi
```

NRPE

• passe par le réseau (TCP/5666 par défaut) pour récupérer des informations :

/usr/lib/nagios/plugins/check_nrpe -H <IP> -c check_load

OK - load average: 0.03, 0.10, 0.09|load1=0.030;15.000;30.000;0; load5=0.100;10.000;25.000;0; load15=0.090;5.000;20.000;0;

Cela lance simplement des scripts (check_*) sur la machine distante via NRPE.

Panorama // Collecte // collectd

Plugins de base en C.

=> Performance des plugins de base

=> Possibilité de nouveaux plugins dans différents langages...

Exemple :

```
./mycpuload.rb -h i-123456  #Terminate the script with Ctrl+c
PUTVAL i-123456/mycpuload/gauge-5_minute_load 1207188959:0.01
PUTVAL i-123456/mycpuload/gauge-5_minute_load 1207188979:0.00
PUTVAL i-123456/mycpuload/gauge-5_minute_load 1207188999:0.08
```

Panorama // Collecte // Plugins Munin

Scripts shell/Perl/Python/C renvoyant une ou plusieurs valeurs.
=> Facilité d'écrire des plugins

Exemple :

```
/etc/munin/plugins# MUNIN_LIBDIR=/usr/share/munin ./load
load.value 0.12
/etc/munin/plugins# MUNIN_LIBDIR=/usr/share/munin ./swap
swap_in.value 127663
swap_out.value 179246
/etc/munin/plugins# munin-run load
load.value 0.11
/etc/munin/plugins# munin-run swap
swap_in.value 127663
swap_out.value 179246
```

Panorama // Collecte // Plugins Sensu

Scripts en ruby, sortie semblable à Munin

Exemple :

```
./vmstat-metrics.rb
stats.swap.in   0   1328153991
stats.swap.out  0   1328153991
stats.memory.active 122160  1328153991
stats.memory.swap_used  8   1328153991
stats.memory.free   48556   1328153991
stats.memory.inactive   73704   1328153991
stats.cpu.waiting   1   1328153991
```

Panorama // Stockage des données

- Fichiers à plat
- Parlons un peu de syslog
- Le célèbre format RRD
- format whisper (Graphite)
- bases de données (SQL ou no-SQL)

Panorama // Stockage des données // RRD

Exemple :

```
rrdtool create temperature.rrd --step 300 \
  DS:temp:GAUGE:600:-273:5000 \
  RRA:AVERAGE:0.5:1:1200 \
  RRA:MIN:0.5:12:2400 \
  RRA:MAX:0.5:12:2400 \
  RRA:AVERAGE:0.5:12:2400
```

Optimisation RRD : rrdcached
(démon pour optimiser les I/O disque)

=> Avantages : optimisation, auto-archivage

Panorama // Stockage des données // whipser

Format semblable au RRD utilisé pour Graphite,
avec certains avantages :

- Gestion des updates irréguliers
(non lié à un step fixe comme RRD)
- Gestion des updates non ordonnés
(ajout de données du passé)

http://graphite.wikidot.com/whisper

Panorama // Affichage des données

- rrdtool
- Munin
- Graphite
- Front-end collectd

Nagios

- Nagvis
- Pnp4Nagios
- OpenPOM

Panorama // Affichage des données // Munin

- Création automatique des images via rrdtool
  - daily/weekly/monthly/yearly
- Nombreux plugins (disques, CPU, mémoire, réseau, charge, Apache, MySQL, etc.)
  - Fonctionne out-of-the-box !
- Gestion centralisée possible de plusieurs clients

Munin v2

- Zoom possible !
- AJAX

MUNIN **Overview :: munin-monitoring.org :: demo.munin-monitoring.org**

demo.munin-monitoring.org :: [1sec::network apache disk logins munin network network:services network:traffic processes system time]

Problems

Critical (0)
Warning (0)
Unknown (0)

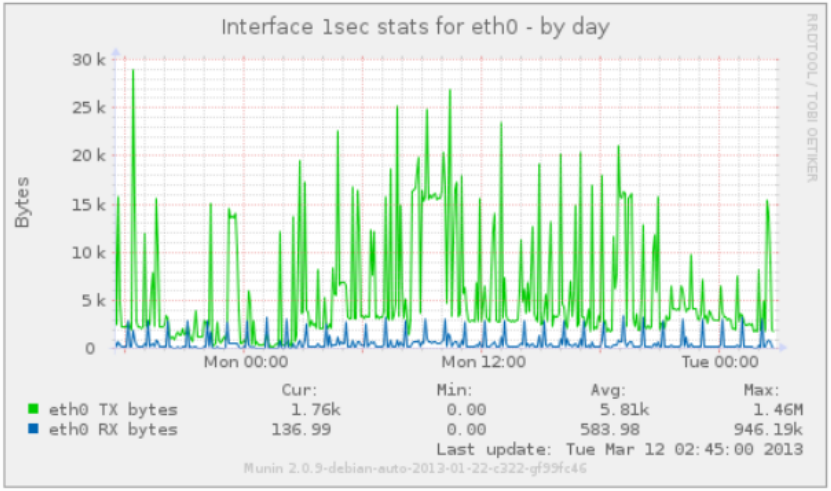
Groups

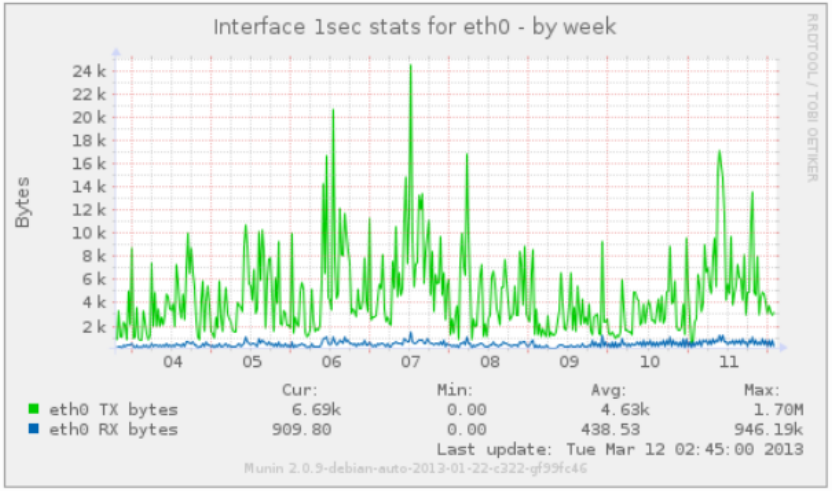
munin-monitoring.org

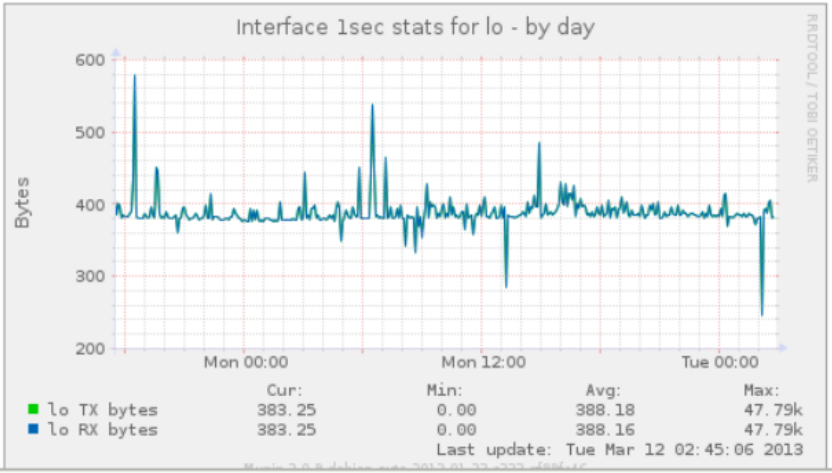
Categories

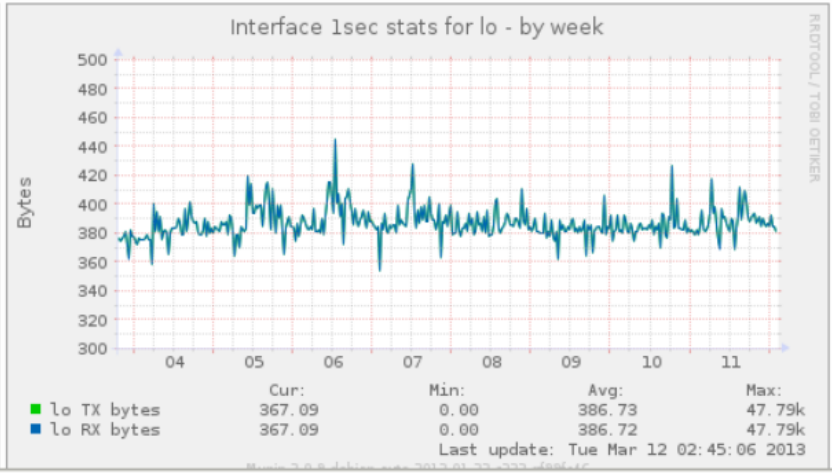
1sec::network [d w m y]
apache [d w m y]
disk [d w m y]
exim [d w m y]
gimbal [d w m y]
http [d w m y]
logins [d w m y]
munin [d w m y]
network [d w m y]
network:services [d w m y]
network:traffic [d w m y]
other [d w m y]
postgresql [d w m y]
processes [d w m y]
system [d w m y]
time [d w m y]
varnish [d w m y]

1sec::network

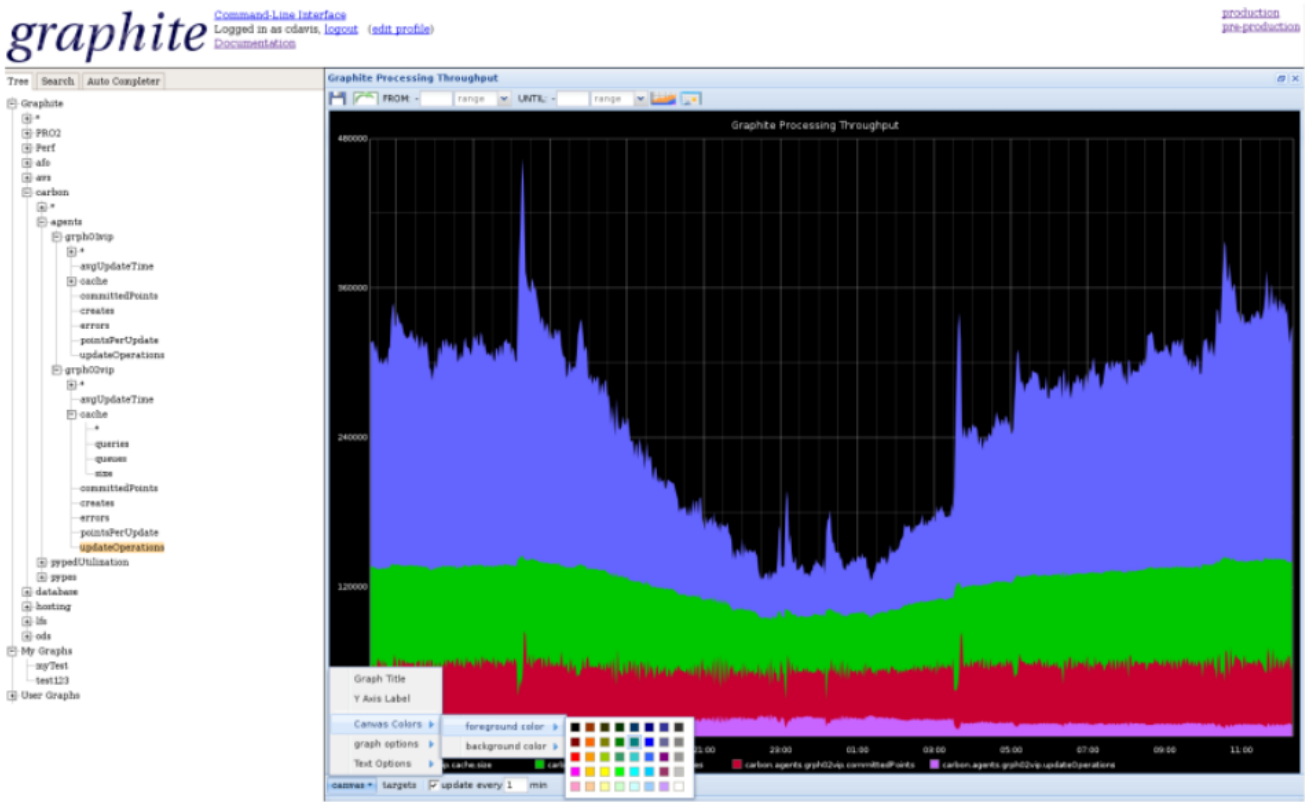






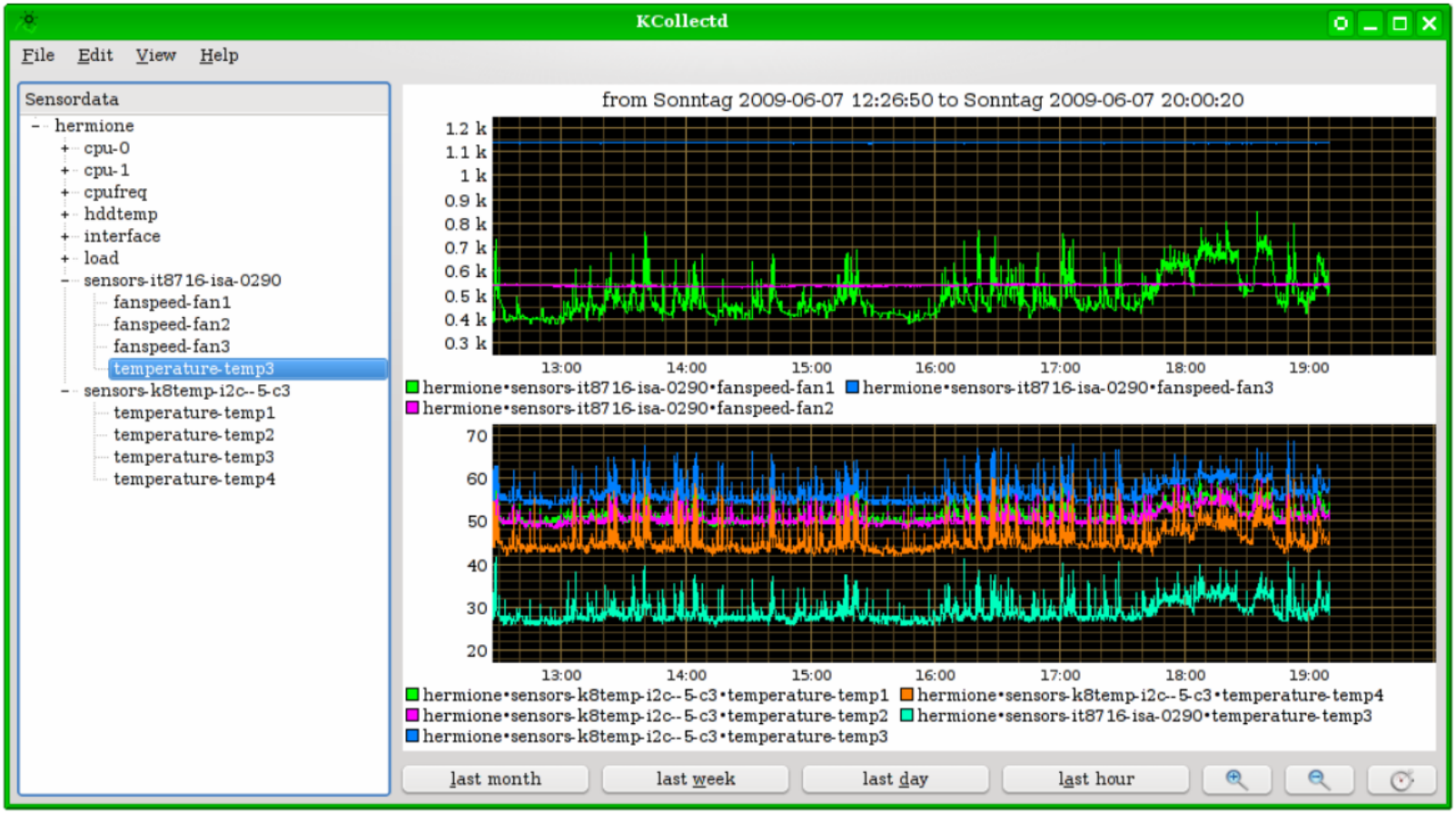


Panorama // Affichage des données // Graphite



- écrit en Python/Django
- Centralisation de milliers de métriques
- gère son propre format rrd-like (whisper)

Panorama // Affichage des données // Front-end collectd

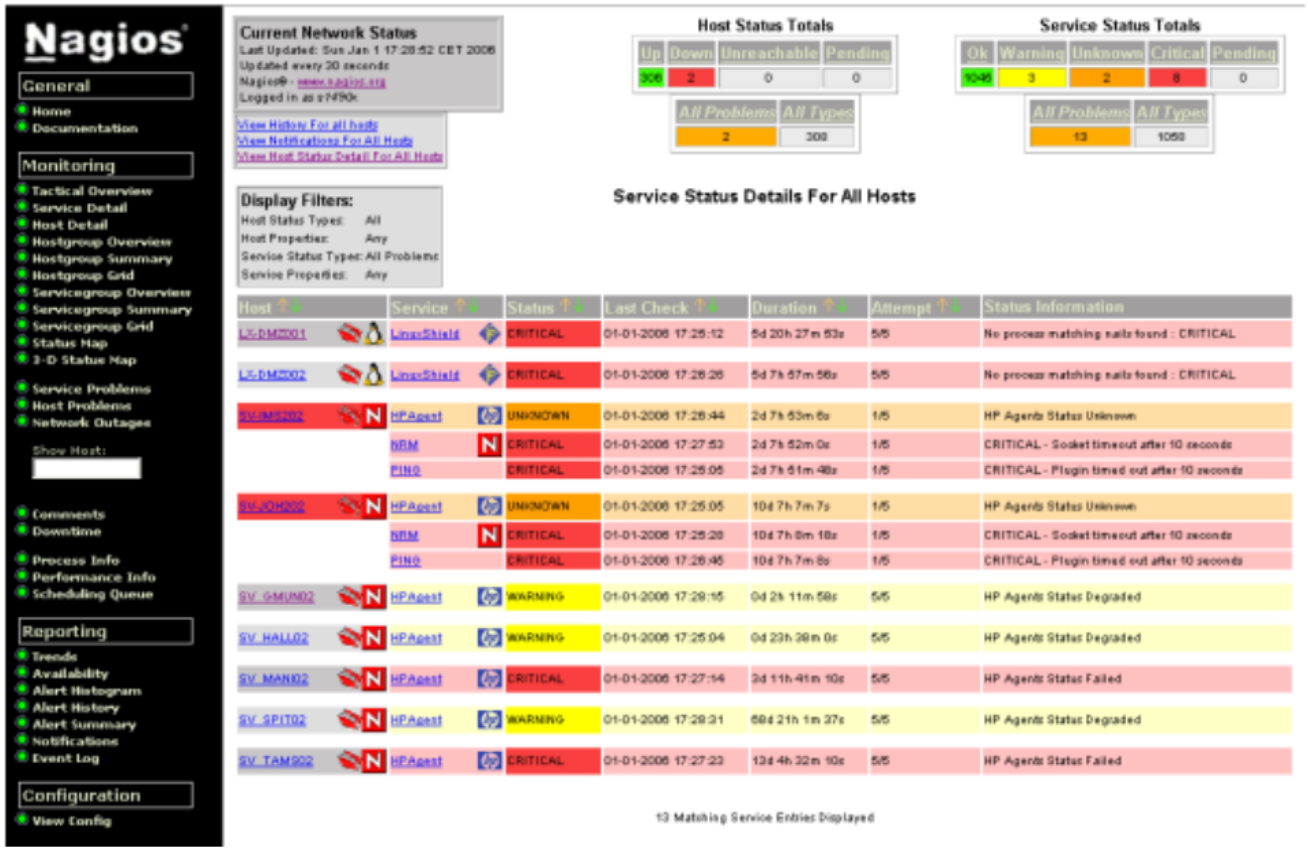


- Superposition des valeurs

Panorama // Alertes

- Nagios / Icingua / Shinken
- Munin
- Monit / God
- SNMP trap
- Sensu
- log2mail/logcheck
- Netdisco
- IDS (Snort, etc.)

Panorama // Alertes // Nagios/Icingua/Shinken



- Workflow très poussé de gestion des alertes

Panorama // Alertes // log2mail / logcheck

log2mail

Pour surveiller un fichier de log et recevoir des alertes par mail si un pattern connu apparaît.
Configuration via /etc/log2mail/config/default.

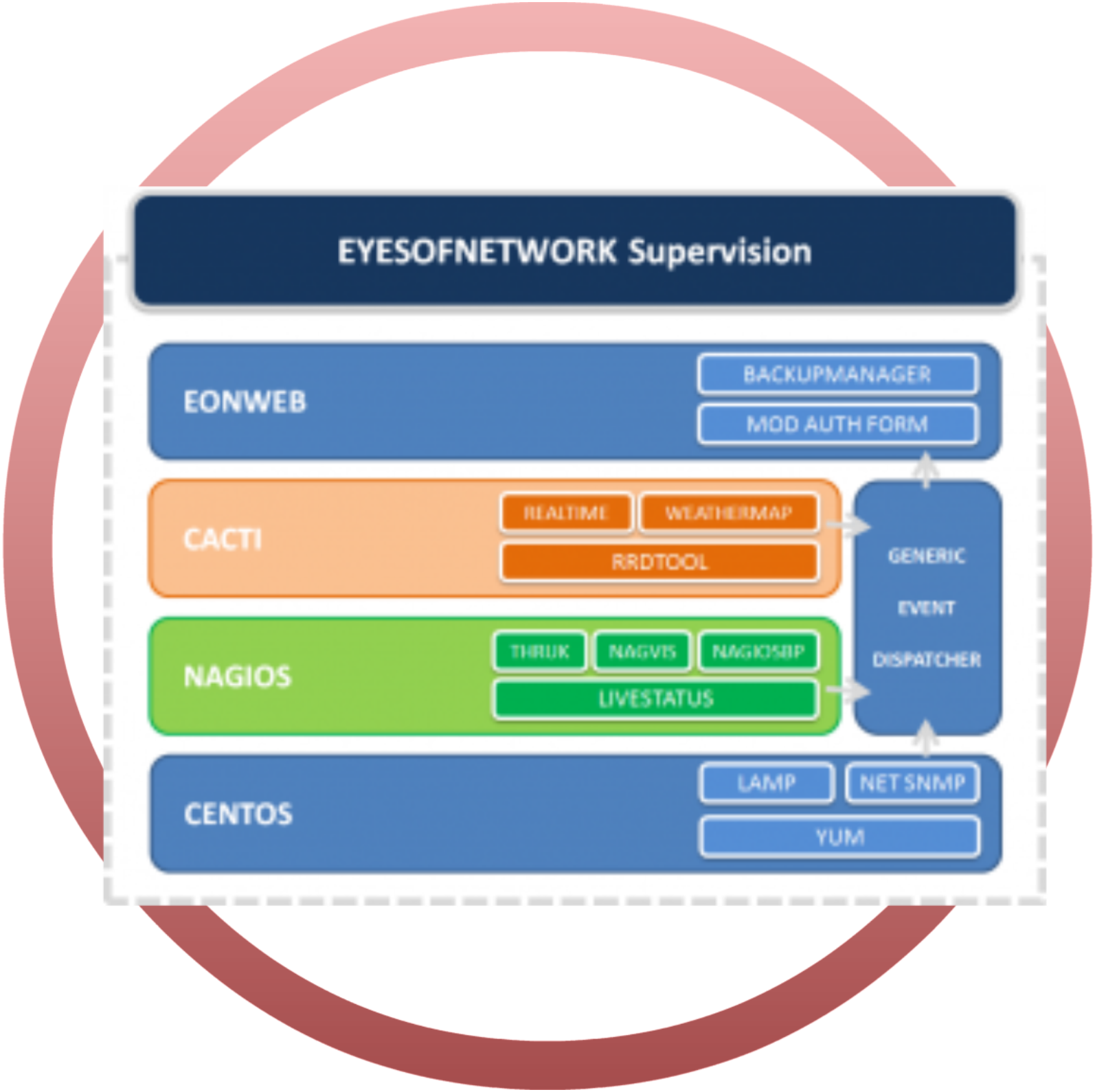
```
file = /var/log/mail.log
pattern = "fatal"
mailto = admin@example.com
template = /etc/log2mail/template.mail-fatal
```

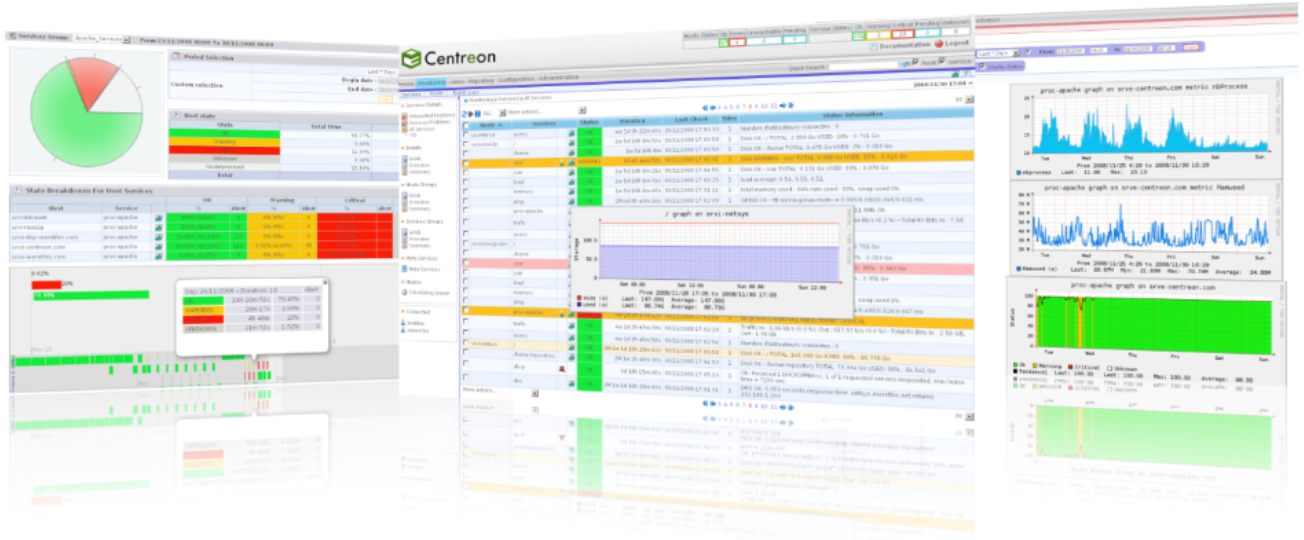
logcheck

Outil lancé toutes les heures via cron pour détecter les patterns inconnus dans des logs (syslog, mail.log, etc.)

Panorama // Usines à gaz^W^W^W Plateformes

- EON
- Centreon
- Zabbix
- OpenNMS
- NTOP
- Zenoss
- Ganglia
- Vigilo


EYESOFNETWORK Supervision
EONWEB
BACKUPMANAGER
MOD AUTH FORM
CACTI
REALTIME
WEATHERMAP
RRDTOOL
NAGIOS
THRUK
NAGVIS
NAGIOSBP
LIVESTATUS
GENERIC
EVENT
DISPATCHER
CENTOS
LAMP
NET SNMP
YUM



Zabbix

OpenNMS

Panorama // Usines à gaz^W^W^W Plateformes

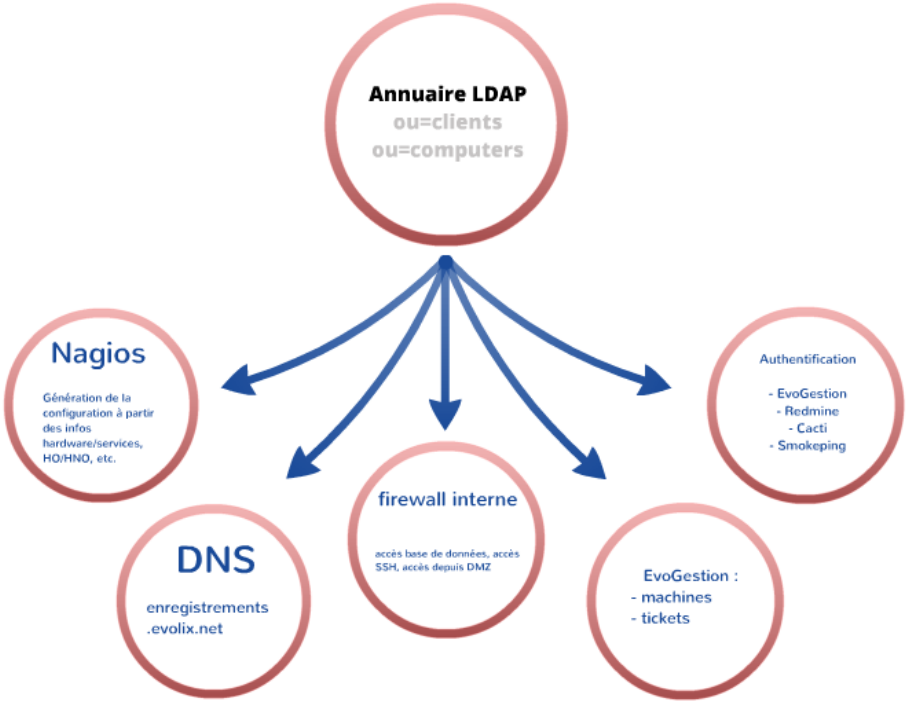
- EON
- Centreon
- Zabbix
- OpenNMS
- NTOP
- Zenoss
- Ganglia
- Vigilo

Outils propriétaires

En mode SaaS :
Newrelic (système et appli), MMS (MongoDB), Pingdom (HTTP), Simonbot (HTTP, client Evolix ;), Boundary etc.

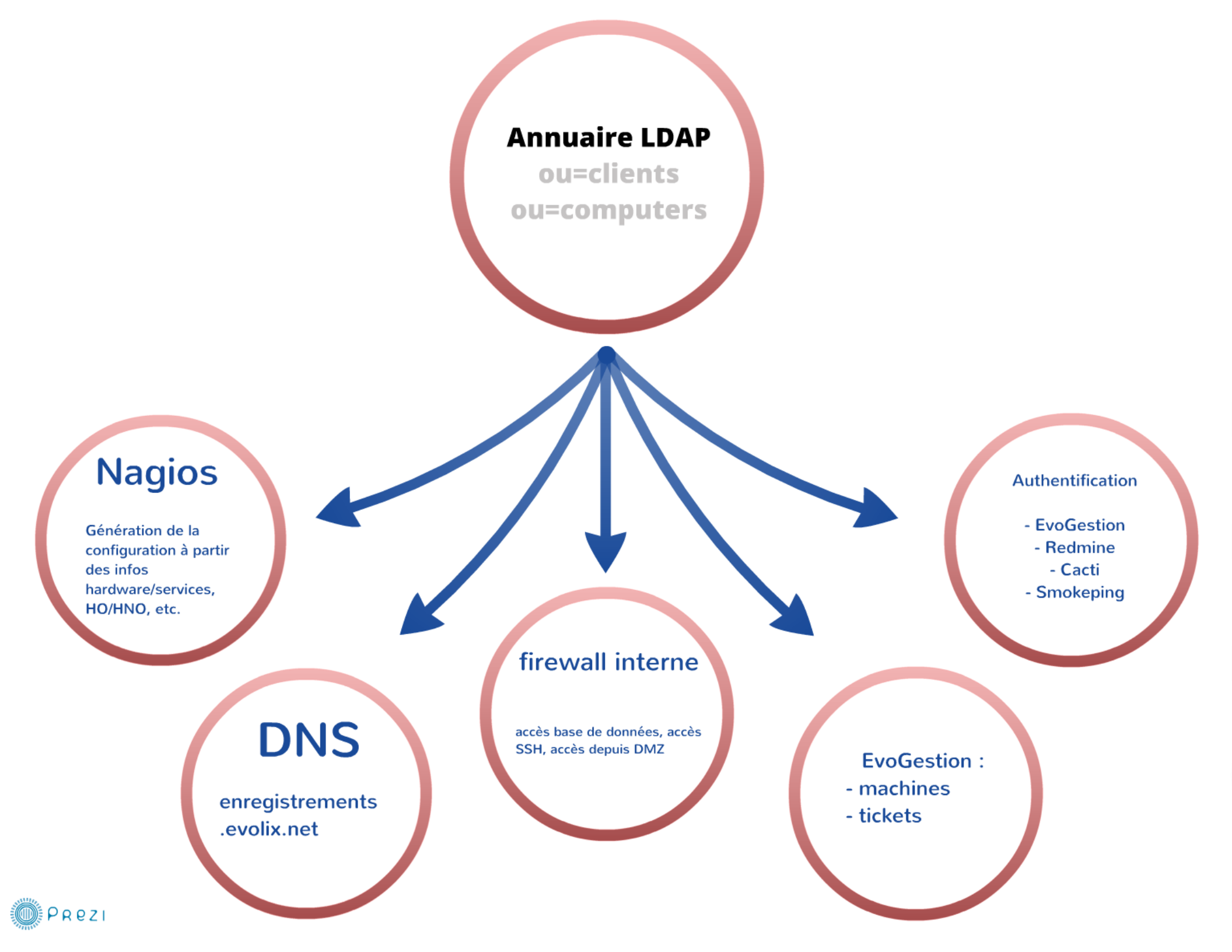
Groundwork, Hyperic, Pandora FMS, NetCrunch, BigBrother, IBM Tivoli etc.

Architecture du monitoring Evolix



- 2 machines Nagios
- NRPE + plugins
- Munin sur chaque machine
- mailgraph, awstats, etc.
- log2mail / logcheck
- Cacti / NFSEN
- Smokeping

Travaux en 2013 : Shinken, OpenNMS, NFSEN


Annuaire LDAP
ou=clients
ou=computers
Nagios
Génération de la configuration à partir des infos hardware/services, HO/HNO, etc.
Authentification
- EvoGestion
- Redmine
- Cacti
- Smokeping
DNS
enregistrements .evolix.net
firewall interne
accès base de données, accès SSH, accès depuis DMZ
EvoGestion :
- machines
- tickets

Nagios

Génération de la configuration à partir des infos hardware/services, HO/HNO, etc.

DNS

enregistrements
.evolix.net

firewall interne

accès base de données, accès SSH, accès depuis DMZ

EvoGestion :

- machines
- tickets

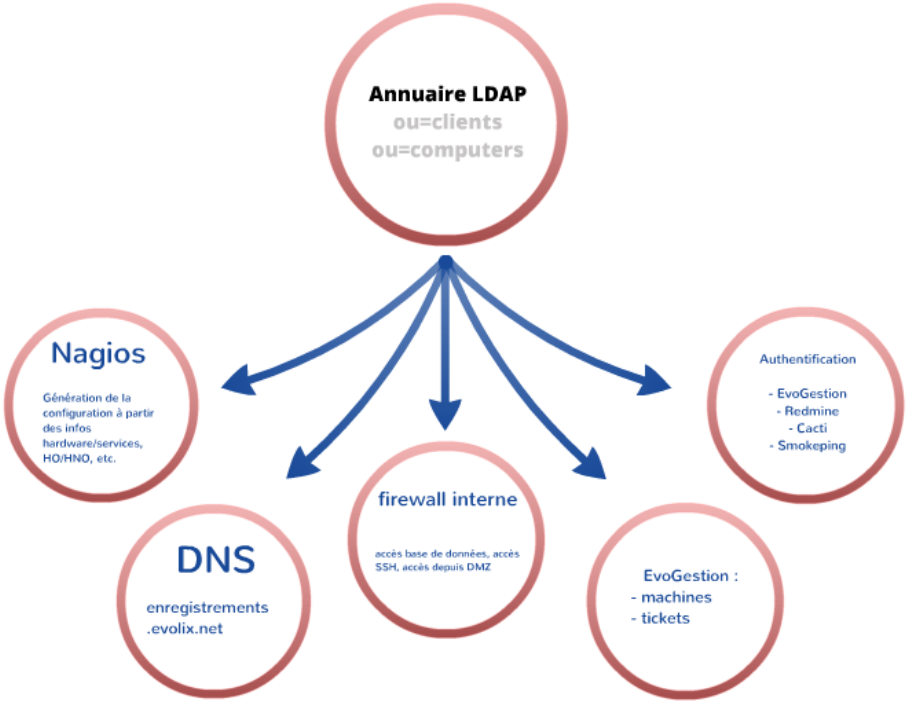
Authentification

- EvoGestion
- Redmine
- Cacti
- Smokeping

Introduction // Contexte Evolix

- Evolix infogère environ 350 serveurs pour une 50 clients, répartis dans différents datacenters et chez nos clients.
- Nous nous efforçons d'améliorer continuellement notre monitoring système & réseau.
- Nous mettons en place également du monitoring pour nos clients qui le souhaitent !

Architecture du monitoring Evolix



- 2 machines Nagios
- NRPE + plugins
- Munin sur chaque machine
- mailgraph, awstats, etc.
- log2mail / logcheck
- Cacti / NFSEN
- Smokeping

Travaux en 2013 : Shinken, OpenNMS, NFSEN