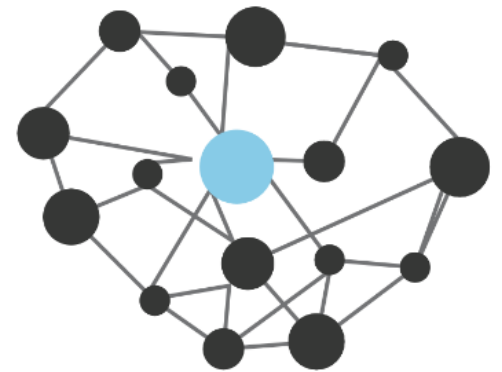


Quelques nouvelles d'Evolix

- Nouveau LOGO :)
- MP2013
- Hébergement V2
- Projets récents

evolix



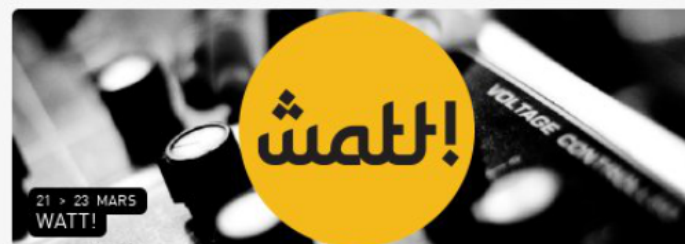
Hébergement et Infogérance Open Source

Quelques nouvelles d'Evolix

- Nouveau LOGO :)
- MP2013
- Hébergement V2
- Projets récents



MARSEILLE-PROVENCE 2013
CAPITALE
EUROPÉENNE
DE LA CULTURE



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 cœurs)
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))



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



Hosting très haute qualité

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



Infrastructure évolutive

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



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)



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 switches / 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

Compétences et missions

Présentation du CG13

Sommaire



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

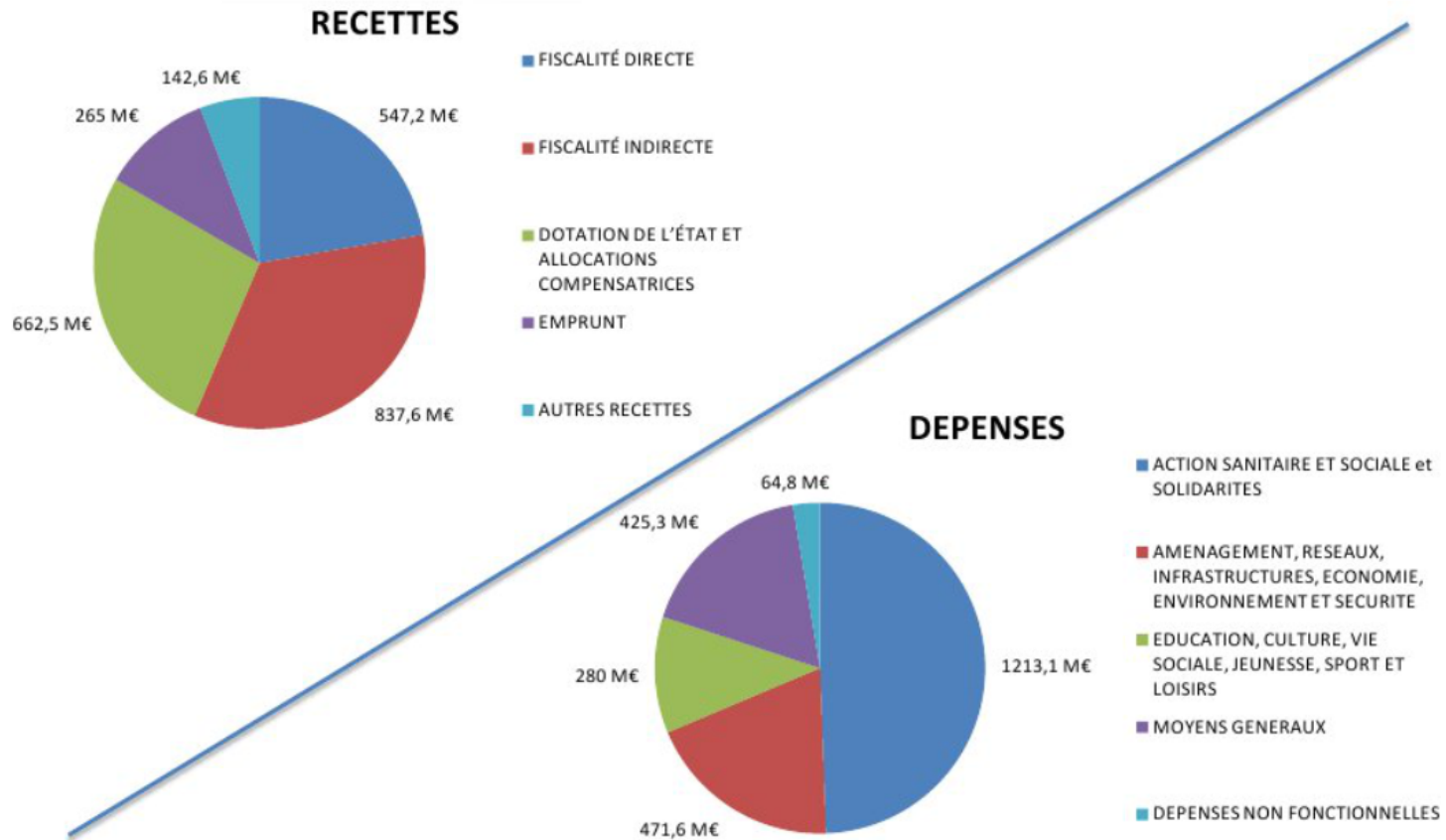
Santé

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

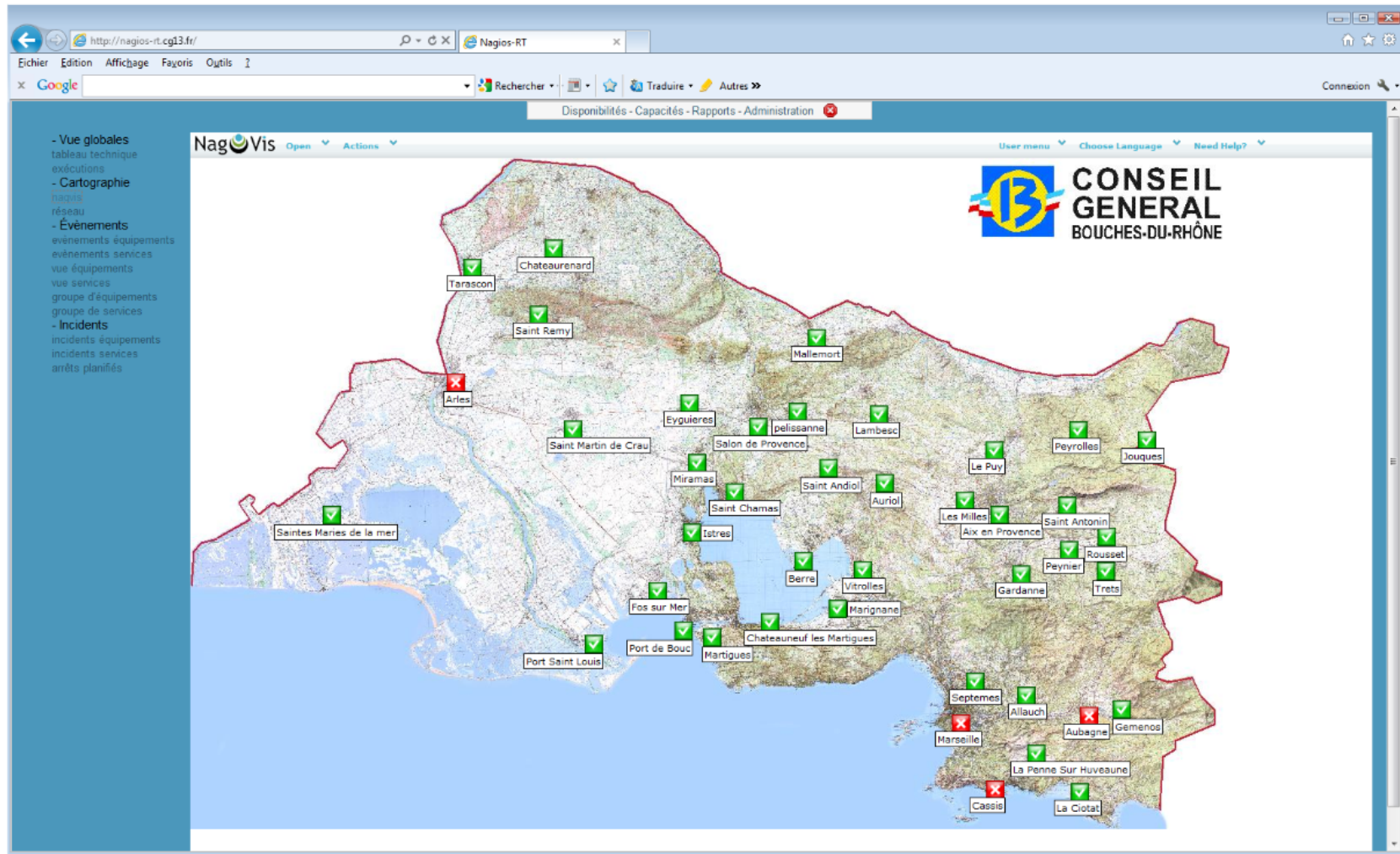
Debian privilégié mais contrainte package OS du CG13

Nos objectifs 2013

Redondance de la console

Développement de dashboards

Exemples (Nagvis): Map

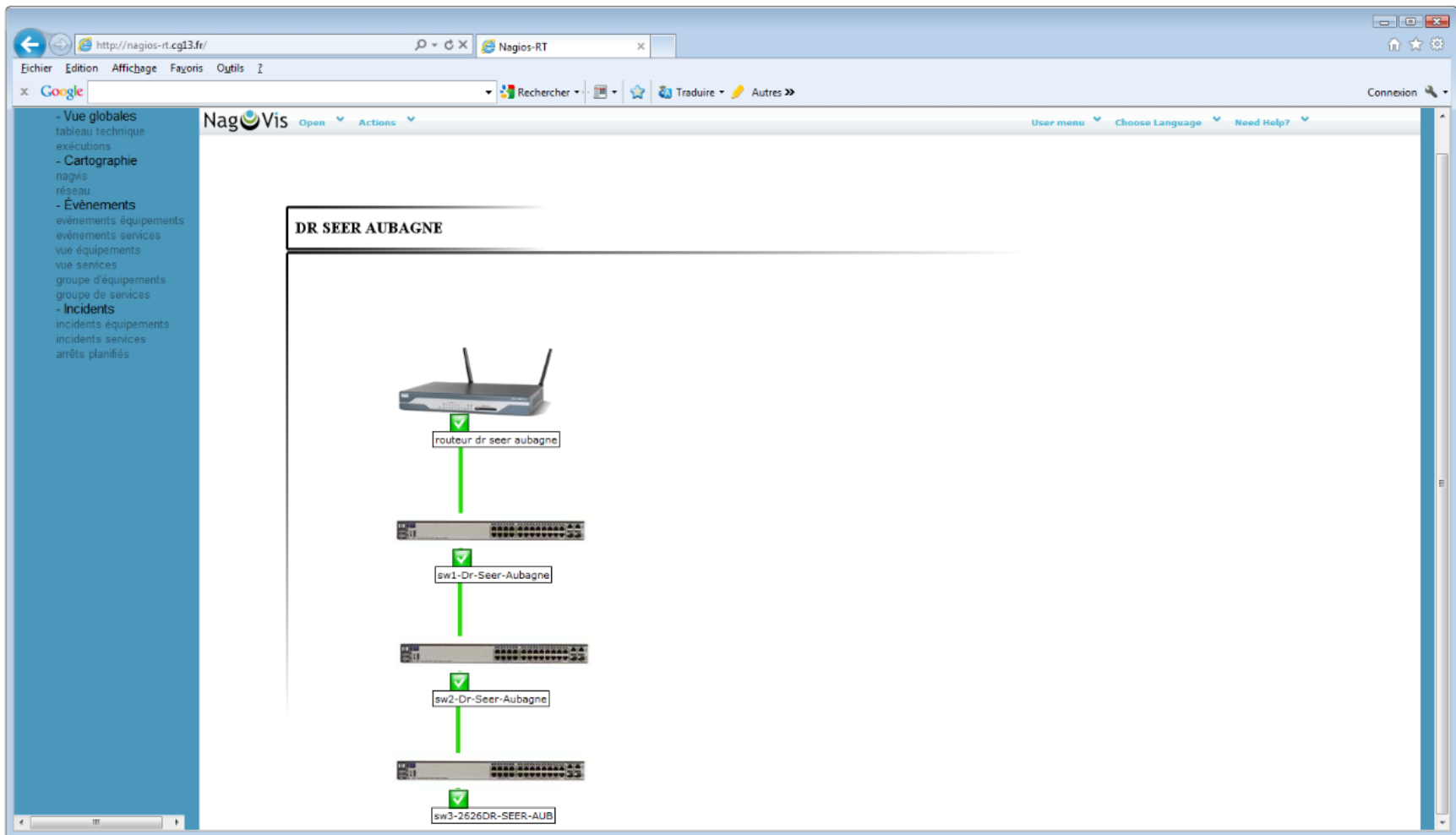


Direction des Systèmes d'Information et Télécommunication

12/03/201

3

Exemples (Nagvis): Topologie réseau



Exemples (Nagvis): Vue des services

Host	Service	Status	Time	Duration	Latency	Output
anker-banc.12box	TRAP	OK	11-03-2013 08:44:45	54d 23h 11m 14s	1/1	OK
anker-banc.cocosa	TRAP	OK	11-03-2013 08:44:46	54d 23h 11m 14s	1/1	OK
amber1	TRAP	OK	11-03-2013 08:44:46	167d 22h 42m 45s	1/1	OK
amber2	TRAP	OK	11-03-2013 08:44:46	167d 22h 46m 5s	1/1	OK
ankesc-rounas	TRAP	OK	11-03-2013 08:44:46	167d 22h 44m 25s	1/1	OK
anchohost	check_cpu	OK	11-03-2013 08:44:48	262d 22h 39m 6s	1/3	CPU OK - used: 2 idle: 98
	check_disk_appl1	OK	11-03-2013 08:44:48	262d 22h 55m 6s	1/3	DISK OK - free space: /APPL1_INA2 15136 MB (94%)
	check_disk_data1	OK	11-03-2013 08:44:49	262d 22h 39m 6s	1/3	DISK OK - free space: /DATA_INA2 33071 MB (91%)
	check_disk_slash	OK	11-03-2013 08:44:49	262d 22h 10m 16s	1/3	DISK OK - free space: / 5736 MB (72%)
	check_disk_usr	OK	11-03-2013 08:44:50	262d 22h 55m 6s	1/3	DISK OK - free space: /usr 13331 MB (83%)
	check_disk_var	OK	11-03-2013 08:44:50	262d 22h 55m 6s	1/3	DISK OK - free space: /var 3862 MB (65%)
	check_disk_work1	OK	11-03-2013 08:44:51	262d 22h 55m 6s	1/3	DISK OK - free space: /WORK_INA2 7508 MB (93%)
	check_disk_workroot	OK	11-03-2013 08:44:51	262d 22h 55m 6s	1/3	DISK OK - free space: /var/root 6723 MB (56%)
	check_mem	OK	11-03-2013 08:44:52	262d 22h 39m 6s	1/3	MEM OK: 38% Used Memory
	check_swap1	OK	11-03-2013 08:44:52	73d 12h 21m 31s	1/3	SWAP OK - 100% free (2048 MB out of 2048 MB)
	check_top_processes	OK	11-03-2013 08:44:53	16d 18h 46m 18s	1/3	6.5% command=mysql user=mysql pid=4350 cpulme=1-02:39:38
mds-berre	TRAP	OK	11-03-2013 08:44:53	54d 23h 11m 7s	1/1	OK
mean-1	TRAP	OK	11-03-2013 08:44:54	167d 22h 42m 44s	1/1	OK
mean-2	TRAP	OK	11-03-2013 08:44:54	167d 22h 46m 4s	1/1	OK
mean-3	TRAP	OK	11-03-2013 08:44:55	136d 17h 35m 3s	1/1	OK
mean-4	TRAP	OK	11-03-2013 08:44:55	136d 17h 37m 32s	1/1	OK
mess-1	TRAP	OK	11-03-2013 08:44:56	167d 22h 42m 43s	1/1	OK
mess-2	TRAP	OK	11-03-2013 08:44:56	167d 22h 46m 3s	1/1	OK
mess-3	TRAP	OK	11-03-2013 08:44:58	125d 0h 41m 15s	1/1	OK
mess-4	TRAP	OK	11-03-2013 08:44:58	125d 0h 43m 44s	1/1	OK
mebn-1	TRAP	OK	11-03-2013 08:44:58	167d 22h 42m 42s	1/1	OK
mebn-2	TRAP	OK	11-03-2013 08:44:58	167d 22h 46m 2s	1/1	OK
mebn-3	TRAP	OK	11-03-2013 08:44:58	124d 10h 0m 53s	1/1	OK
mebn-4	TRAP	OK	11-03-2013 08:44:59	54d 23h 11m 2s	1/1	OK
mrabeau-et-1-1	TRAP	OK	11-03-2013 08:45:00	54d 23h 11m 2s	1/1	OK
mrabeau-et-1-2	TRAP	OK	11-03-2013 08:45:00	54d 23h 11m 1s	1/1	OK
mrabeau-et-1-3	TRAP	OK	11-03-2013 08:45:01	54d 23h 11m 1s	1/1	OK
mrabeau-et-1-4	TRAP	OK	11-03-2013 08:45:01	167d 22h 42m 40s	1/1	OK
mrabeau-et11-1	TRAP	OK	11-03-2013 08:45:02	54d 23h 11m 0s	1/1	OK
mrabeau-et11-2	TRAP	OK	11-03-2013 08:45:02	54d 23h 11m 0s	1/1	OK
mrabeau-et11-1	TRAP	OK	11-03-2013 08:45:04	54d 23h 10m 59s	1/1	OK

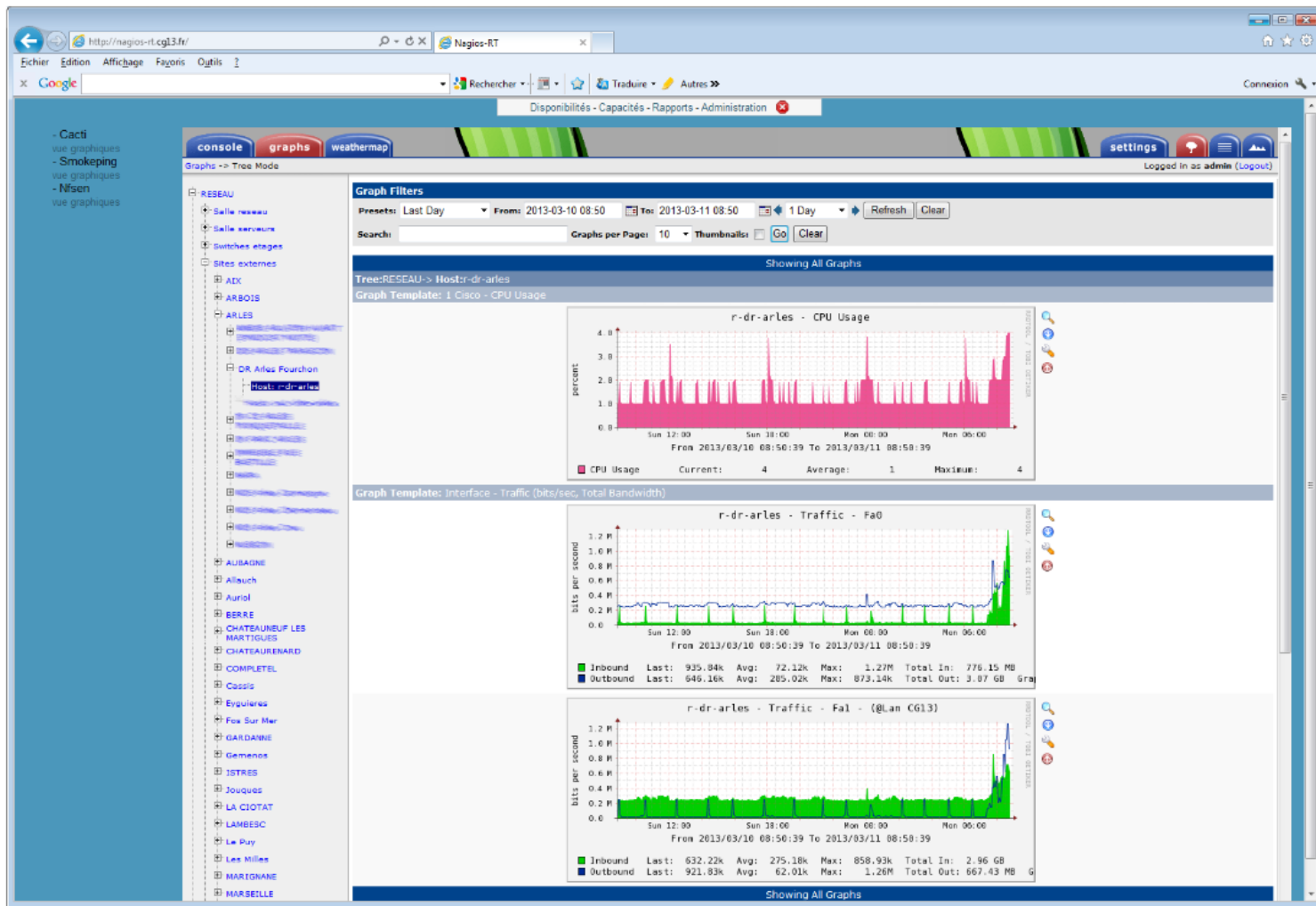
Exemples (Nagios) : Overview

The screenshot displays the Nagios RT web interface. The browser address bar shows 'http://nagios-rt.cg13.fr/'. The page title is 'Nagios-RT'. The navigation menu includes 'Disponibilités - Capacités - Rapports - Administration'. The main content area is titled 'Tactical Monitoring Overview' and includes the following sections:

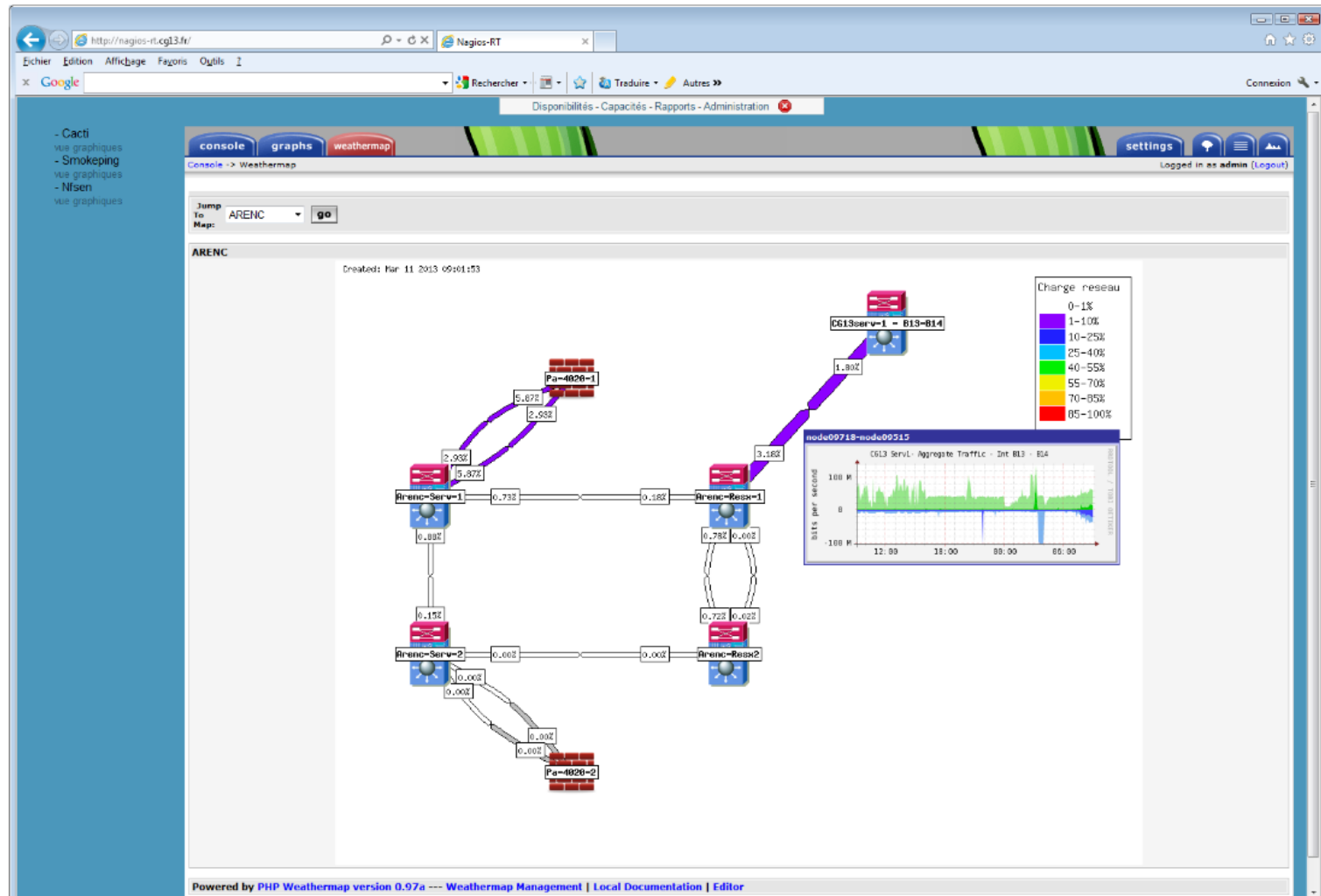
- Monitoring Performance:**
 - Service Check Execution Time: 0.00 / 1.23 / 0.025 sec
 - Service Check Latency: 0.00 / 0.28 / 0.135 sec
 - Host Check Execution Time: 0.01 / 10.01 / 0.288 sec
 - Host Check Latency: 0.00 / 7.18 / 0.285 sec
 - # Active Host / Service Checks: 753 / 606
 - # Passive Host / Service Checks: 45 / 0
- Network Health:**
 - Host Health: ██████████
 - Service Health: ██████████
- Network Outages:**
 - 7 Outages
 - 2 Clicking Outages
- Hosts:**
 - 18 Down, 2 Unreachable, 778 Up, 0 Pending
 - 18 Unhandled Problems, 2 Unhandled Problems, 4 Disabled
 - 3 Acknowledged
- Services:**
 - 0 Critical, 0 Warning, 0 Unknown, 606 Ok, 0 Pending
- Monitoring Features:**

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled 183 Services Disabled No Services Flapping All Hosts Enabled No Hosts Flapping	Enabled 4 Services Disabled 8 Hosts Disabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled 8 Hosts Disabled	Enabled 27 Services Disabled 1 Hosts Disabled

Exemples (Cacti) : Graphes



Exemples (weathermap): Charge liens



Exemples (Nagios): Rapport

The screenshot displays the Nagios RT web interface for a host named 'Dr-Ce-Copernic'. The main content area shows the 'Host Availability Report' for the period from 01-03-2013 00:00:00 to 11-03-2013 08:53:22. The report indicates that the host has been 'UP' for 100.000% of the time. Below this, there are two tables: 'Host State Breakdowns' and 'State Breakdowns For Host Services'. The 'Host State Breakdowns' table shows that the host is 'UP' for 100.000% of the time, with no 'DOWN' or 'UNREACHABLE' states. The 'State Breakdowns For Host Services' table shows that the service 'TRAP' is 'OK' for 100.000% of the time. At the bottom, there is a table of 'Host Log Entries' showing various events, including 'HOST UP (HARD)' and 'HOST UNREACHABLE (HARD)'. The interface also includes a sidebar with navigation links and a top navigation bar with options like 'Disponibilités', 'Capacités', 'Rapports', and 'Administration'.

Host Availability Report
 Last Updated: Mon Mar 11 08:53:22 CET 2013
 Nagios® Core™ 3.2.3 - www.nagios.org
 Logged in as nagiosadmin

Host 'Dr-Ce-Copernic'
 01-03-2013 00:00:00 to 11-03-2013 08:53:22
 Duration: 10d 8h 53m 22s

[Availability report completed in 0 min 0 sec]

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	10d 8h 53m 22s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	10d 8h 53m 22s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	10d 8h 53m 22s	100.000%	100.000%

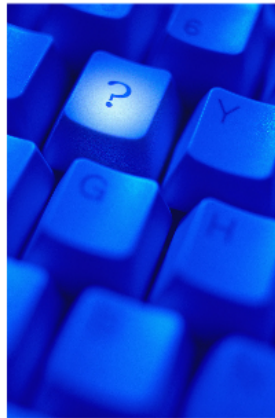
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
TRAP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Host Log Entries:
 [View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
25-02-2013 00:00:00	26-02-2013 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 12.84 ms
26-02-2013 00:00:00	27-02-2013 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 12.64 ms
27-02-2013 00:00:00	28-02-2013 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 12.88 ms
28-02-2013 00:00:00	28-02-2013 11:18:07	0d 11h 18m 7s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 12.85 ms
28-02-2013 11:18:07	28-02-2013 11:28:27	0d 0h 10m 20s	HOST UNREACHABLE (HARD)	CRITICAL - Time to live exceeded (172.24.75.241)
28-02-2013 11:28:27	01-03-2013 00:00:00	0d 12h 31m 33s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 12.33 ms
01-03-2013 00:00:00	02-03-2013 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 12.72 ms
02-03-2013 00:00:00	03-03-2013 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 13.98 ms
03-03-2013 00:00:00	04-03-2013 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 13.29 ms

Questions



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, équipement) / 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


 lilac configurator

🔍 Search:


[General](#) [Templates](#) [Network](#) [Tools](#) [About](#)


General Configuration


 **Nagios Daemon Configuration**
Modify the general configuration of the Nagios Daemon


 **Nagios Web Interface Configuration**
Modify the configuration of the Web Interface for Nagios


 **Nagios Resources**
Modify the collection of resources to use as Nagios Macros


 **Nagios Commands**
Nagios commands are used to check on devices, notifications and pro-active problem recovery.

 **Time Periods**
Time Periods are used to designate ranges of times and exceptions

 **Contacts**
Manage the collection of people who use the monitoring system

 **Contact Groups**
Contact groups are collections of contacts which are responsible for hosts and services in the system

 **Host Groups**
Host Groups are collections of hosts which share similar characteristics

 **Service Groups**
Service groups are collections of services which share similar characteristics

- 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 :

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

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



Problems

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

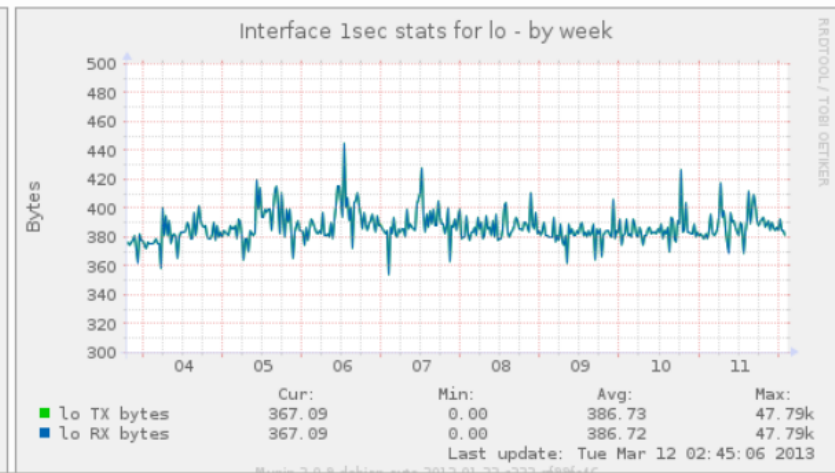
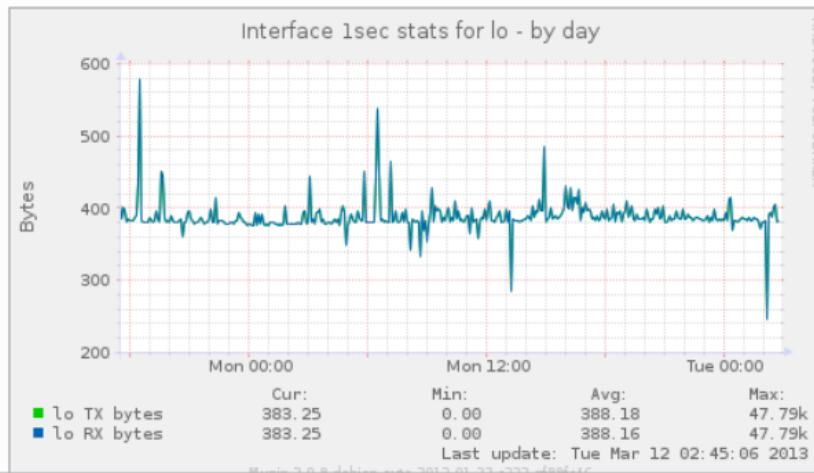
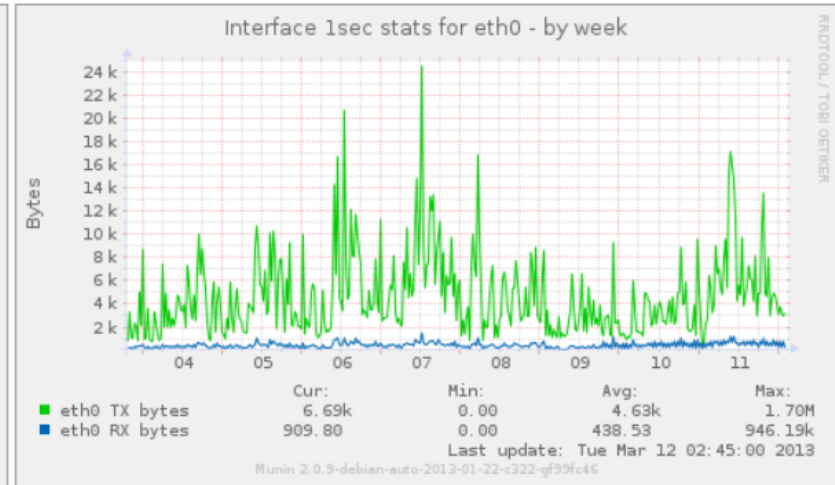
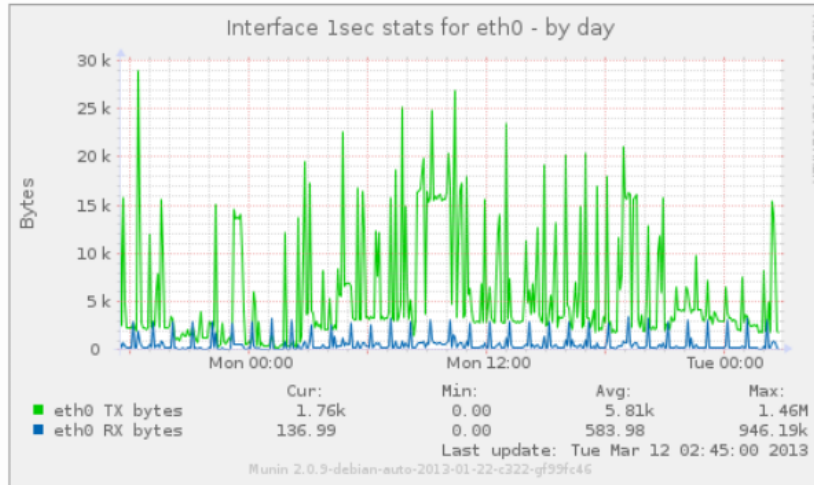
Groups

munin-monitoring.org

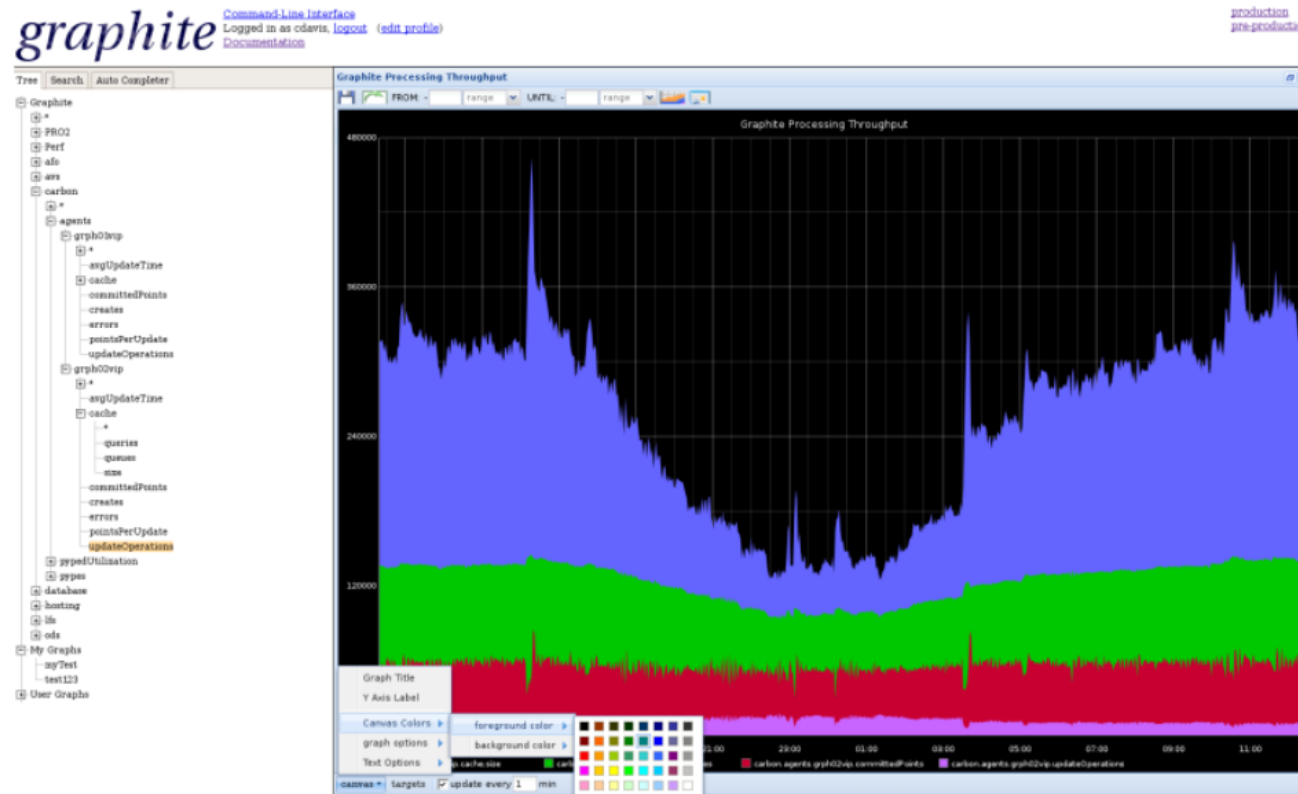
Categories

- 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

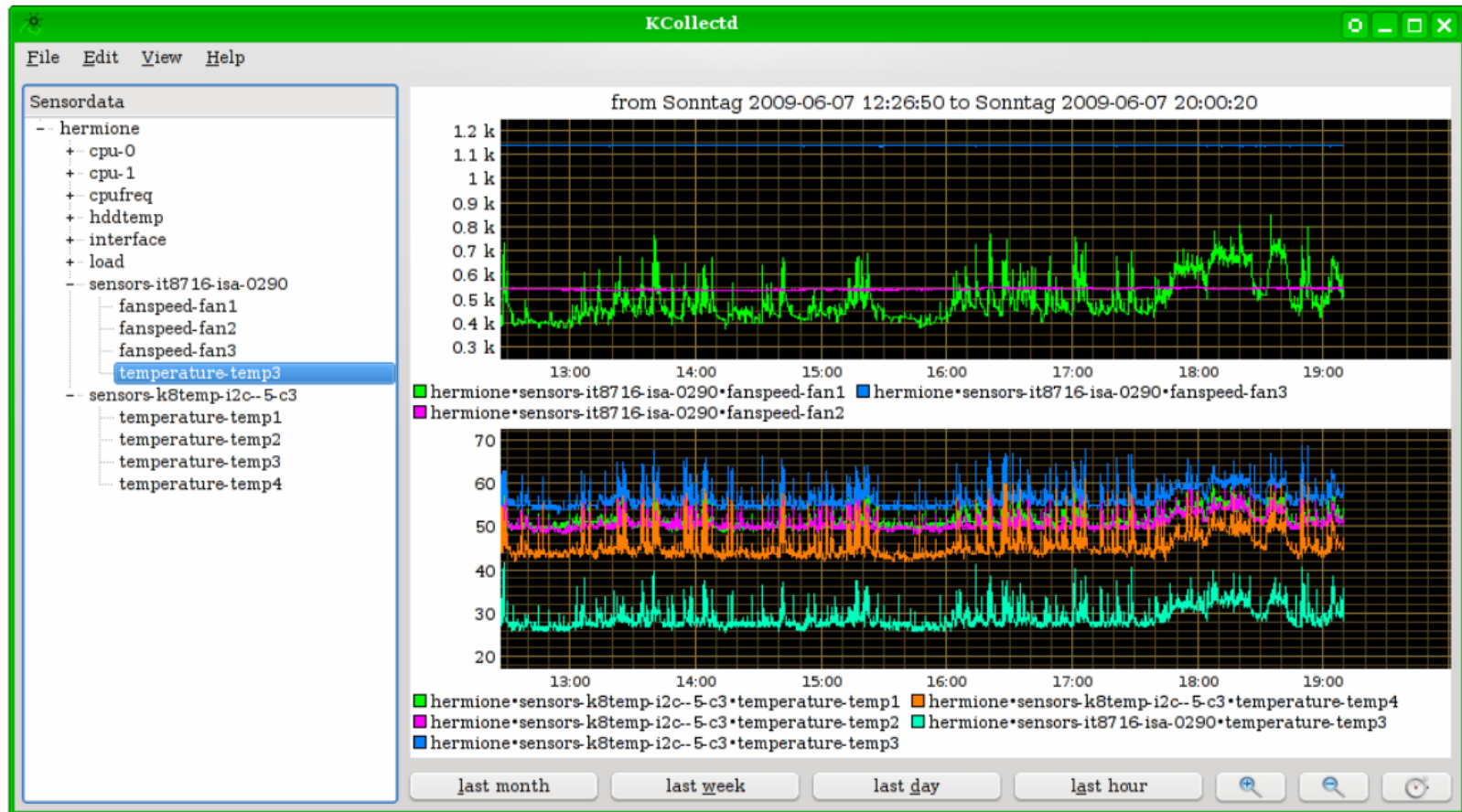


Panorama // Affichage des données // Graphite



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

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

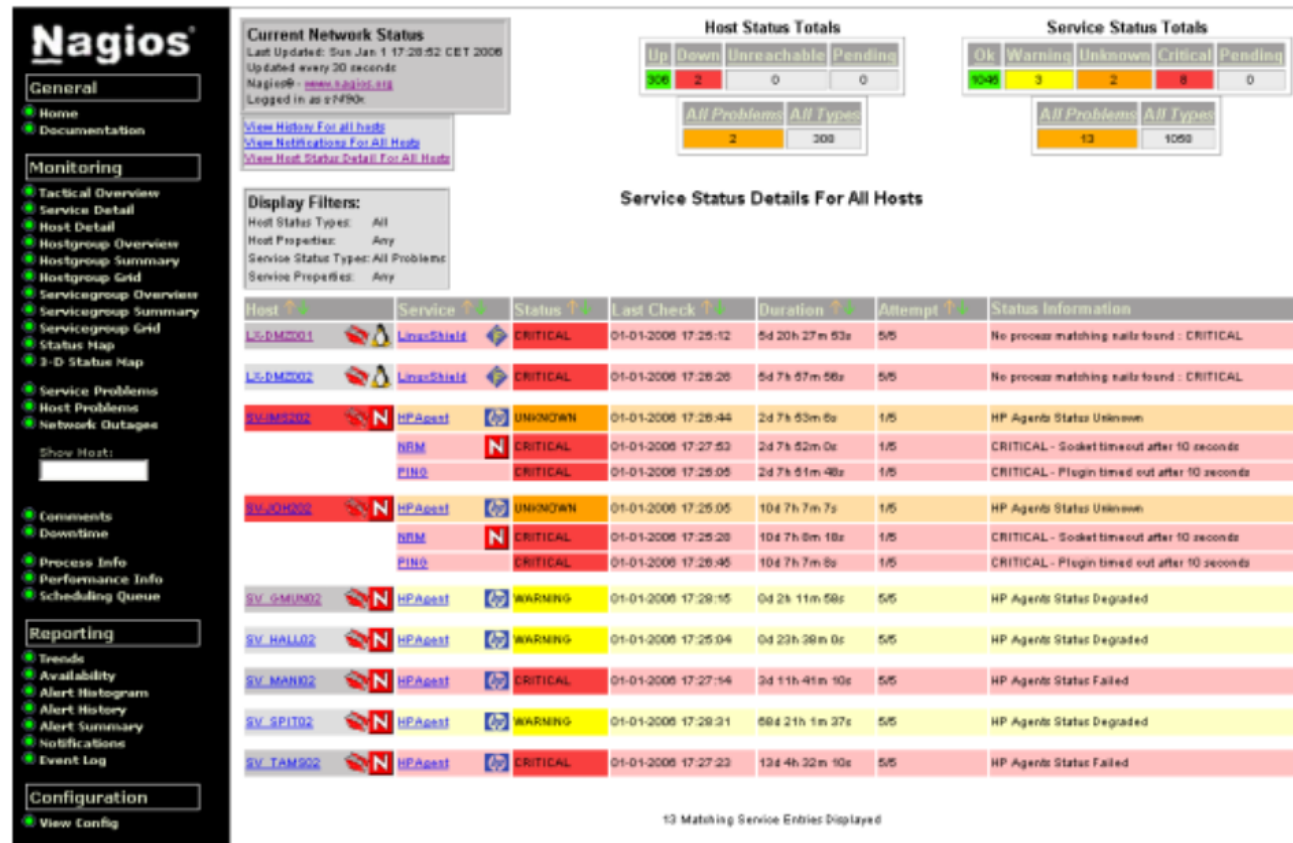


- Superposition des valeurs

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

THRIUK

NAGVIS

NAGIOSIP

LIVESTATUS

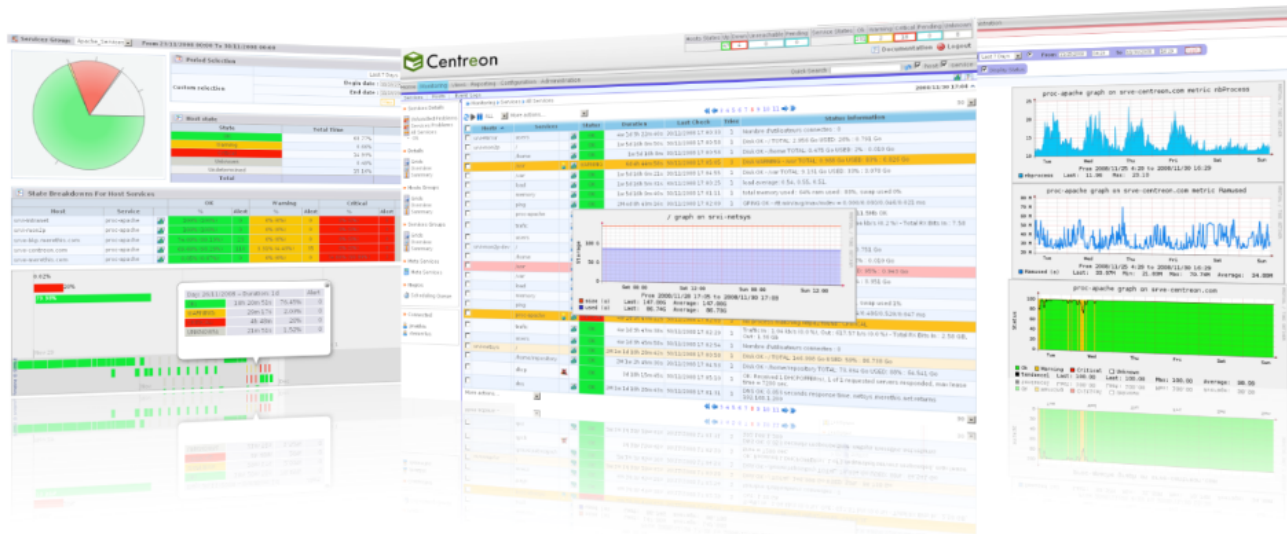
GENERIC
EVENT
DISPATCHER

CENTOS

LAMP

NET SNMP

YUM



Zabbix

The screenshot displays the Zabbix website interface. At the top left is the ZABBIX logo with the tagline 'The Enterprise-class Monitoring Solution for Everyone'. To the right are language options: Español, Latviski, and Русский, along with a 'Customer Login' link. A navigation bar contains links for Home, Product, Services, Training, Partners, Download, Community, and About Us. On the left side, a 'Product' menu lists: Product Overview (selected), What's New, Features, Screenshots, System Requirements, Documentation, Download, License, and News. The main content area is titled 'What is Zabbix' and contains a paragraph describing Zabbix as an open-source monitoring solution, followed by a bulleted list of features.

ZABBIX The Enterprise-class Monitoring Solution for Everyone

Español Latviski Русский Customer Login ▶

Home Product Services Training Partners Download Community About Us

Product

- Product Overview
- What's New
- Features
- Screenshots
- System Requirements
- Documentation
- Download
- License
- News

What is Zabbix

Zabbix is the ultimate open source availability and performance monitoring solution. Zabbix offers advanced monitoring, alerting, and visualization features today which are missing in other monitoring systems, even some of the best commercial ones. Below is a short list of features available in Zabbix:

- auto-discovery of servers and network devices
- low-level discovery
- distributed monitoring with centralized web administration
- support for both polling and trapping mechanisms
- server software for Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X
- native high performance agents (client software for Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista)
- agent-less monitoring
- secure user authentication
- flexible user permissions
- web-based interface

OpenNMS

.COM | ENG Stay Connected
New OpenNMS

openNMS Wiki | Live Demo | Events | News | Contact Us

Enterprise Support: (877) ONMS-911

Home About OpenNMS Get OpenNMS Get Support Get Involved Get Stuff

openNMS **OUCE 2013**
User Conference Europe
March 12-15 | Fulda | Germany



World's first open source, enterprise grade network management application platform

[Download Now](#)

[Get Support](#) [Get Involved](#)

See a Live Demo

OpenNMS provides ...

- Automated and Directed Discovery and Provisioning
- Event and Notification Management
- Service Assurance
- Performance Measurement

[Learn More](#)

Get the Network to Work® with OpenNMS!

OpenNMS is the world's first enterprise grade network management application platform developed under the open source model.

Well, what does that mean?

World's First: The OpenNMS Project was started in July of 1999 and registered an Sourced-orig in March of 2000. It has years of experience on the alternatives.

Enterprise Grade: It was designed from "day one" to manage tens of thousands to ultimately unlimited devices with a single instance. It offers the power, scalability and flexibility that enterprises and carriers demand.

Application Platform: While OpenNMS is useful "out of the box", it is designed to be highly customizable to create a unique and integrated management solution.

Get OpenNMS

[Download Now](#)

Get Support

[Learn More](#)

Get Involved

[Learn How](#)

Stay Connected

Get the latest on OpenNMS News and Events!

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

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

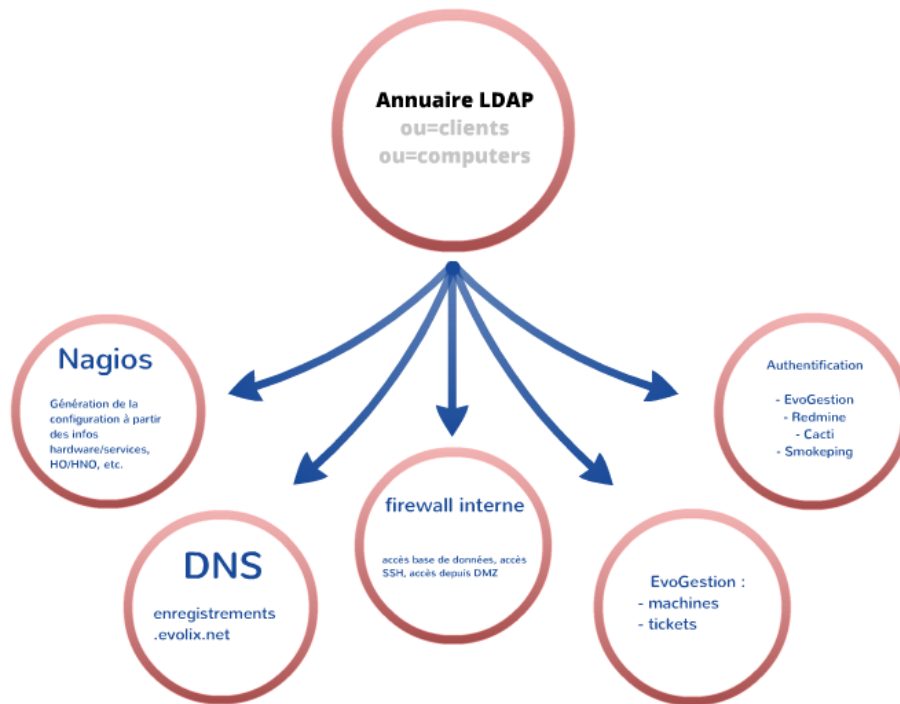
Outils propriétaires

En mode SaaS :

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

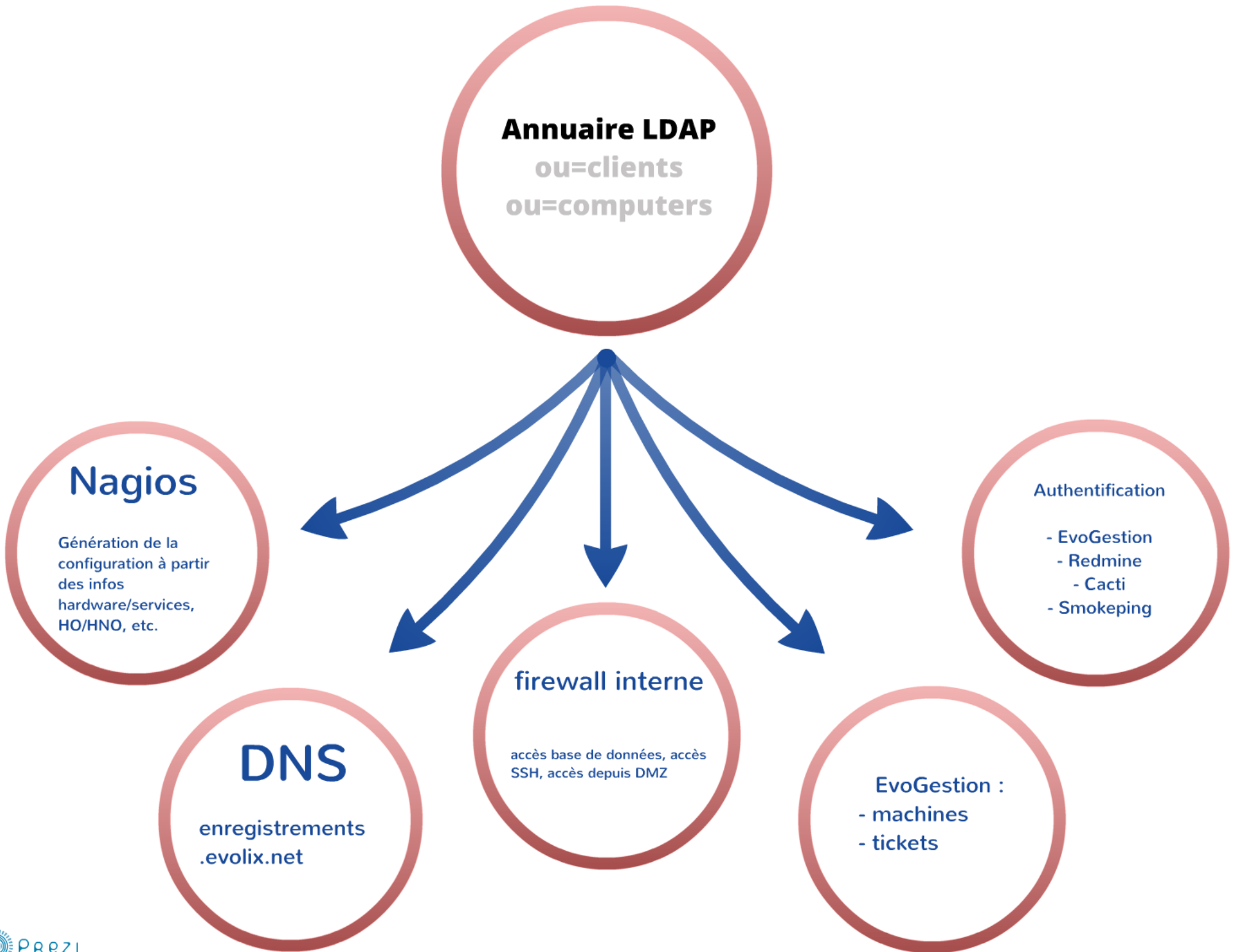
Groundwork, Hyperic, Pandora FMS, NetCrunch, BigBrother, IBM Tivoli etc.

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



Nagios

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

DNS

enregistremnts
.evolix.net

firewall interne

accès base de données, accès
SSH, accès depuis DMZ

- 
- EvoGestion :**
- machines**
 - tickets**

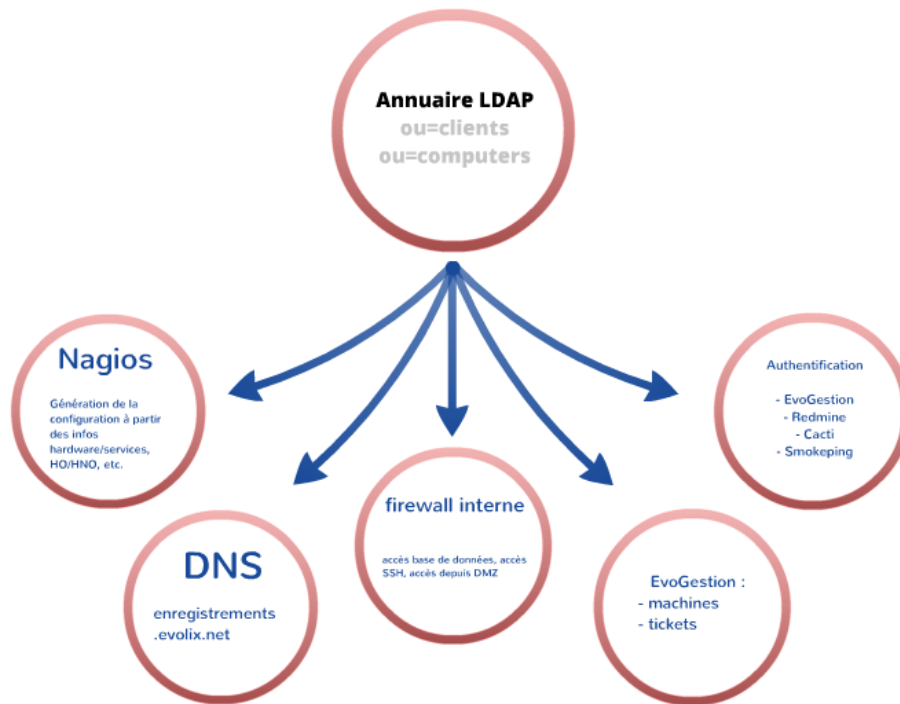
Authentication

- 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

