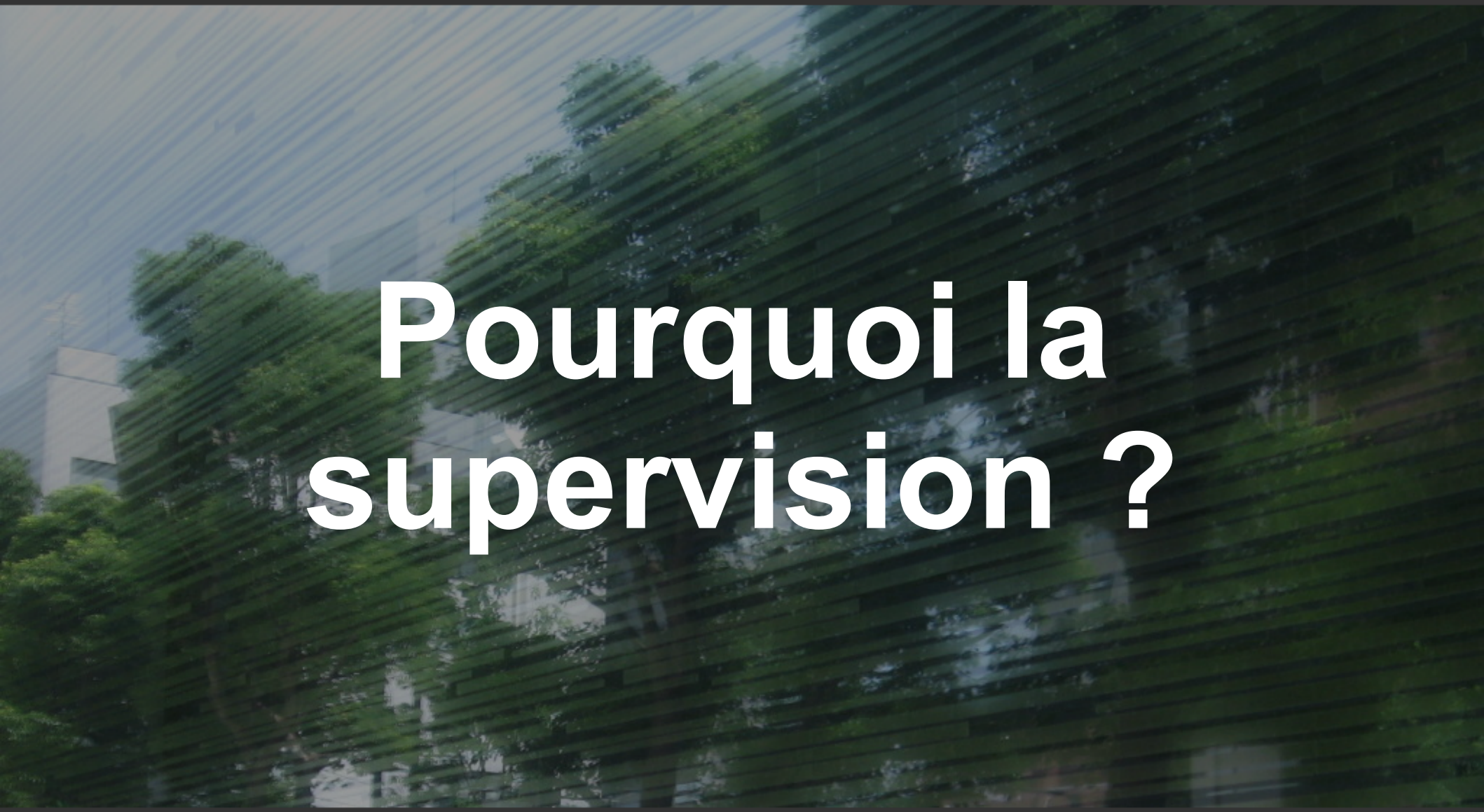
Présentation de Nagios

La supervision, Nagios et son écosystème.

Jérémy MATHEVET



Pourquoi la supervision ?

C'est très simple.

Pourquoi la supervision ?

Pourquoi la supervision ?

Pourquoi la supervision ?

"Quand il y a un ça va... C'est quand il y en a beaucoup qu'il y a des problèmes !"

La supervision consiste à surveiller le fonctionnement d’un système.

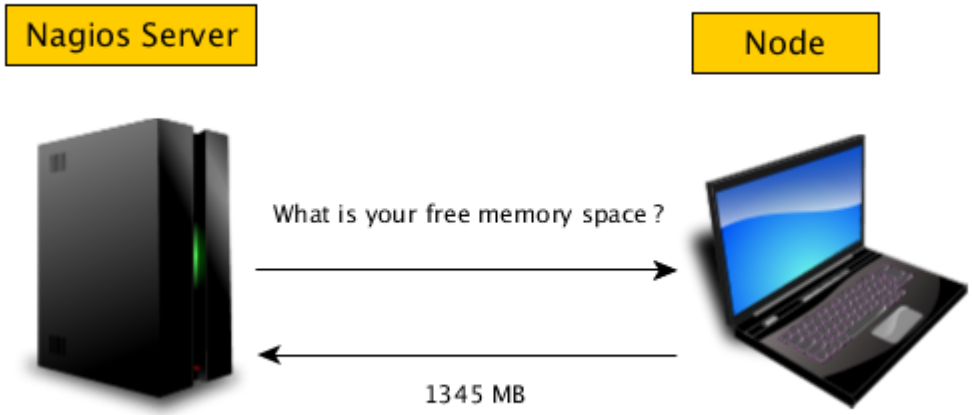
Elle permet de surveiller, détecter, et si besoin est, signaler un fonctionnement normal ou
anormal du système.

Ce qu'il est possible de superviser :

- La charge système, la mémoire, la température
- Les processus, les services
- La connectivité réseau, le traffic
- À peu près tout, grâce aux scripts...

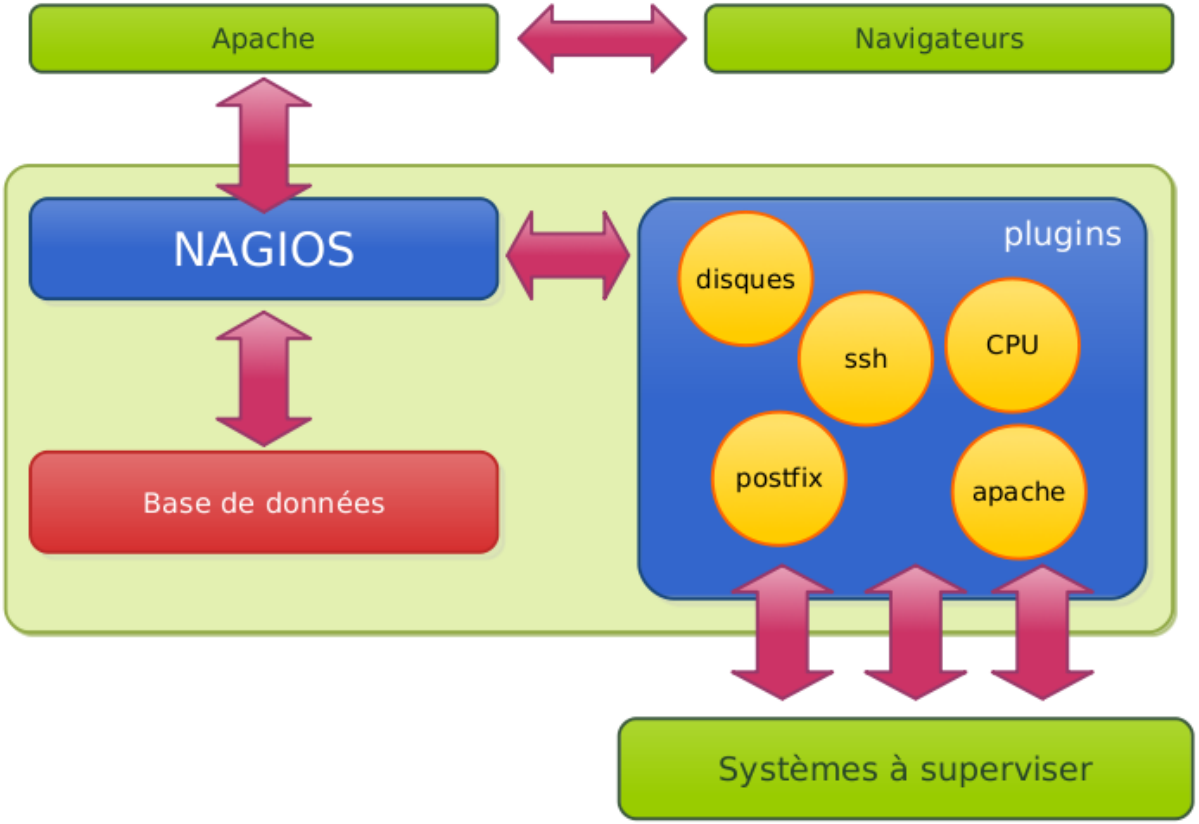
Fonctionnement

Architecture client/serveur



- Nagios est composé de 3 parties :
  - Un ordonnanceur
  - Des plugins
  - Une interface web

Fonctionnement



Pour récupérer les informations, utilisation de plugins. Il existe différentes méthodes d'interrogation :

- Active check
  - Protocole SNMP
  - NRPE
- Passive check
  - NSCA

Quel que soit leur type, les plugins doivent retourner un code et une chaine.

Valeur	Statut
0	OK
1	Warning
2	Critical
3	Unknown

- Active check

  C'est le serveur Nagios qui initie la demande d'information.

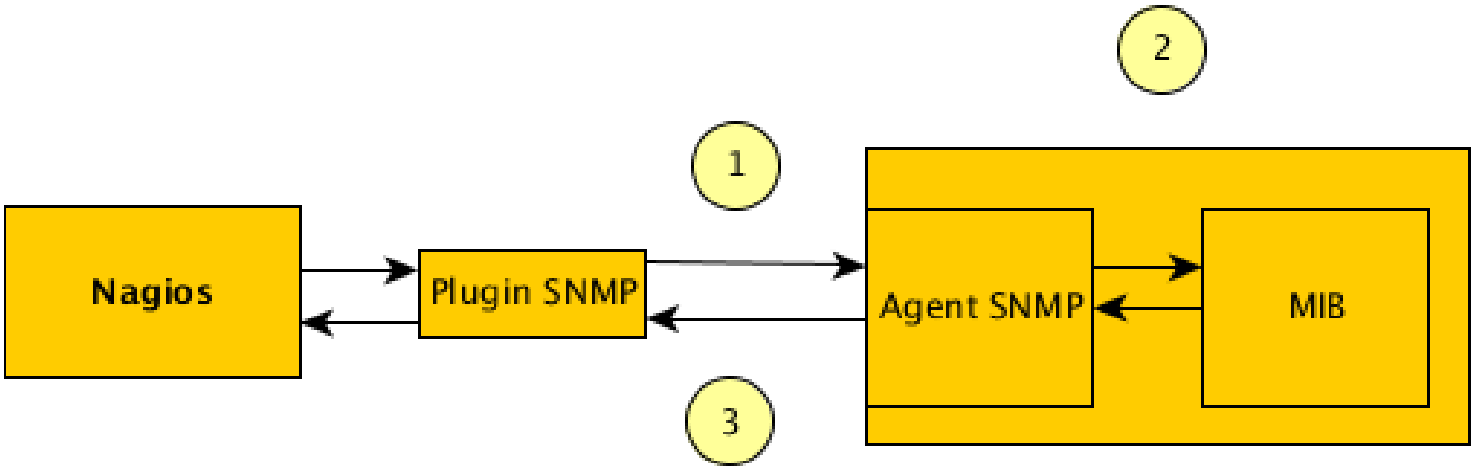
- Passive check

  Le serveur est à l'écoute d'informations envoyées par un script distant.

- SNMP

  Simple Network Management Protocol

  Va lire des informations propres à un matériel, dans la MIB (Management Information Base) et les transmet via le port UDP 161.



- 1. Requête SNMP
- 2. Récupération de l'objet désiré dans la MIB
- 3. Réponse SNMP

Il existe plusieurs versions de SNMP.

SNMP v1 et v2 : peu sécurisés.
Un “mot de passe”, la communauté.

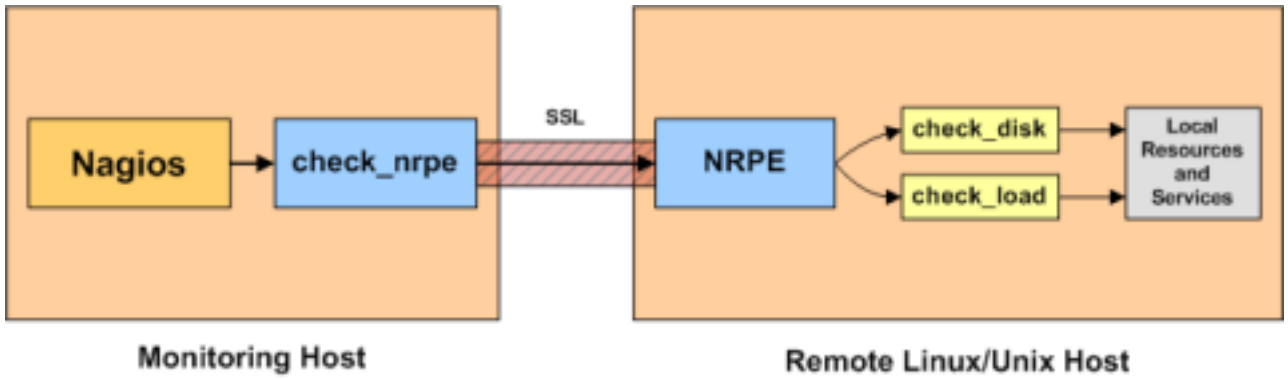
SNMP v3 : bien plus sécurisé.
Chiffrement, authentificaton, timestamp.

- NRPE (Nagios Remote Plugin Executor)

  Un plugin de Nagios va interroger un démon installé sur le serveur distant. Ce démon va exécuter un script pour obtenier les informations, puis les envoyer.

  Le script peut être écrit en n'importe quel langage.

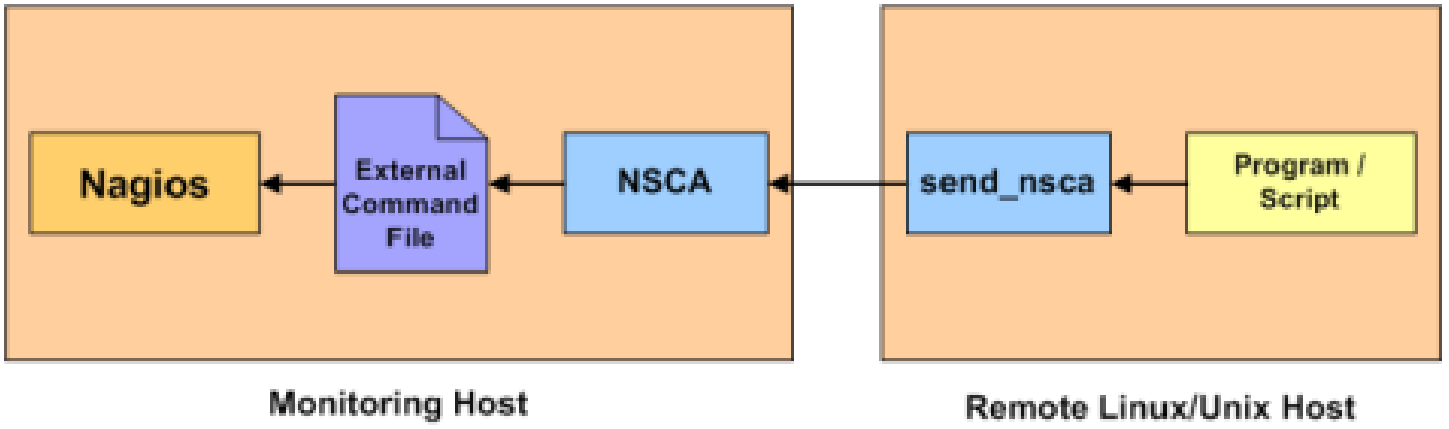
NRPE


Nagios
check_nrpe
SSL
NRPE
check_disk
check_load
Local Resources and Services
Monitoring Host
Remote Linux/Unix Host

- NSCA

  C'est une vérification passive : le serveur Nagios possède un démon NSCA, qui ne fait qu'écouter l'arrivée d'informations de clients. C'est le client qui émet ces informations.

NSCA


Nagios
External Command File
NSCA
send_nsca
Program / Script
Monitoring Host
Remote Linux/Unix Host


Interface

Interface Nagios

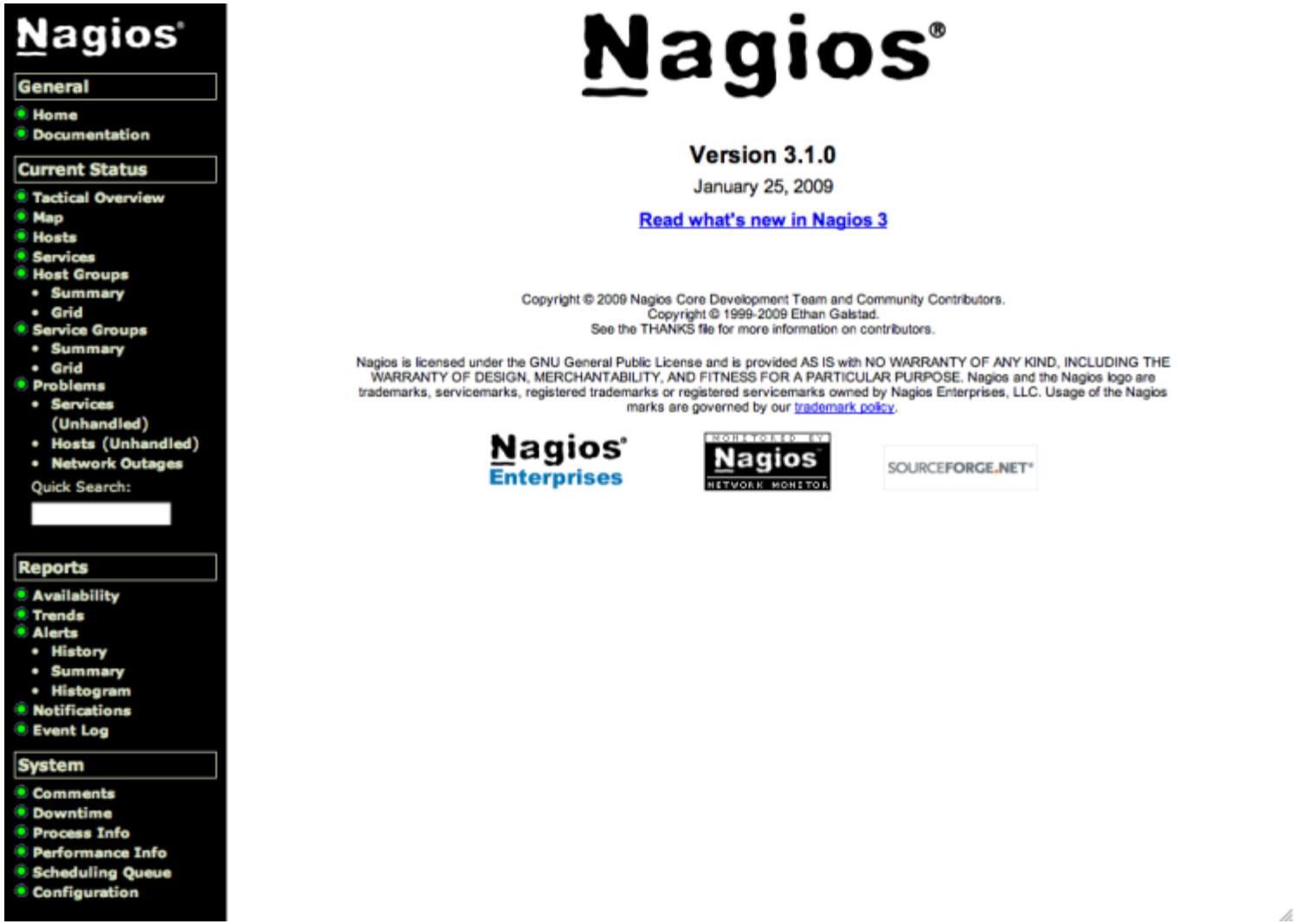
L'interface de base de Nagios est un peu vieillote.

Elle est au moins fonctionnelle.

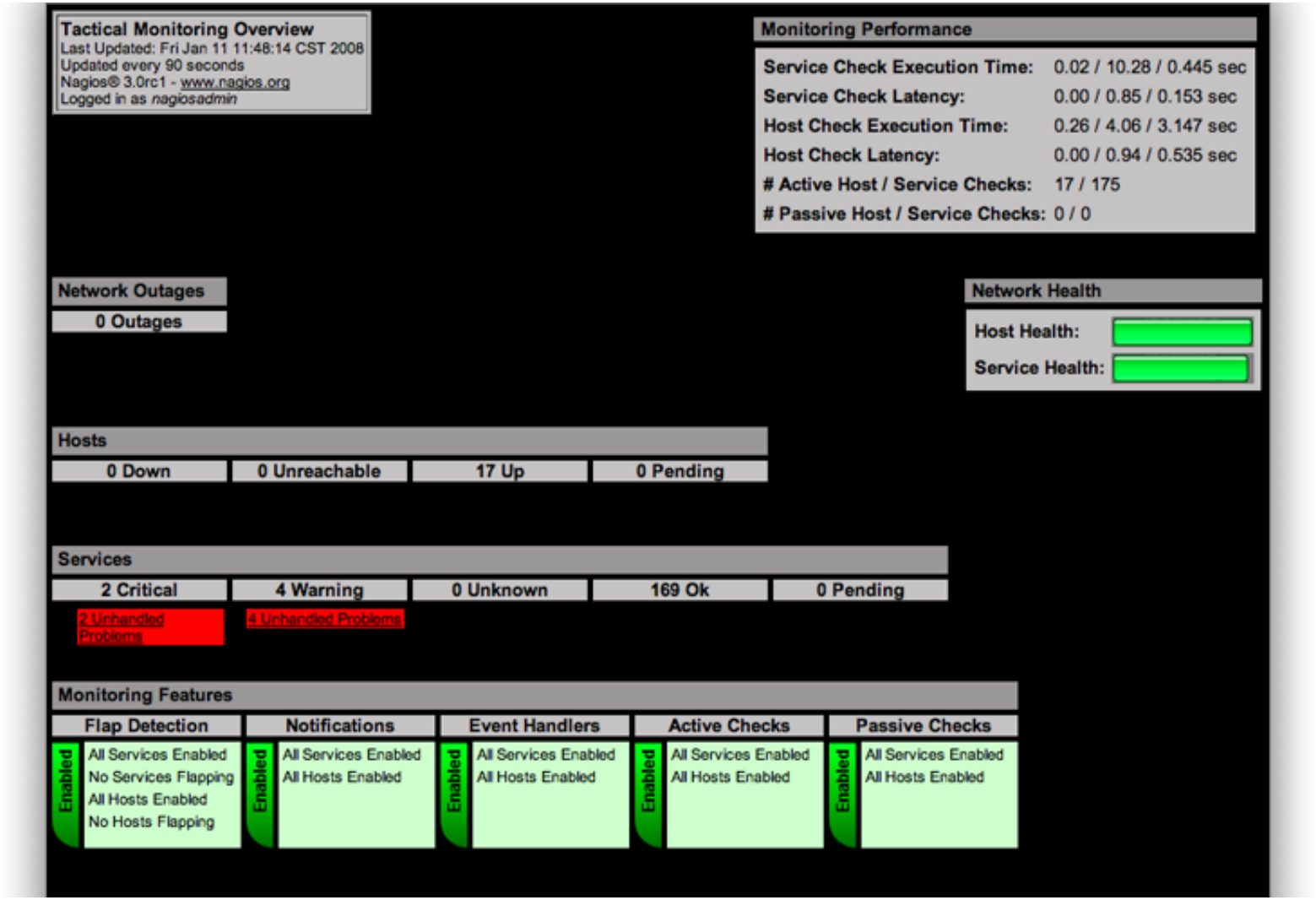
Possibilité de visualiser le parc par services, par hôtes, vue d'ensemble...

http://your-domain.tld/nagios3

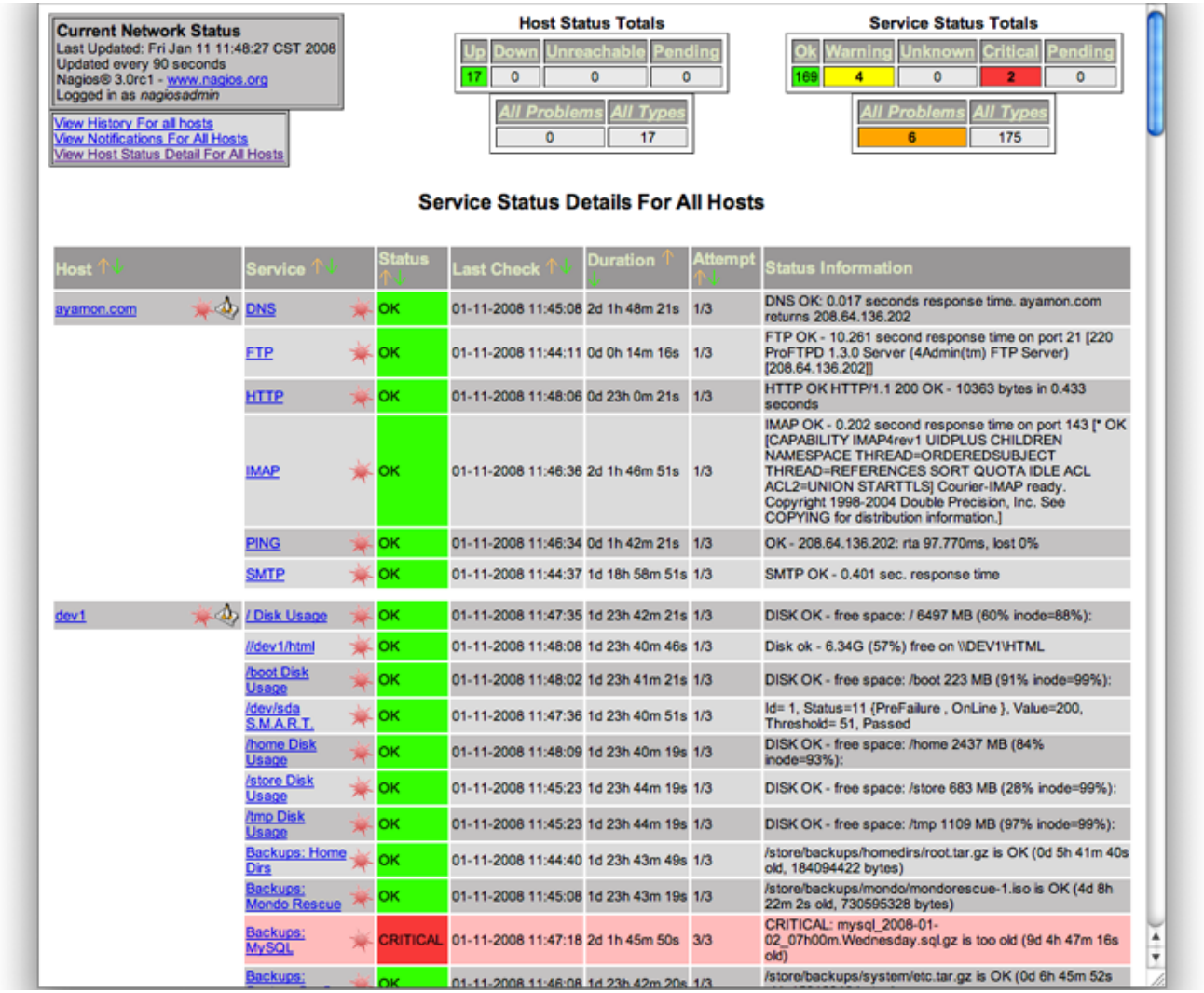
Interface Nagios



Interface Nagios



Interface Nagios



Current Network Status
Last Updated: Fri Jan 11 11:48:27 CST 2008
Updated every 90 seconds
Nagios® 3.0rc1 - 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
17	0	0	0

All Problems	All Types
0	17

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
169	4	0	2	0

All Problems	All Types
6	175

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ayamon.com	DNS	OK	01-11-2008 11:45:08	2d 1h 48m 21s	1/3	DNS OK: 0.017 seconds response time. ayamon.com returns 208.64.136.202
	FTP	OK	01-11-2008 11:44:11	0d 0h 14m 16s	1/3	FTP OK - 10.261 second response time on port 21 [220 ProFTPD 1.3.0 Server (4Admin(tm) FTP Server) [208.64.136.202]]
	HTTP	OK	01-11-2008 11:48:06	0d 23h 0m 21s	1/3	HTTP OK HTTP/1.1 200 OK - 10363 bytes in 0.433 seconds
	IMAP	OK	01-11-2008 11:46:36	2d 1h 46m 51s	1/3	IMAP OK - 0.202 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2004 Double Precision, Inc. See COPYING for distribution information.]
	PING	OK	01-11-2008 11:46:34	0d 1h 42m 21s	1/3	OK - 208.64.136.202: rta 97.770ms, lost 0%
	SMTP	OK	01-11-2008 11:44:37	1d 18h 58m 51s	1/3	SMTP OK - 0.401 sec. response time
dev1	/ Disk Usage	OK	01-11-2008 11:47:35	1d 23h 42m 21s	1/3	DISK OK - free space: / 6497 MB (60% inode=88%):
	//dev1/html	OK	01-11-2008 11:48:08	1d 23h 40m 46s	1/3	Disk ok - 6.34G (57%) free on \\DEV1\HTML
	/boot Disk Usage	OK	01-11-2008 11:48:02	1d 23h 41m 21s	1/3	DISK OK - free space: /boot 223 MB (91% inode=99%):
	/dev/sda S.M.A.R.T.	OK	01-11-2008 11:47:36	1d 23h 40m 51s	1/3	Id= 1, Status=11 {PreFailure , OnLine }, Value=200, Threshold= 51, Passed
	/home Disk Usage	OK	01-11-2008 11:48:09	1d 23h 40m 19s	1/3	DISK OK - free space: /home 2437 MB (84% inode=93%):
	/store Disk Usage	OK	01-11-2008 11:45:23	1d 23h 44m 19s	1/3	DISK OK - free space: /store 683 MB (28% inode=99%):
	/tmp Disk Usage	OK	01-11-2008 11:45:23	1d 23h 44m 19s	1/3	DISK OK - free space: /tmp 1109 MB (97% inode=99%):
	Backups: Home Dirs	OK	01-11-2008 11:44:40	1d 23h 43m 49s	1/3	/store/backups/homedirs/root.tar.gz is OK (0d 5h 41m 40s old, 184094422 bytes)
	Backups: Mondo Rescue	OK	01-11-2008 11:45:08	1d 23h 43m 19s	1/3	/store/backups/mondo/mondorescue-1.iso is OK (4d 8h 22m 2s old, 730595328 bytes)
	Backups: MySQL	CRITICAL	01-11-2008 11:47:18	2d 1h 45m 50s	3/3	CRITICAL: mysql_2008-01-02_07h00m.Wednesday.sql.gz is too old (9d 4h 47m 16s old)
	Backups:	OK	01-11-2008 11:46:08	1d 23h 42m 20s	1/3	/store/backups/system/etc.tar.gz is OK (0d 6h 45m 52s


Configuration

Basiquement, nous devons définir :

- Des hôtes

  une machine physique, virtuelle, un équipement.

- Des services

  une ressource ou un service à surveiller sur une machine.

- Des commandes

  une association nom de commande - script

- hosts.cfg

```
define host
{
use generic-host
host_name host1
alias myHost
address 127.0.0.1
check_command check-host-alive
max_check_attempts 20
notification_interval 60
notification_period 24x7
notification_options d,u,r
 }
```

- services.cfg

```
define service
{
use generic-service
host_name host1
service_description PING
is_volatile 0
check_period 24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
notification_interval 240
notification_period 24x7
notification_options c,r
check_command          check_ping
}
```

- Options de notification
  envoi d'une notification lors d'un état.

- Pour les hôtes :
  - d = DOWN
  - u = UNREACHABLE
  - r = retour en NORMAL
  - n = none
- Pour les services :
  - w = WARNING
  - u = UNKNOWN
  - r = retour en NORMAL
  - n = none

À propos des notifications

En plus de l'interface web, Nagios est capable d'envoyer des notifications :

- Par mail
- Par sms
- Par curl (Ex : Twitter)

- commands.cfg

```
define command
{
command_name command_name
command_line command_line
}
```

Il y a encore bien des choses à configurer, mais nous avons ici le minimum pour que Nagios fonctionne.

Décupler la puissance de Nagios

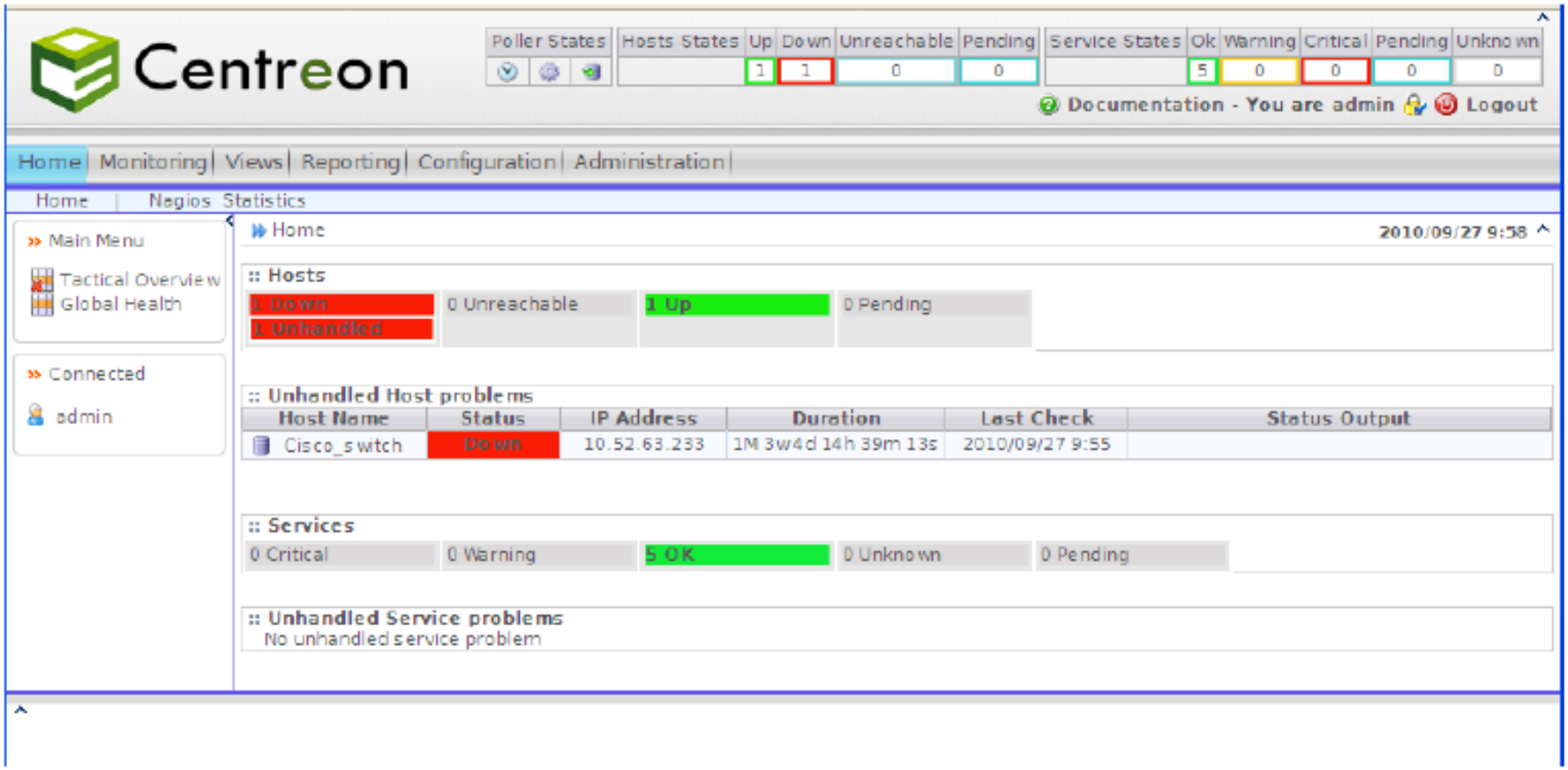
Décupler la puissance de Nagios

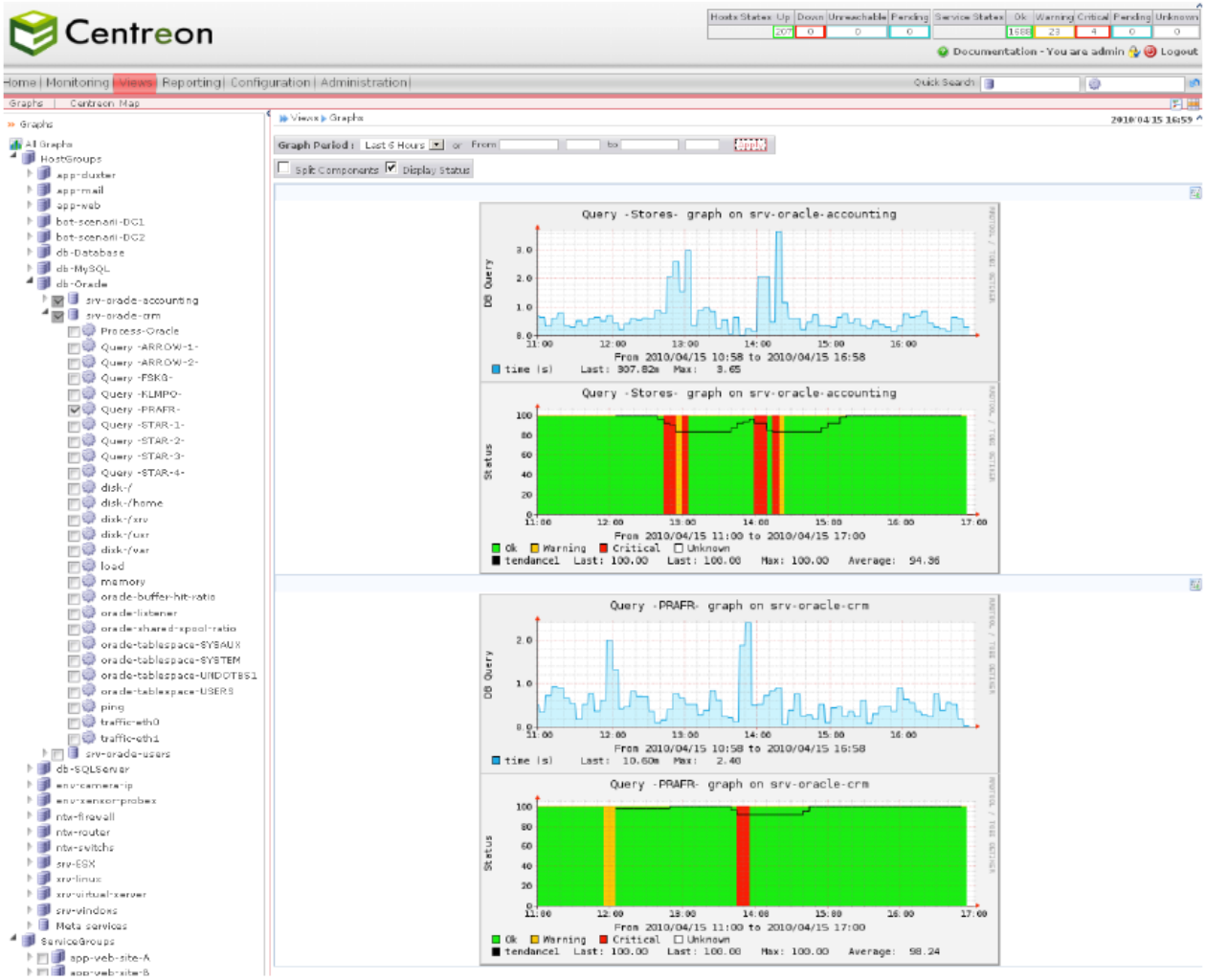
- Plusieurs projets ont pour objectif d'étoffer les fonctionnalités de Nagios, de le compléter, de l'améliorer, ou de simplifier son utilisation.
  - Centreon
  - Cacti
  - Shinken
  - EoN

Centreon

- Utilisation de l'ordonnanceur et des plugins de Nagios.
- Interface web plus moderne.
- Administration directement via l'interface web.
- Exportation des configs vers Nagios.
- Graphes

Centreon

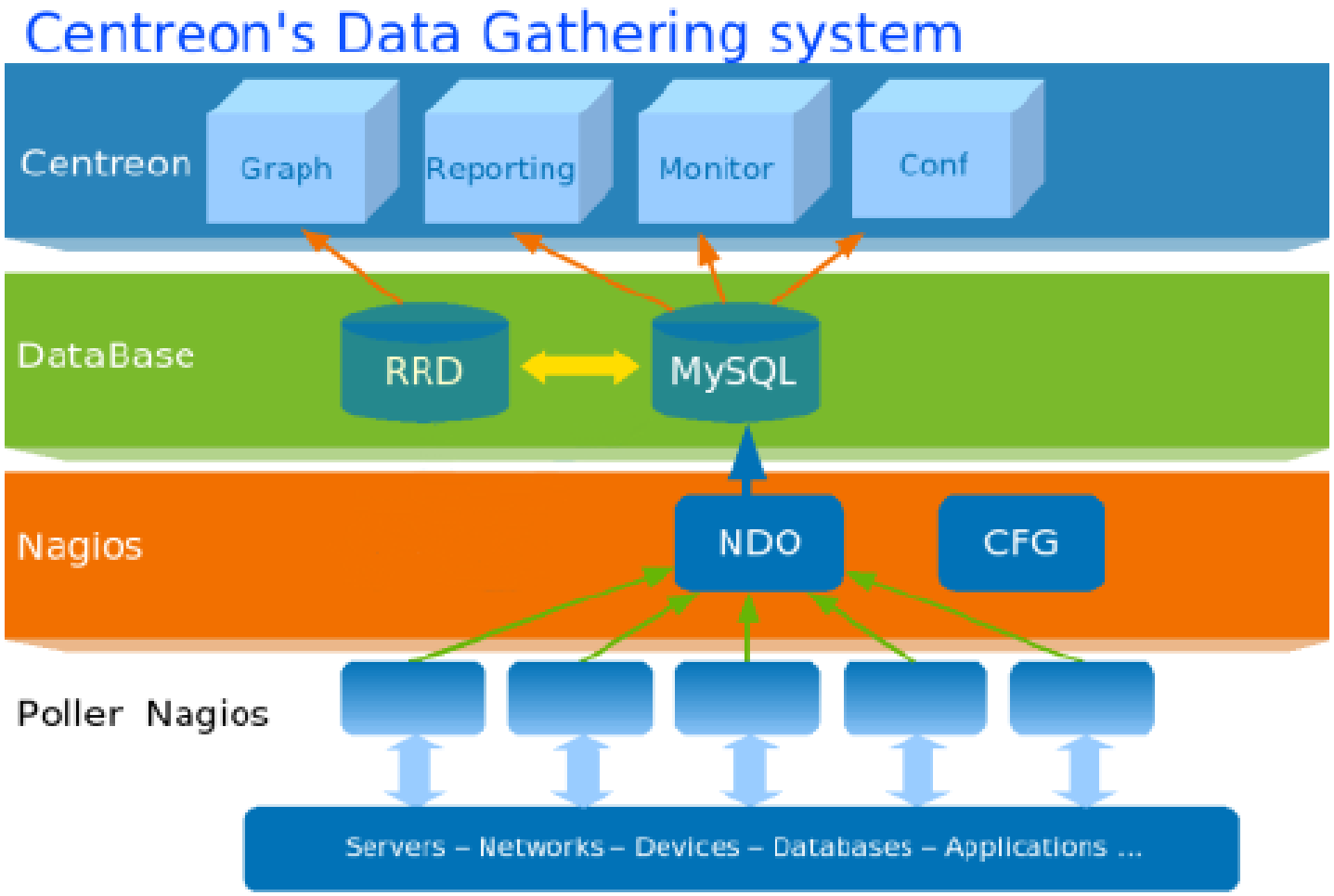

Centreon
Poller States
Hosts States Up Down Unreachable Pending
1 1 0 0
Service States Ok Warning Critical Pending Unknown
5 0 0 0 0
Documentation - You are admin Logout
Home Monitoring Views Reporting Configuration Administration
Home Nagios Statistics
Main Menu
Tactical Overview
Global Health
Connected
admin
Home
2010/09/27 9:58
:: Hosts
1 Down
1 Unhandled
0 Unreachable
1 Up
0 Pending
:: Unhandled Host problems
Host Name Status IP Address Duration Last Check Status Output
Cisco_switch Down 10.52.63.233 1M 3w4d 14h 39m 13s 2010/09/27 9:55
:: Services
0 Critical
0 Warning
5 OK
0 Unknown
0 Pending
:: Unhandled Service problems
No unhandled service problem


Centreon
Home | Monitoring | Views | Reporting | Configuration | Administration
Graphs | Centreon Map
Query -Stores- graph on srv-oracle-accounting
DB Query
From 2010/04/15 10:58 to 2010/04/15 16:58
Query -Stores- graph on srv-oracle-accounting
Status
From 2010/04/15 11:00 to 2010/04/15 17:00
Query -PRAFR- graph on srv-oracle-crm
DB Query
From 2010/04/15 10:58 to 2010/04/15 16:58
Query -PRAFR- graph on srv-oracle-crm
Status
From 2010/04/15 11:00 to 2010/04/15 17:00

- Couplage Nagios-Centreon
  - Nagios stocke les résultats des vérifications dans des fichiers binaires.

    => peu optimisé

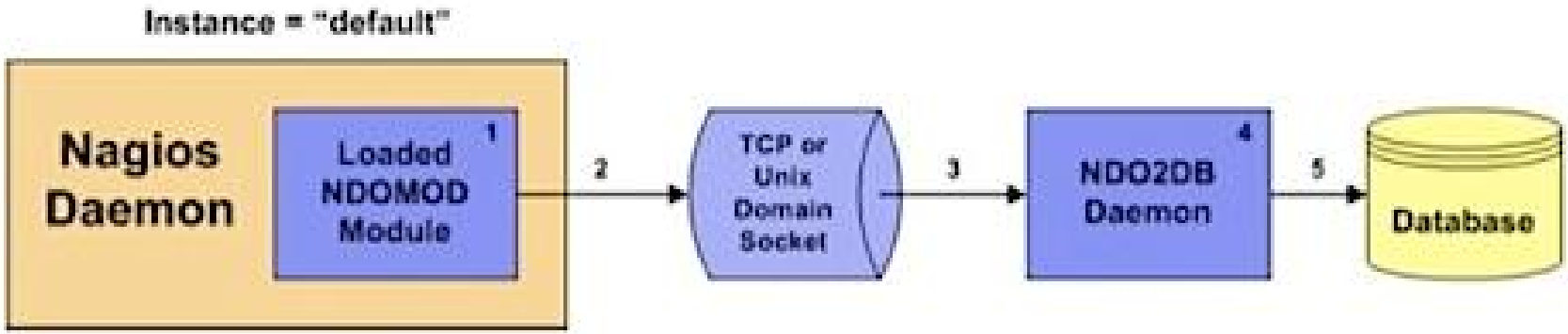
    => pas réutilisable par des programmes tiers
  - Nous allons donc forcer Nagios à stocker ses résultats dans une base de données, grâce à NDOUtils (Nagios Data Output Utils).


Centreon's Data Gathering system
Centreon
Graph
Reporting
Monitor
Conf
DataBase
RRD
MySQL
Nagios
NDO
CFG
Poller Nagios
Servers – Networks – Devices – Databases – Applications ...

NDO est composé de 2 modules : **NDOMOD** et **NDO2DB**

NDOMOD doit être lancé sur le serveur Nagios et permet de récupérer les informations remontées par Nagios pour les transmettre via TCP (ou un socket Unix) vers NDO2DB.

NDO2DB est un daemon qui écoute sur un port TCP (ou un socket Unix) et écrit les données reçues dans une base de donnée (MySQL ou PostgreSQL).

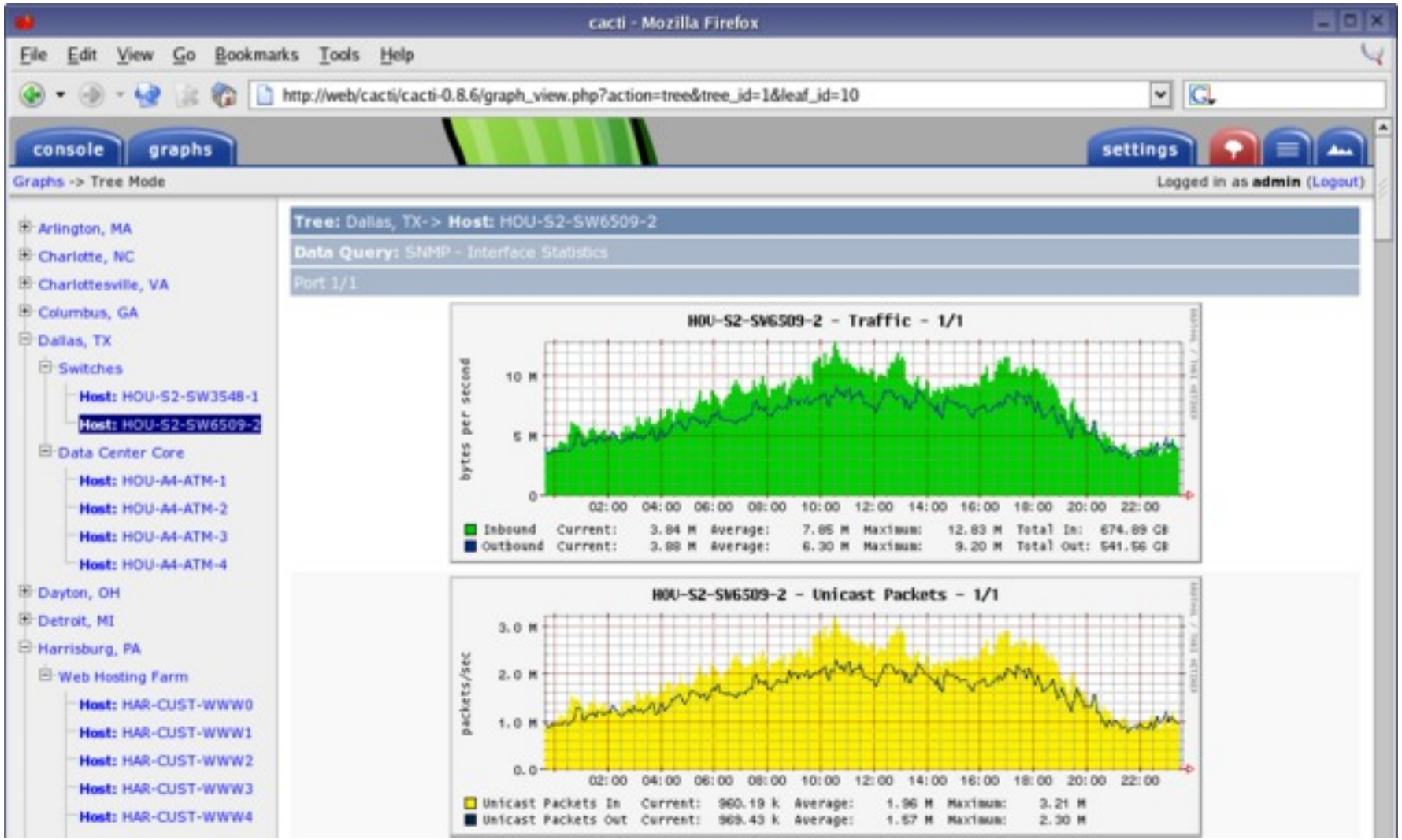

Instance = "default"
Nagios Daemon
Loaded NDOMOD Module
1
2
TCP or Unix Domain Socket
3
NDO2DB Daemon
4
5
Database

Cacti

Cacti

- Cacti n'a pas de lien direct avec Nagios (à part l'utilisation de SNMP). Il est souvent utilisé en complément de Nagios.
- Permet de collecter des données et de générer des graphiques à partir de celles-ci.
- Possibilité d'importer des hôtes nagios dans Cacti.

Cacti

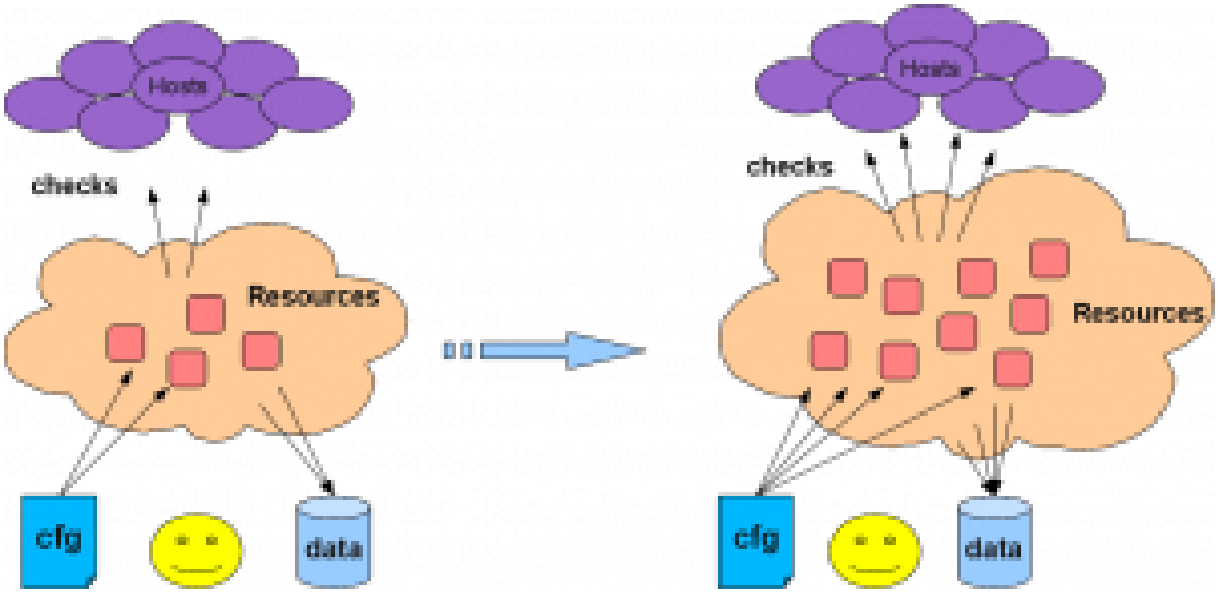

cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://web/cacti/cacti-0.8.6/graph_view.php?action=tree&tree_id=1&leaf_id=10
console
graphs
settings
Graphs -> Tree Mode
Logged in as admin (Logout)
Arlington, MA
Charlotte, NC
Charlottesville, VA
Columbus, GA
Dallas, TX
Switches
Host: HOU-S2-SW3548-1
Host: HOU-S2-SW6509-2
Data Center Core
Host: HOU-A4-ATM-1
Host: HOU-A4-ATM-2
Host: HOU-A4-ATM-3
Host: HOU-A4-ATM-4
Dayton, OH
Detroit, MI
Harrisburg, PA
Web Hosting Farm
Host: HAR-CUST-WWW0
Host: HAR-CUST-WWW1
Host: HAR-CUST-WWW2
Host: HAR-CUST-WWW3
Host: HAR-CUST-WWW4
Tree: Dallas, TX-> Host: HOU-S2-SW6509-2
Data Query: SNMP - Interface Statistics
Port 1/1
HOU-S2-SW6509-2 - Traffic - 1/1
bytes per second
10 M
5 M
0
02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00
Inbound Current: 3.84 M Average: 7.85 M Maximum: 12.83 M Total In: 674.89 GB
Outbound Current: 3.88 M Average: 6.30 M Maximum: 9.20 M Total Out: 541.56 GB
HOU-S2-SW6509-2 - Unicast Packets - 1/1
packets/sec
3.0 M
2.0 M
1.0 M
0.0
02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00
Unicast Packets In Current: 960.19 k Average: 1.96 M Maximum: 3.21 M
Unicast Packets Out Current: 969.43 k Average: 1.57 M Maximum: 2.30 M

Shinken

Shinken est un projet de réécriture du noyau de Nagios (l'ordonnanceur) en python, avec une architecture plus modulaire.

Plusieurs processus font chacun une tâche spécifique => gain de performances. (environ x5)

Supervision distribuée, similaire au cloud.


Hosts
checks
Resources
cfg
data
Hosts
checks
Resources
cfg
data

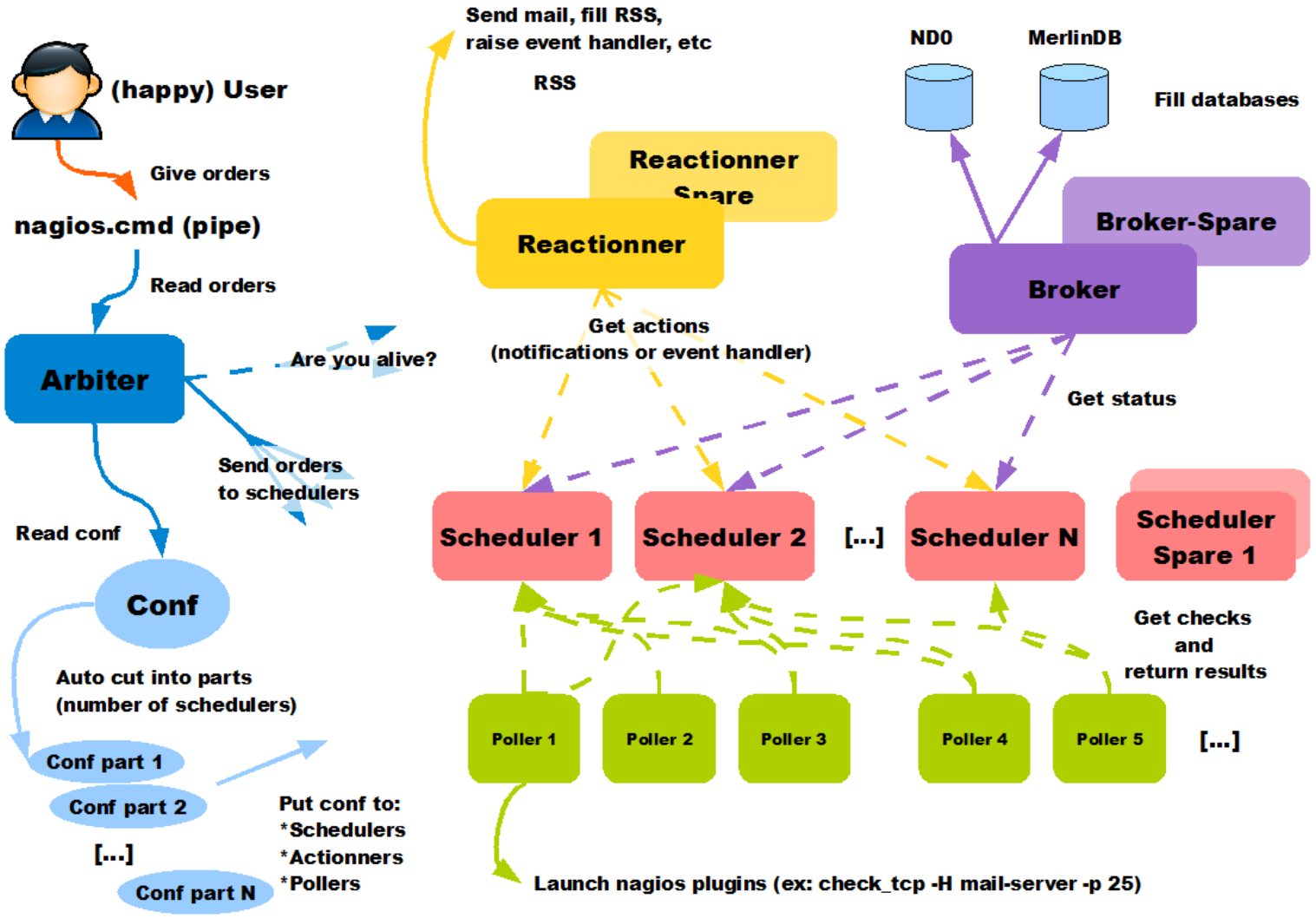
Arbiter : lit la config, la coupe en autant de parties qu'il y a de schedulers.

Schedulers : planifient les vérifications, l'analyse des résultats et le suivi des actions.

Pollers : lancent les plugins demandés par les schedulers. Renvoient les résultats aux schedulers.

Reactionners : lèvent des notifications ou des événements.

Broker : récupère les données des schedulers et les stocke.


(happy) User
Give orders
nagios.cmd (pipe)
Read orders
Arbiter
Are you alive?
Send orders
to schedulers
Read conf
Conf
Auto cut into parts
(number of schedulers)
Conf part 1
Conf part 2
[...]
Conf part N
Put conf to:
*Schedulers
*Actionners
*Pollers
Send mail, fill RSS,
raise event handler, etc
RSS
Reactionner
Reactionner Spare
Get actions
(notifications or event handler)
NDO
MerlinDB
Fill databases
Broker-Spare
Broker
Get status
Scheduler 1
Scheduler 2
[...]
Scheduler N
Scheduler Spare 1
Get checks
and
return results
Poller 1
Poller 2
Poller 3
Poller 4
Poller 5
[...]
Launch nagios plugins (ex: check_tcp -H mail-server -p 25)

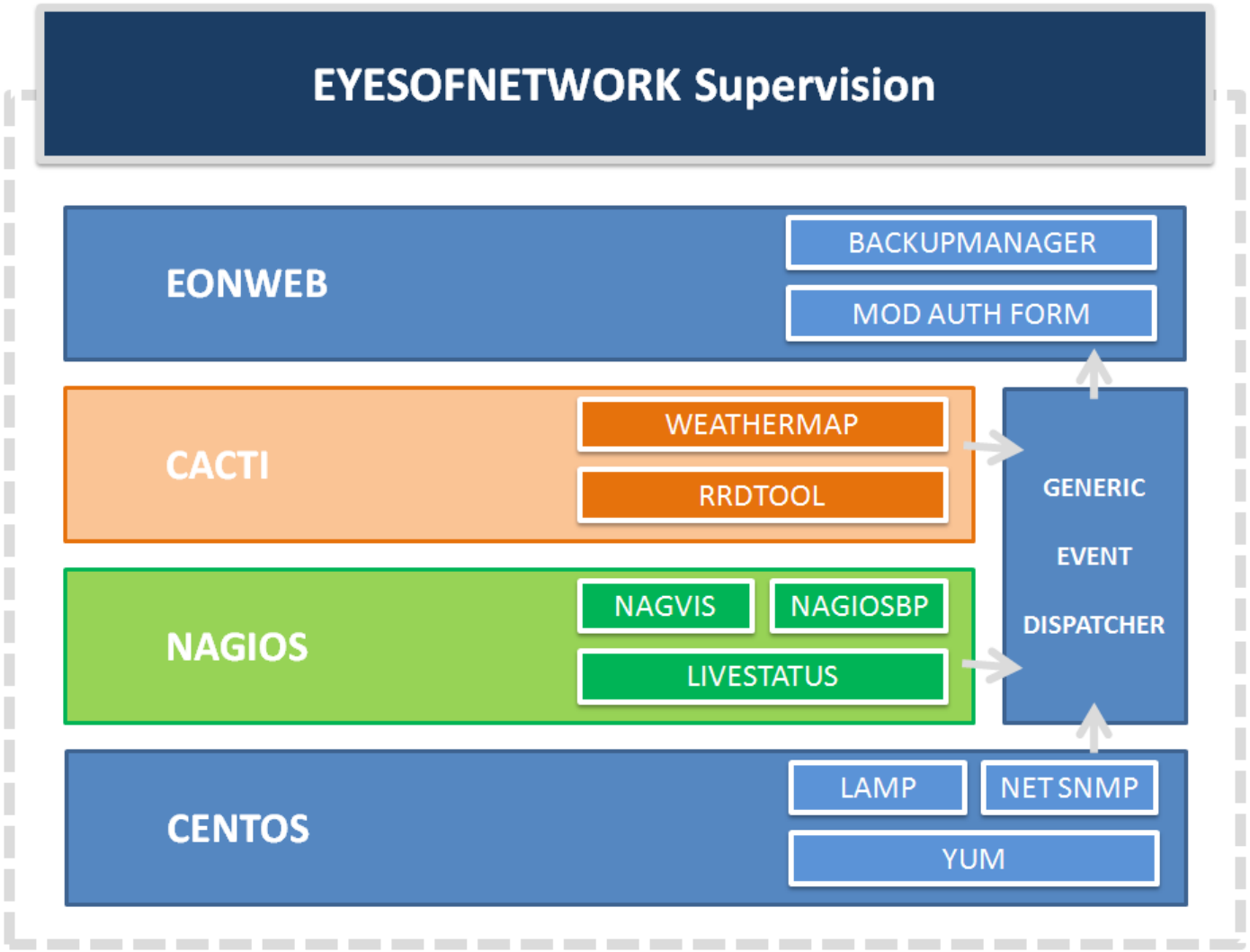
EoN

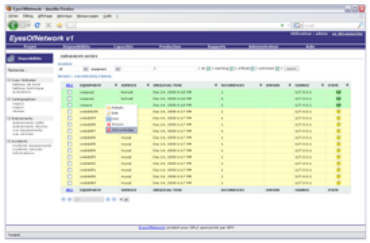
Eyes of Network

Une distribution basée sur CentOS qui possède de nombreux outils de supervision et de gestion de parc préinstallés.

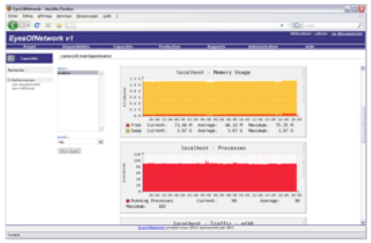
Interface centralisée, et import/export entre certaines applications simplifiées.

Nagios, Nagvis, Cacti, Weathermap, GLPI, etc...


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

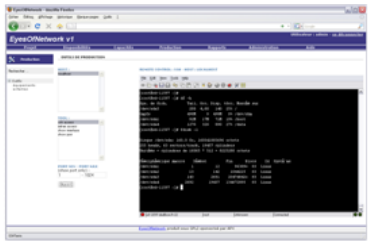


GESTION DE LA DISPONIBILITE



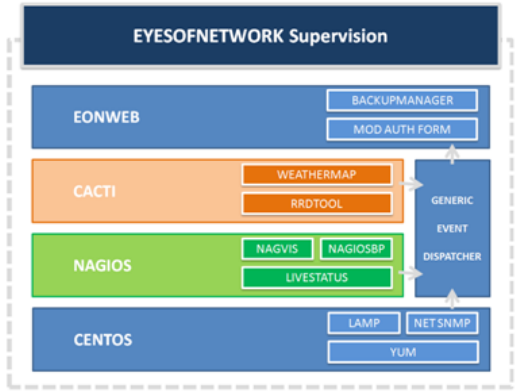
GESTION DE LA CAPACITE

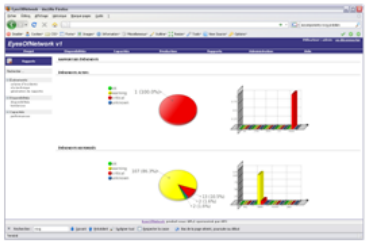
CARTOGRAPHIES



GESTION DE LA PRODUCTION

CENTRALISATION

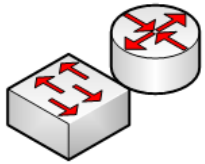




GENERATION DE RAPPORTS

Produit sous licence GPL2
sponsorisé par :

APX Services &Technologies



RESEAUX & STOCKAGE

SERVEURS

APPLICATIONS

De nombreux autres outils...


Questions ?

Contact

Email : jeremy.mathevet@supinfo.com
Twitter : @JeyG

Blog : www.jeyg.info