



Monitoring des Ressources Informatiques au LAL

Journées Informatique IN2P3 DAPNIA 2004 - HOURTIN
Jacquelin Charbonnel - printemps 2004

- solution basée sur 2 logiciels libres

- nagios

- www.nagios.org

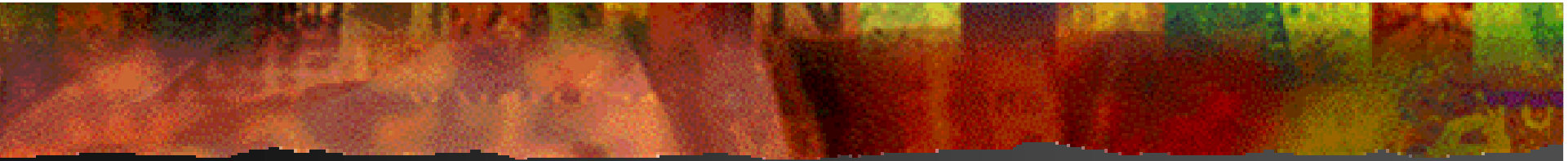
- rrdtool

- www.rrdtool.com

- + développement « maison » minimal

- couche d'interfaçage

- couche de présentation



Nagios

www.nagios.org

Nagios

- système de supervision de services
 - services réseaux (SMTP,HTTP...)
 - ressources systèmes (CPU, espaces disque)
 - au passage, supervision d'équipements (host down, host unreachable)

■ historique

- successeur de NetSaint
- aujourd'hui
 - version 1.2
 - version 2 en version alpha

■ prérequis

- Unix
- Apache (recommandé)

fonctionnalités

- acquisition d'états
- déclenchement d'actions
 - actions de prévention
 - notification via email, pager ou autre
 - lorsqu'une situation change d'état
- interface web
 - pour consultation
 - pour administration (partielle)

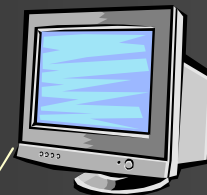
architecture

- nagios = moteur + interface web
 - 1 daemon + CGIs
 - programmes C
- acquisitions et actions assurées par des plugins
 - petits programmes autonomes
 - développés indépendamment du moteur
 - distribués séparément du moteur

serveur de monitoring



requête réseau



machines à surveiller



requête réseau

environnement

- fichiers de configuration
 - classiques (variable=valeur)
- logs
 - au choix via syslog ou dans fichier spécifique
 - rotation gérée
- données
 - description d'objets dans des fichiers textes
 - les valeurs collectées sont stockées au choix
 - dans des fichiers textes
 - dans une base de données (postgres ou mysql)

principaux objets de nagios

- objets cibles des tests

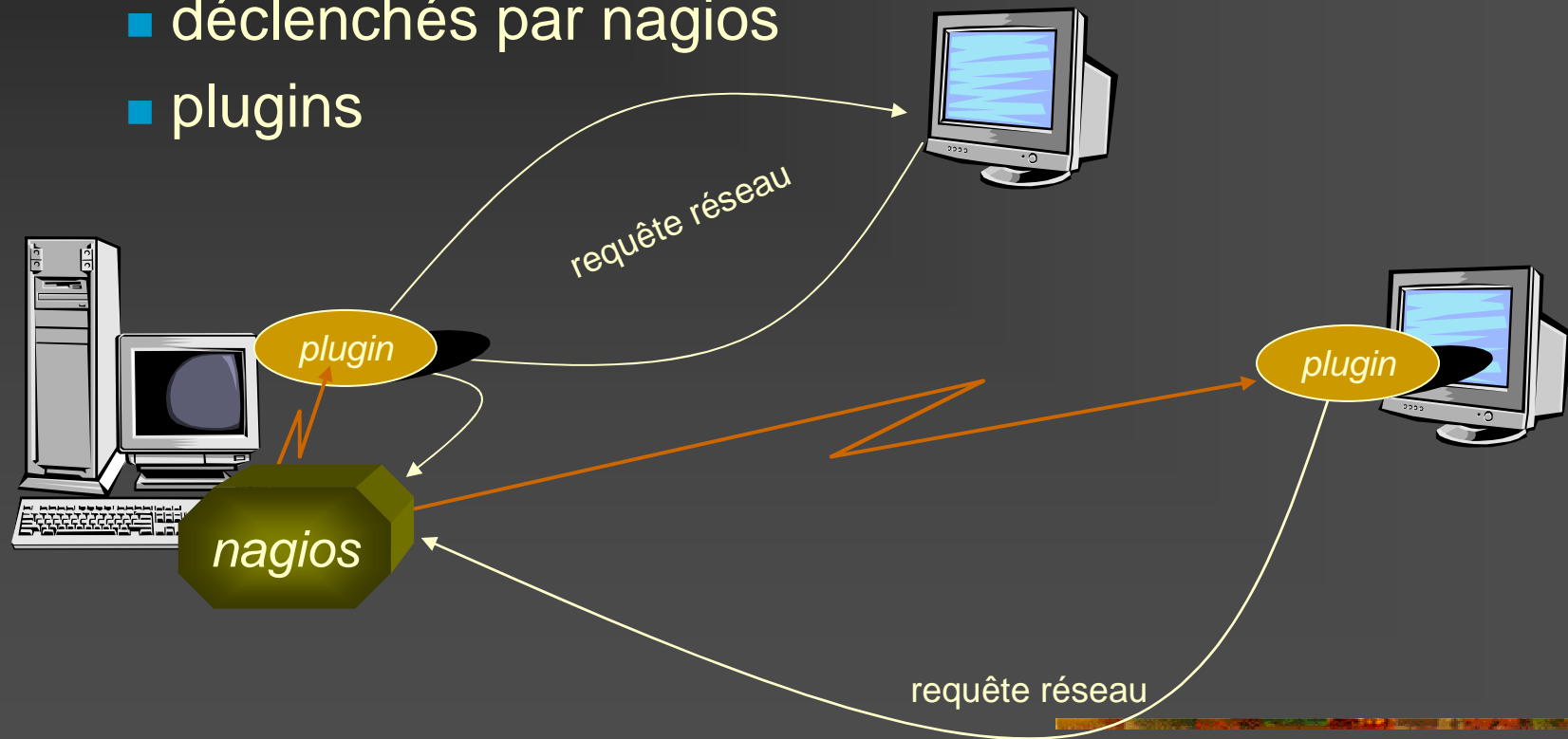
- host
- service

- autres objets

- hostgroup
- contact
- time-period
- command

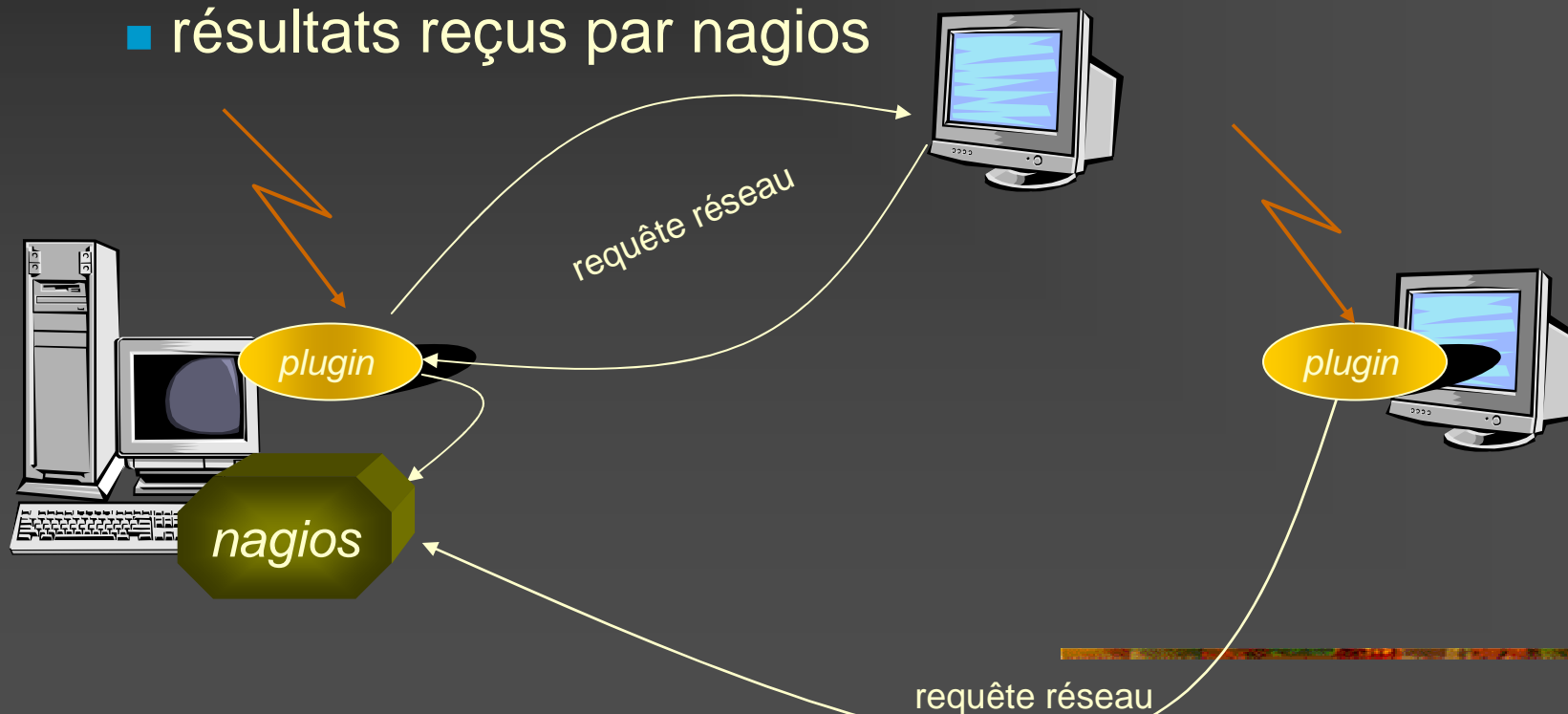
acquisitions

- active checks
 - déclenchés par nagios
 - plugins



acquisitions

- passive check
 - déclenchement externe indépendant de nagios
 - résultats reçus par nagios



actions

- handler
 - déclenchés par nagios
 - programme externe, destiné à tenter de résoudre un problème avant d'alerter
 - ne renvoie pas d'information à Nagios

états

à tout moment :

- un host se trouve dans un des états :
 - ok
 - unreachable
 - down
- un service se trouve dans un des états :
 - ok
 - warning
 - critical
 - unknown

2 types d'état

- soft
 - l'état courant est en cours de caractérisation
 - pas de notification possible
 - possibilité d'agir (handler)
- hard
 - l'état de la situation courante est identifié
 - possibilité de notification

notification

- déclenchée lors d'un changement d'état, lorsque le nouvel état est de type HARD
- pertinence de l'envoi d'une notification

test d'1 service

si problème

alors test du host

si problème

alors envoi d'1 seule notification pour ce host

sinon envoi d'1 notification pour ce service

host

```
define host{
    host_name      atlas
    address        134.158.88.87

    // périodicité des re-notifications
    notification_interval 0

    // horaire pour les notifications
    notification_period 24x7

    // down, unreachable et/ou recovery
    notification_options d,u

    // # essais pour de passer de soft à hard
    max_check_attempts 2

    check_command  check-host-alive
    parent         giga_sw
}
```

hostgroup

```
define hostgroup {  
  host_group name    network_equipment  
  members           grouter,gsw208,bridgelan3,airport1  
  contact_groups    network_contact  
}
```

service

```
define service{
  service_name          ssh response
  hostgroup_name        unix_servers

  check_period          24x7
  normal_check_interval 15
  retry_check_interval  5

  notification_interval 0
  notification_period   24x7

  // warning, critical, unknown et/ou recovery
  notification_options  c,u

  max_check_attempts    2

  check_command          check-ssh
  contact_groups         unix_admin
}
```

contact

```
define contact {
  contact_name      charbonnel
  alias             Jacquelin Charbonnel
  email             charbonnel@lal.in2p3.fr

  service_notification_period 24x7
  host_notification_period    24x7

  service_notification_options w,u,c,r
  host_notification_options    d,u,r

  service_notification_commands service-notify-by-email
  host_notification_commands   host-notify-by-email
}
```

period

```
define timeperiod
{
  timeperiod_name    24x7


  sunday             00:00-24:00
  monday             00:00-24:00
  tuesday            00:00-24:00
  wednesday          00:00-24:00
  thursday           00:00-24:00
  friday             00:00-24:00
  saturday           00:00-24:00
}
```

Host Group	Host Status Totals	Service Status Totals
auger (auger_group)	9 UP	18 OK
clu_nis (clu_nis_group)	2 UP	32 OK
dns (dns_group)	2 UP	92 OK 4 WARNING 1 CRITICAL
fs (fs_group)	2 UP	24 OK
grid (grid_group)	3 UP	3 OK
link (link_group)	4 UP	No matching services
lsf (lsf_group)	23 UP	102 OK
mac (mac_group)	2 UP	6 OK
network_equipment (network_equipment_group)	32 UP	33 OK
networker (networker_group)	17 UP	68 OK
nis (nis_group)	31 UP	103 OK
nis_serv (nis_serv_group)	3 UP	37 OK
printer (printer_group)	6 UP	5 OK 1 WARNING
ssh (ssh_group)	20 UP	68 OK
ssh_si (ssh_si_group)	3 UP	47 OK
vmstat (vmstat_group)	1 UP	15 OK
windows (windows_group)	5 UP	10 OK

[ssh_si](#) ([ssh_si_group](#))

Host	Services
as3 	[lsf] lsf [master] ps [net] si ssh [net] APX [net] ftp [net] http [net] lpr gateway [net] networker [net] nfs [net] smtp [net] ypbind [net] ypserv [proc] MIMEdfang [proc] ftp [report] mail attachments [report] mail spam
asa 	[lsf] lsf [master] ps [net] si ssh [net] APX [net] ftp [net] http [net] lpr gateway [net] networker [net] nfs [net] smtp [net] ypbind [net] ypserv [proc] MIMEdfang [proc] ftp [report] mail attachments [report] mail spam
super 	[exec] vmstat [fs] / [fs] /home [fs] /tmp [fs] /var [master] fs [master] ps [net] si ssh [net] dns [net] http [net] mysql [net] networker [net] smtp [net] ypbind [proc] nagios

[vmstat](#) ([vmstat_group](#))

Host	Services
super 	[exec] vmstat [fs] / [fs] /home [fs] /tmp [fs] /var [master] fs [master] ps [net] si ssh [net] dns [net] http [net] mysql [net] networker [net] smtp [net] ypbind [proc] nagios

[windows](#) ([windows_group](#))

Host	Services
pcadsrv 	[net] netbios [net] networker
pcmqc 	[net] netbios [net] networker
pcserv 	[net] netbios [net] networker
wincenter2 	[net] ica [net] netbios

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑ ↓	Attempt ↑↓	Status Information
lx1	[fs] /var P	OK	2004-03-23 21:31:15	1d 11h 35m 52s	1/2	419Mo free - 14% of 509Mo used
	[lsf] lsf P	OK	2004-03-23 21:32:41	6d 0h 51m 54s	1/2	ok
	[master] fs	OK	2004-03-23 21:31:14	1d 11h 36m 22s	1/2	1 passive check(s) generated
	[master] ps	OK	2004-03-23 21:32:57	6d 0h 51m 42s	1/3	3 passive check(s) performed
	[net] ssh	OK	2004-03-23 21:29:33	6d 0h 49m 19s	1/3	SSH OK - OpenSSH_3.7.1p2 (protocol 1.99)
	[net] ypbind	OK	2004-03-23 21:35:17	1d 2h 35m 21s	1/1	OK: RPC program ypbind version 1 version 2 udp running
	[proc] afpd P	OK	2004-03-23 21:32:57	6d 0h 50m 45s	1/1	papd: 1 match(es)
	[proc] atalkd P	OK	2004-03-23 21:32:57	6d 0h 50m 45s	1/1	papd: 1 match(es)
	[proc] papd P	OK	2004-03-23 21:32:57	6d 0h 3m 12s	1/1	papd: 1 match(es)
super	[exec] vmstat	OK	2004-03-23 21:32:05	6d 0h 48m 33s	1/2	user:8 sys:3 idle:89
	[fs] / P	OK	2004-03-23 21:35:23	1d 11h 30m 52s	1/2	3Go free - 57% of 7Go used
	[fs] /home P	OK	2004-03-23 21:35:23	5d 11h 49m 15s	1/2	7Go free - 4% of 7Go used
	[fs] /tmp P	OK	2004-03-23 21:30:24	5d 11h 49m 15s	1/2	456Mo free - 3% of 493Mo used
	[fs] /var P	OK	2004-03-23 21:30:24	5d 11h 49m 15s	1/2	6Go free - 14% of 7Go used
	[master] fs	OK	2004-03-23 21:35:23	5d 11h 38m 7s	1/2	4 passive check(s) generated
	[master] ps	OK	2004-03-23 21:32:04	6d 0h 38m 3s	1/3	1 passive check(s) performed
	[net] sip ssh	OK	2004-03-23 21:33:46	6d 0h 49m 59s	1/3	SSH OK - OpenSSH_3.5p1 (protocol 1.99)
	[net] dns	OK	2004-03-23 21:35:22	6d 0h 48m 32s	1/2	DNS ok - 0 seconds response time, Address(es) is/are 216.109.117.205
	[net] http	OK	2004-03-23 21:32:05	1d 1h 59m 13s	1/1	HTTP ok: HTTP/1.1 200 OK - 0.008 second response time
	[net] mysql	OK	2004-03-23 21:33:46	1d 2h 25m 36s	1/2	Uptime: 1814398 Threads: 2 Questions: 41793416 Slow queries: 0 Opens: 701670 Flush tables: 1 Open tables: 19 Queries per second avg: 23.034
	[net] networker	OK	2004-03-23 21:35:27	6d 0h 38m 2s	1/1	TCP OK - 0.001 second response time on port 7937 // TCP OK - 0.001 second response time on port 7938
	[net] smtp	OK	2004-03-23 21:32:05	1d 2h 16m 5s	1/2	SMTP OK - 0 second response time
	[net] ypbind	OK	2004-03-23 21:34:51	1d 2h 36m 13s	1/1	OK: RPC program ypbind version 1 version 2 udp running
	[proc] nagios P	OK	2004-03-23 21:32:05	5d 23h 33m 44s	1/1	nagios: 3 match(es)

autres concepts

- dépendance $host_i \rightarrow host_k$
- dépendance $(host,service)_i \rightarrow (host,service)_k$
- flapping detection
- escalade notification
- monitoring distribué

principe du plugin

- programme autonome
- doit renvoyer
 - 1 ligne de texte décrivant l'état courant
 - un état
 - ok
 - warning
 - critical
 - unknown
- doit traiter l'option `--help`

concrètement

- programme écrit en C, perl, shell...
- qui écrit une ligne de texte sur stdout
- qui renvoie un code compris entre 0 et 3

extrait de nagios-plugins

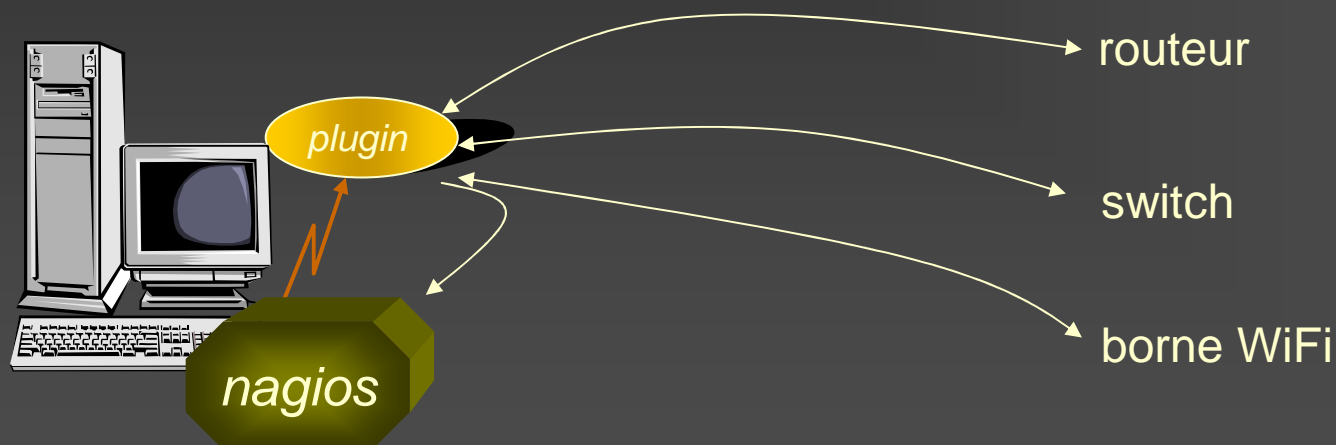
check_breeze	check_http	check_mysql	check_procs	check_time
check_by_ssh	check_nagios	check_real	check_udp	
check_citrix	check_users	check_nntp	check_rpc	check_ups
check_dig	check_imap	check_nt	check_sensors	
check_disk	check_ircd	check_ntp	check_simap	check_vsz
check_disk_smb		check_ldap	check_nwstat	check_smtp
check_dns	check_load	check_oracle	check_snmp	negate
check_log	check_overcr	check_spop	check_wave	
check_flexlm	check_mailq	check_pgsql	check_ssh	
check_ftp	check_mrtg	check_ping	check_swap	
check_hpjd	check_mrtgtraf	check_pop	check_tcp	

ressources LAL monitorées

- connectivité du réseau
 - services réseaux
 - ressources systèmes des serveurs
 - taux d'occupation des files systems
 - service d'impression et imprimantes
 - indicateurs déduits de l'analyse des logs
 - bon déroulement des backups
 - filtrage des spams
 - anti-virus sur le mail
-

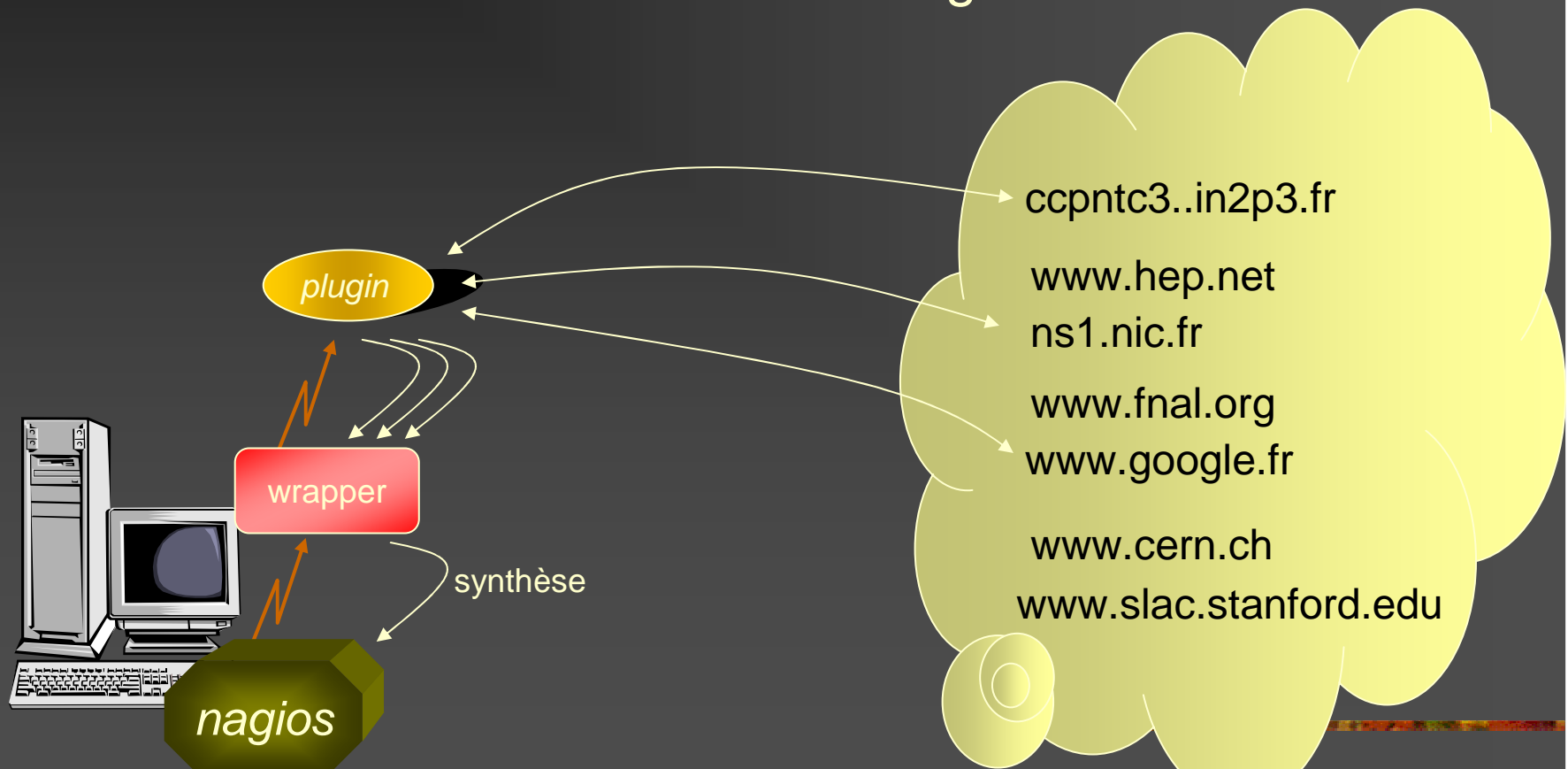
connectivité du réseau local

- utilisation classique des plugins
- test de l'accessibilité de la couche IP des différents équipements réseaux



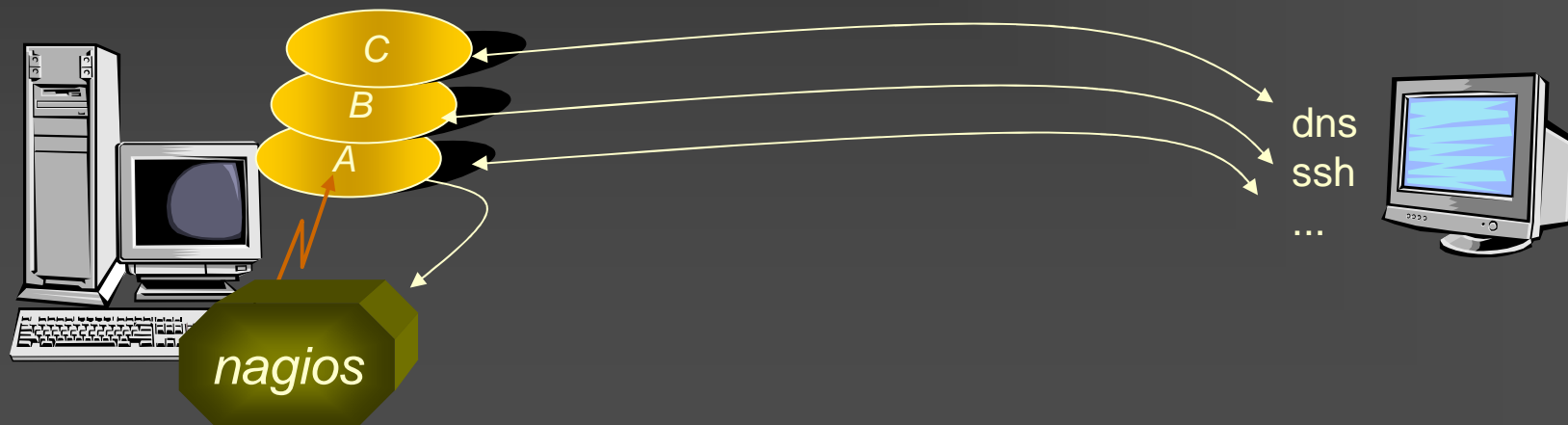
connectivité Internet

- la connectivité Internet = 1 service nagios



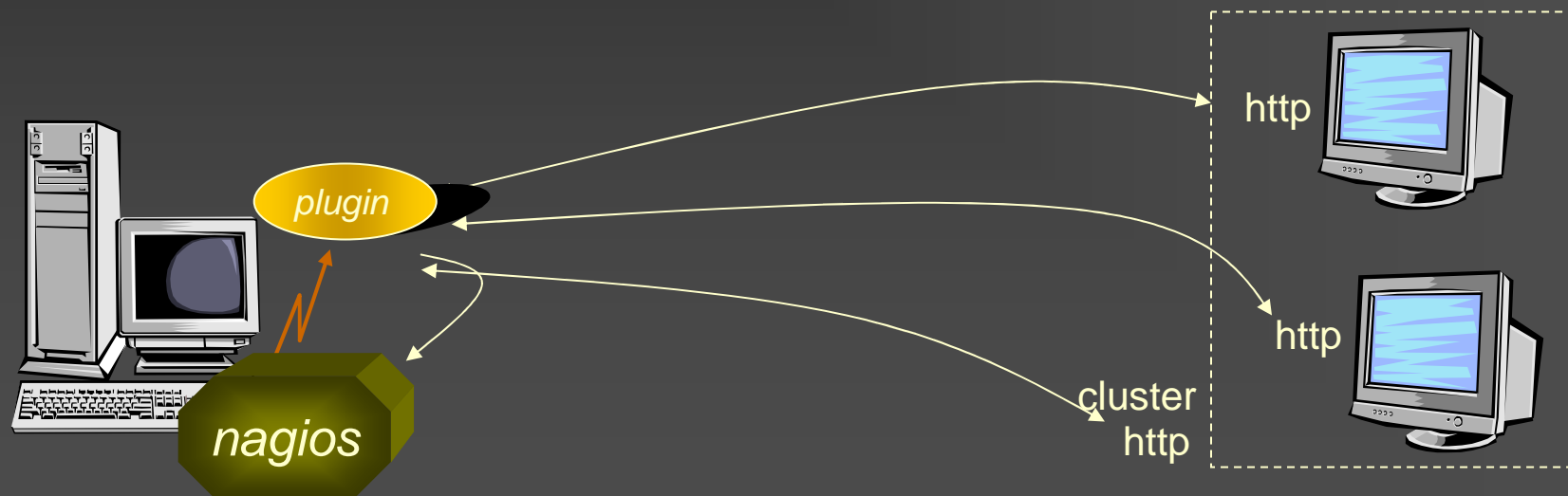
services réseaux

- utilisation classique des plugins
- 1 service réseau = 1 service nagios



services réseaux cluster

- utilisation classique des plugins
- 1 service réseau = n+1 services nagios
- services surveillés :
 - http, ftp, smtp, imap, lpd, nfs, nis



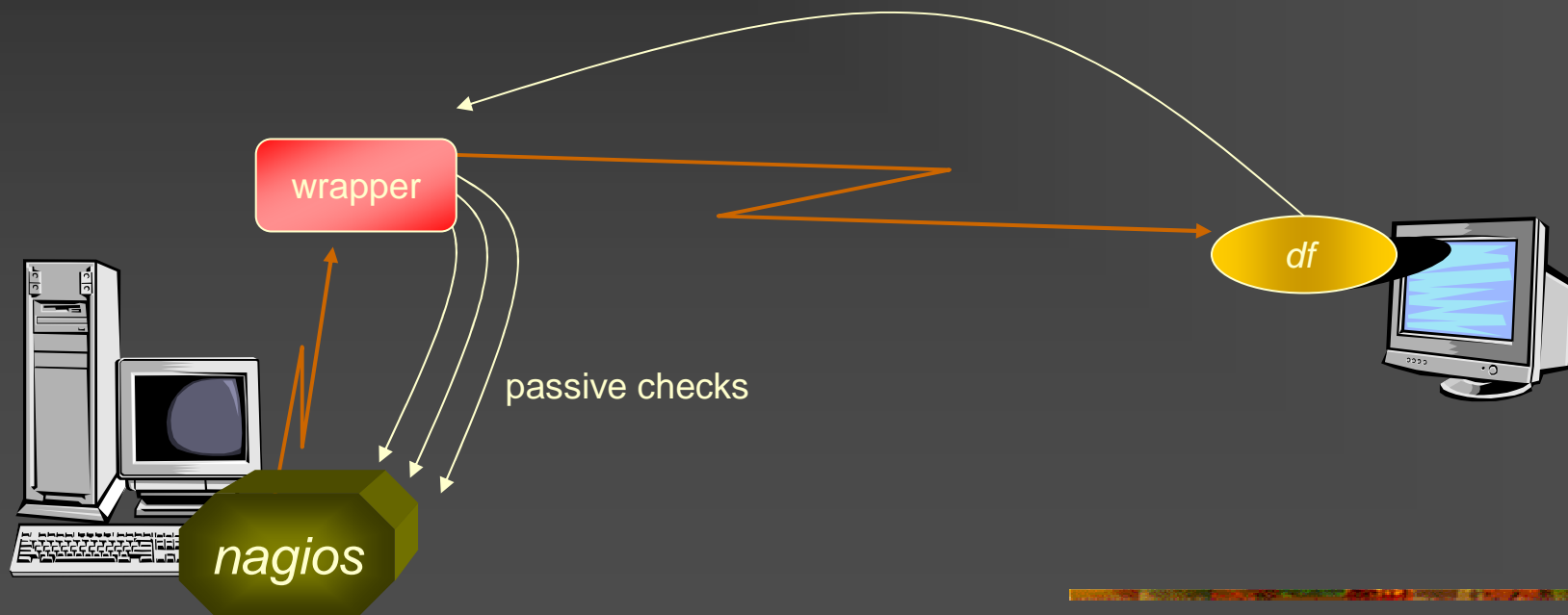
ressources élémentaires serveurs

- utilisation classique des plugins
- ressources monitorées :
 - mail queue, cpu...



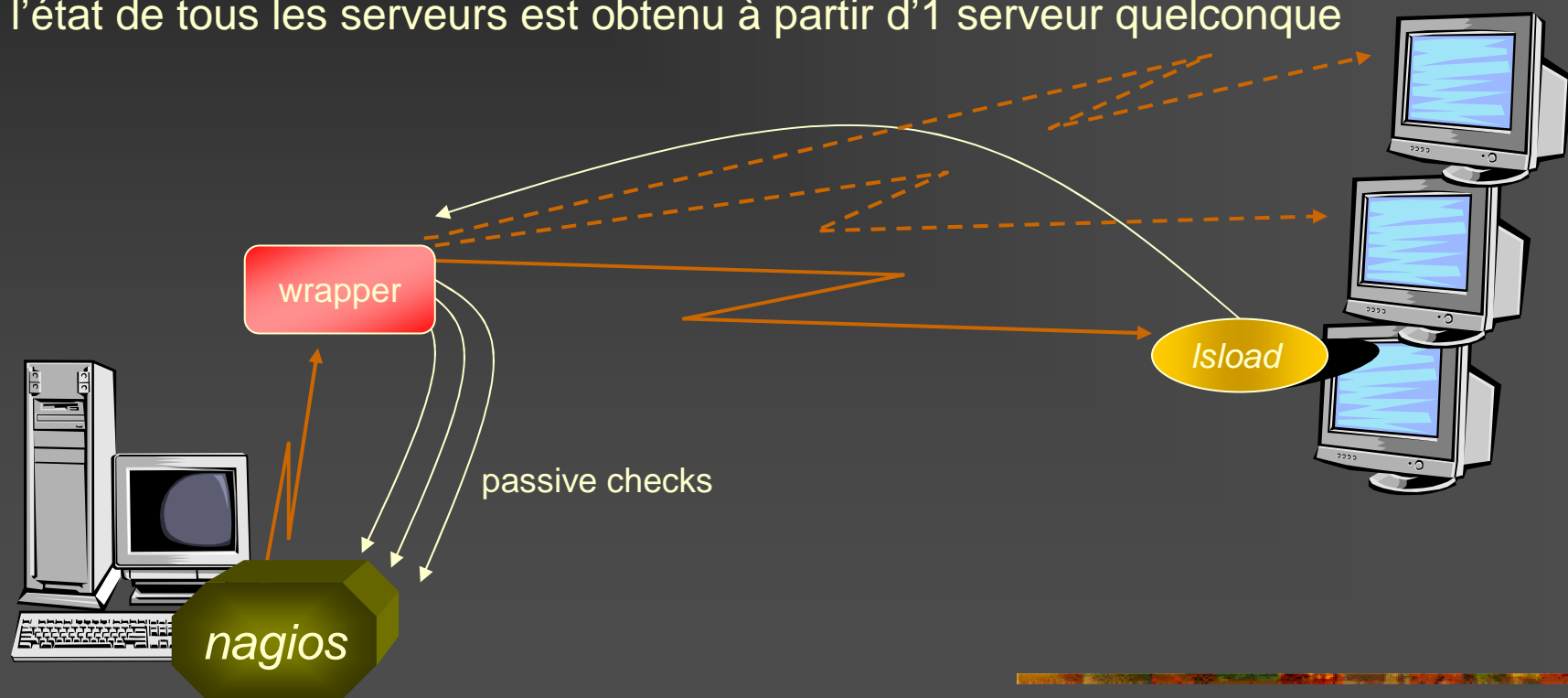
files systems

- 1 files system = 1 service nagios
- plugin : df
- 1 df → état de tous les files systems du serveur



Isf

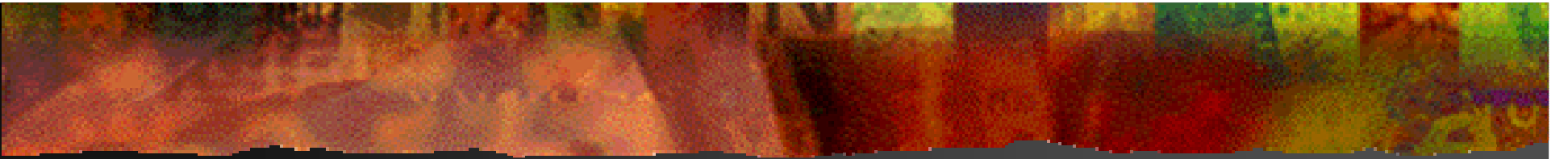
- n services nagios par serveur Isf
 - cpu, paging, io...
- l'état de tous les serveurs est obtenu à partir d'1 serveur quelconque



Conclusion

- bilan sur Nagios
 - robuste, peu de bugs
 - prévu pour supporter la charge
 - bien documenté
 - flexible (ex: wrapper)

- nagios n'archive pas les états
 - besoin de suivre l'évolution dans le temps
 - besoin de visualisations graphiques

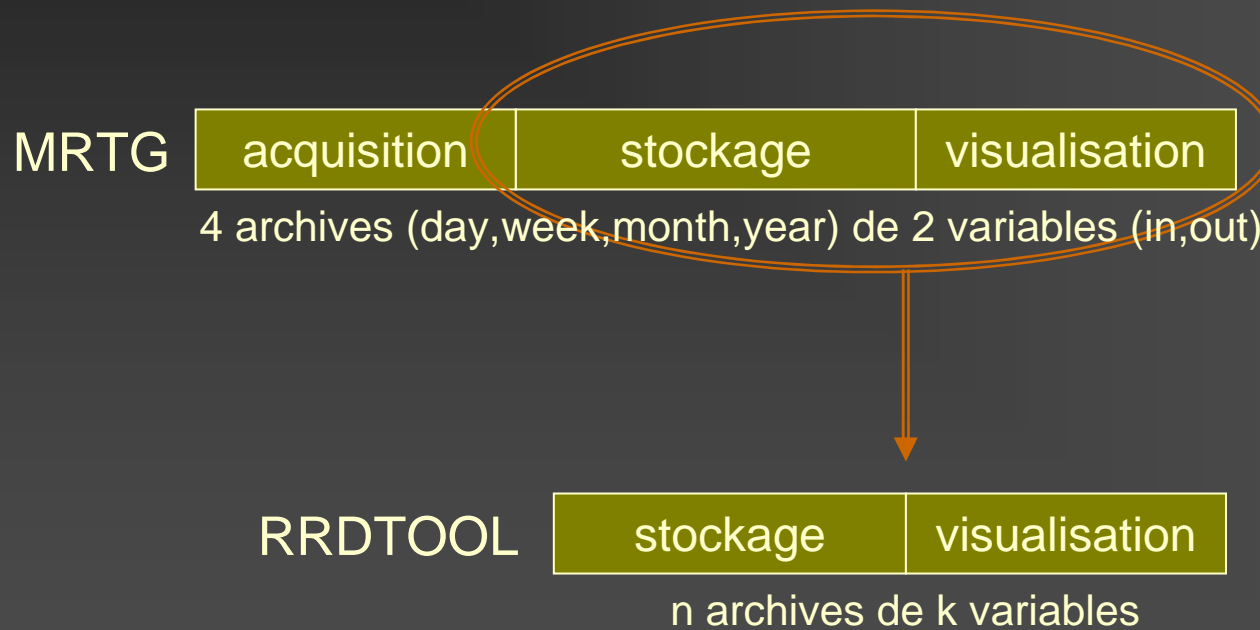


RRDtool

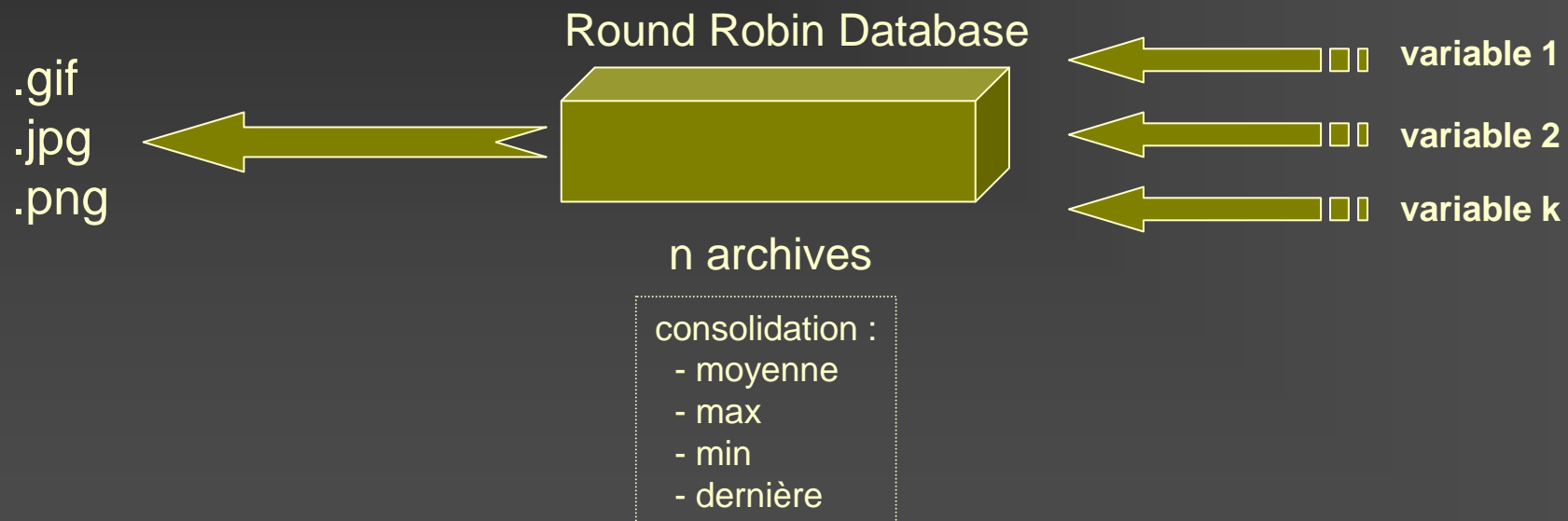
www.rrdtool.com

RRDtool

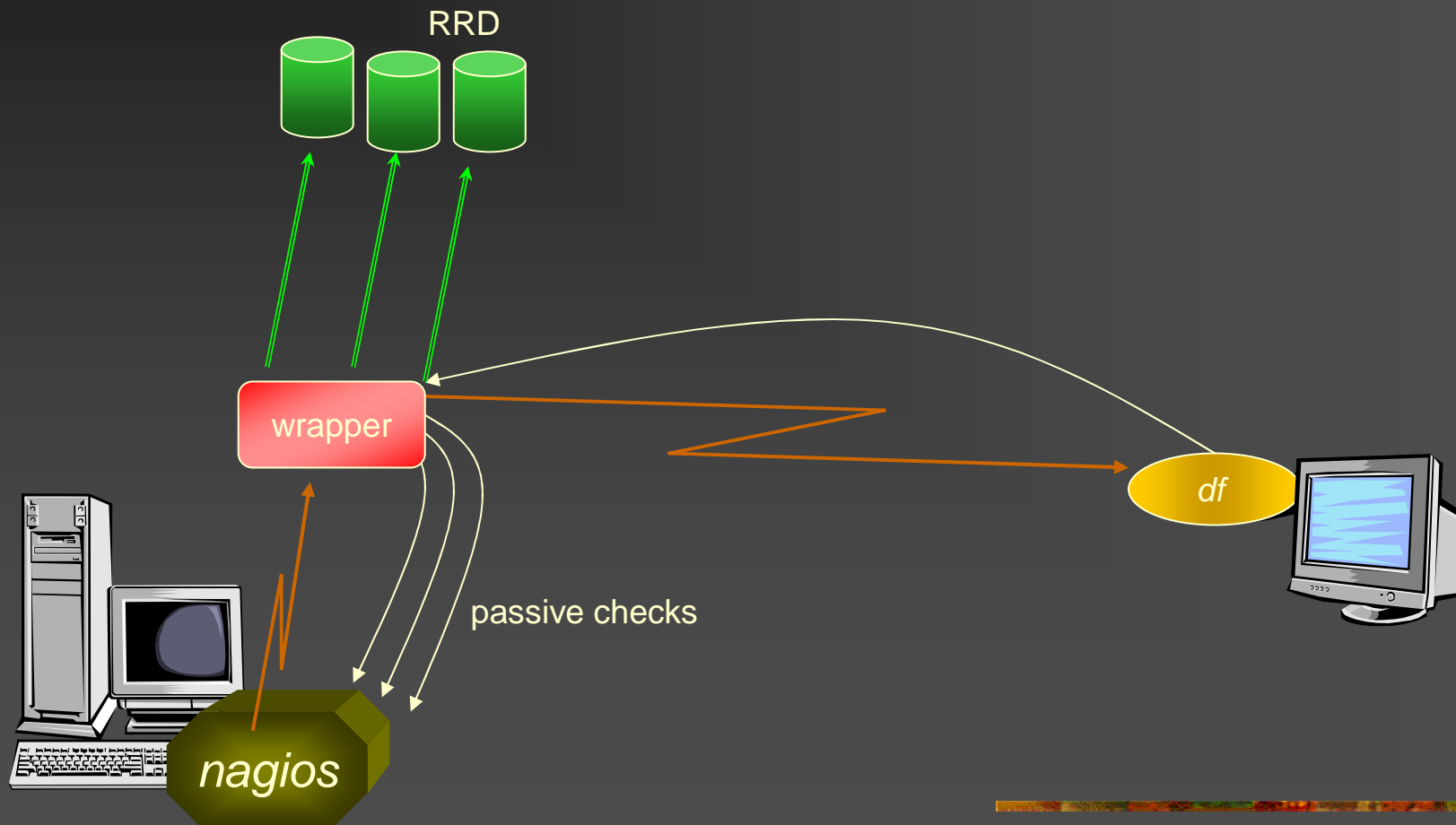
■ successeur de MRTG



principe de RRDtool

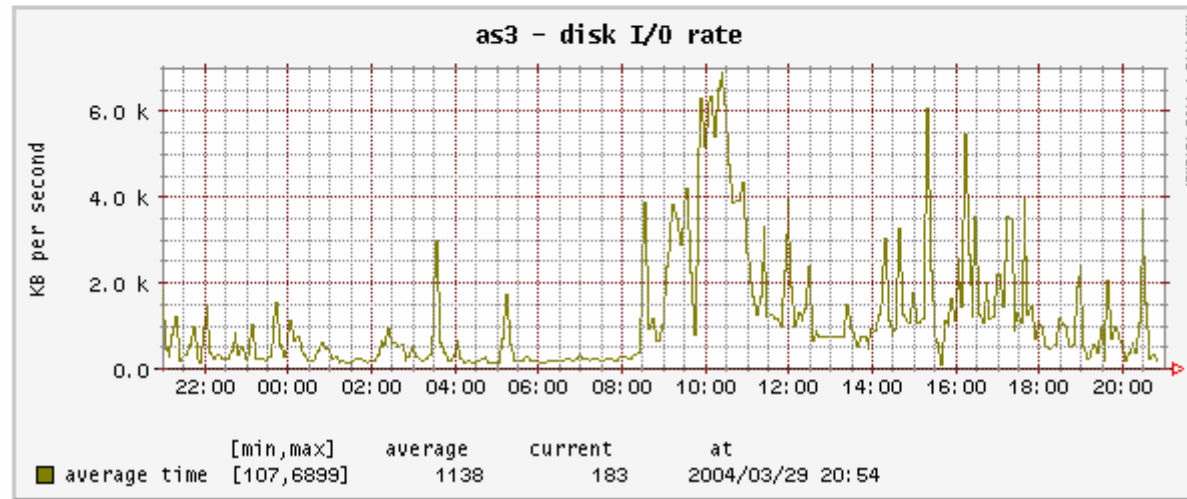
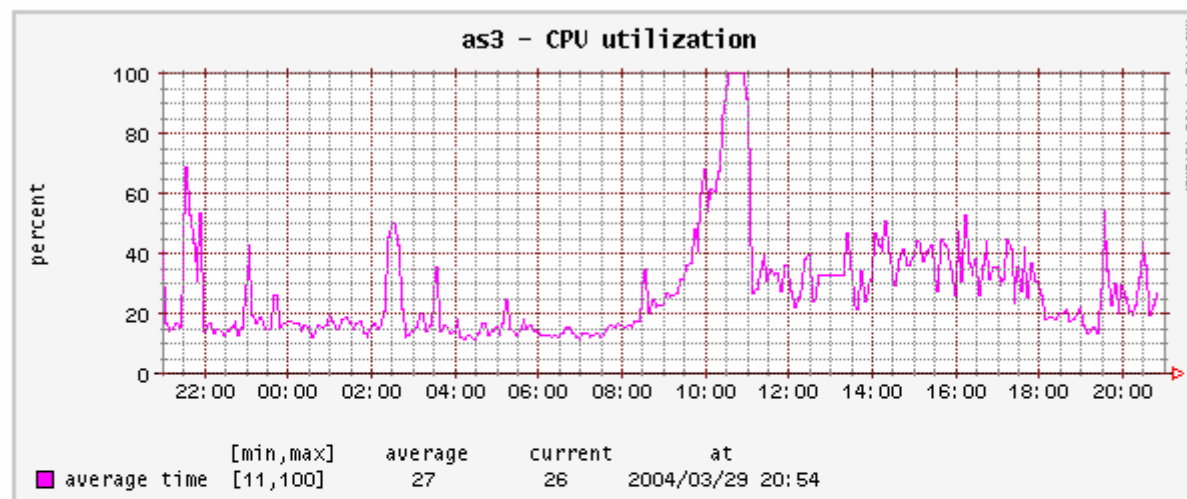


intégration Nagios / RRDtool



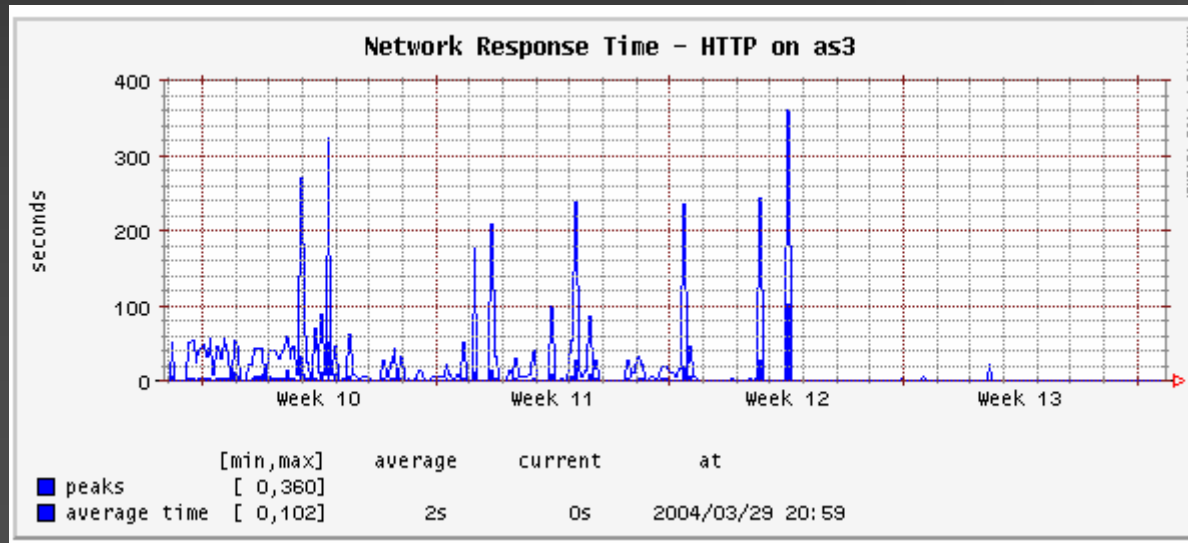
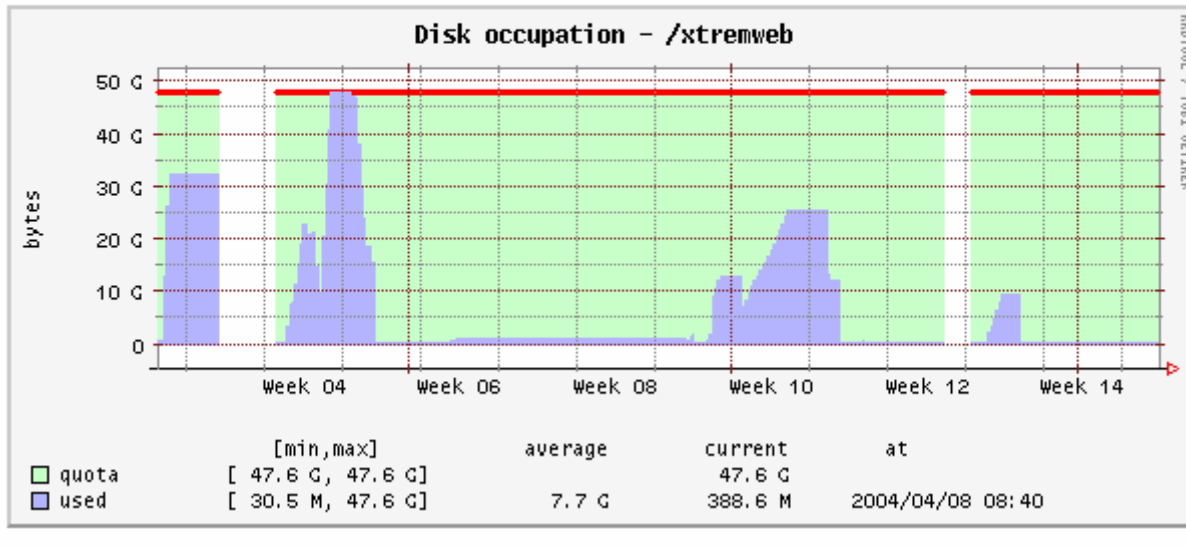
Δx 1 day 1 week 1 month 1 quarter 1 year

graphs ut pg io r15s r1m r15m peaks



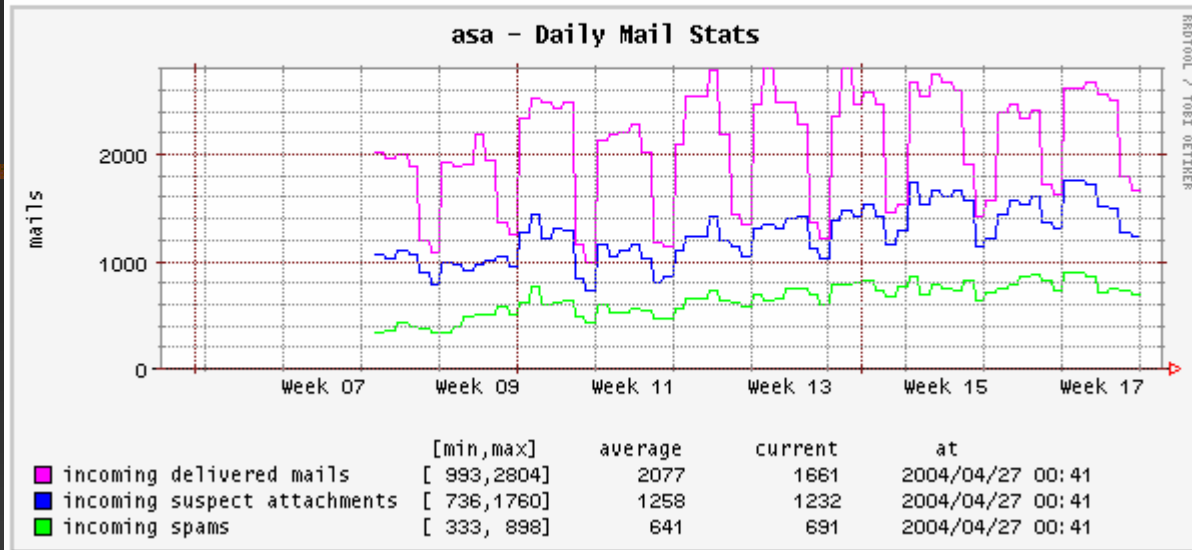
Δx 1 day 1 week 1 month 1 quarter 1 year

O_y zero floating



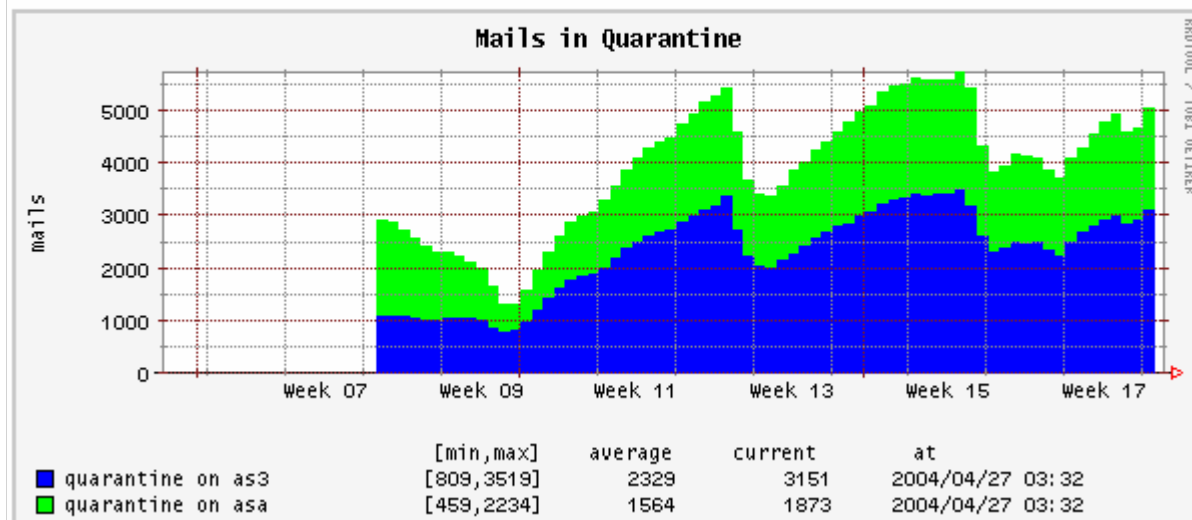
Δx 1 month 1 quarter 1 year

O_y zero floating **graphs** delivered spam cleaned peaks



Δx 1 quarter 1 year

O_y zero floating **graphs** asa as3



- Hourtin du 10 au 14 mai 2004

(Nagios,RRDtool) : conclusions

- combinaison intéressante
- ce qu'il manque
 - pour les administrateurs
 - possibilité de créer des « vues » synthétiques
 - par regroupement (mail, web...)
 - pour les utilisateurs
 - possibilité de créer des « vues » compréhensibles
 - par regroupement (communauté d'utilisateurs)
 - possibilité de commenter et d'expliquer

(Nagios,RRDtool) : conclusions

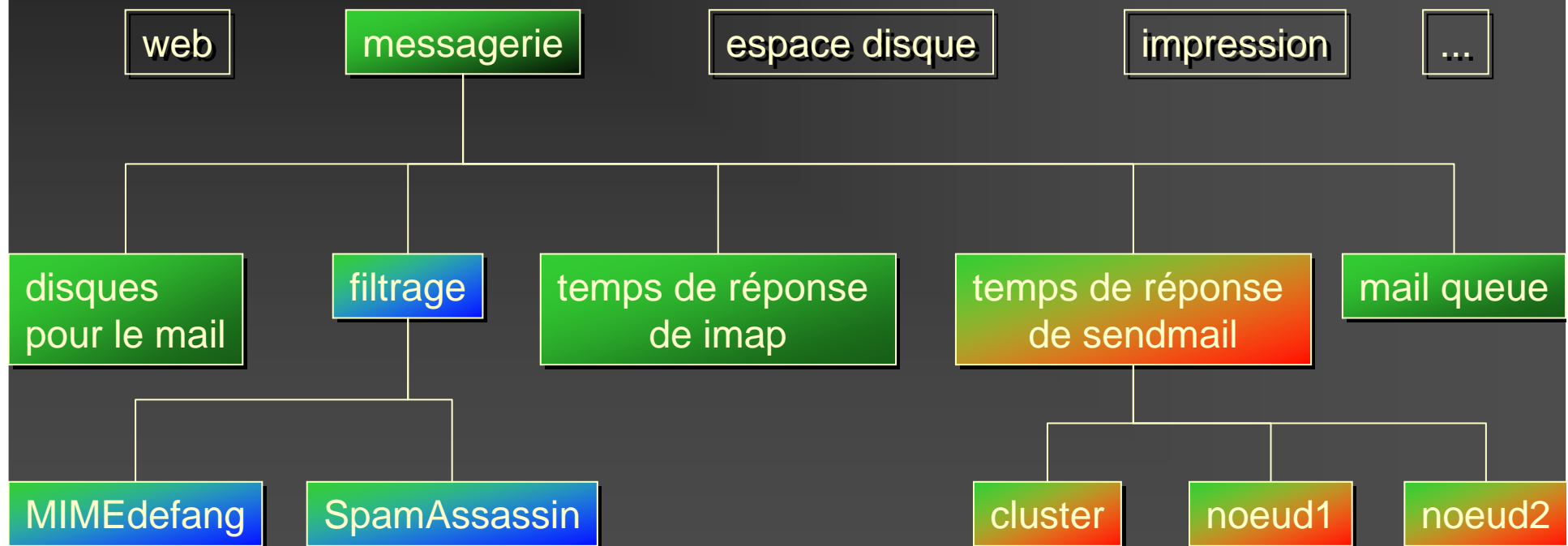
- développement d'une bibliothèque pour faciliter le développement de wrappers :
 - multiplexer l'exécution de plugins sur un ensemble de cibles
 - synthétiser les résultats pour Nagios
 - générer des passives checks
 - alimenter les databases de RRDtool



Générateur de tableaux de bord

Présentation des résultats

- présenter les indicateurs de Nagios en arborescence
 - feuille = service nagios
 - noeud = thème
 - impression
 - file system
- principe
 - $\text{val}(\text{noeud}) = \max(\text{val}(\text{sous-noeuds}))$



Définitions

- 1 noeud est défini par ses fils
- une feuille est définie par
 - le nom du host
 - le nom du service
- une famille de feuilles est définie par
 - une RE identifiant des hosts
 - une RE identifiant des services

exemple

Synthèse
IP inactives

Synthèse

	messagerie: rien à signaler
	web: rien à signaler
	ftp: ok
	login: OK
	cluster Tru64: RAS
	cluster Isf: RAS
	services d'impression: OK
	réseau: RAS
	services sous-jacents: RAS

	vue utilisateur: service dégradé
	exploitation: problème



```
stat(main,
```

```
(mail0,web0,ftp0,login0,cluster0,print0,  
net0,sub0,users0,exploit0),
```

Synthèse
IP inactives

Synthèse

-  messagerie: rien à signaler
-  web: rien à signaler
-  ftp: ok
-  login: OK
-  cluster Tru64: RAS
-  cluster Isf: RAS
-  services d'impression: OK
-  réseau: RAS
-  services sous-jacents: RAS

-  vue utilisateur: service dégradé
-  exploitation: problème

```
stat(mail0,  
  messaging,  
  (disk,filtrage,sendmail,mailq,imap  
    ,quarantine,quarantine_detail),  
  rien à signaler,  
  à surveiller,  
  problème,  
  Oops !,  
)
```

Internet

Adresse <http://super/priv/index.cgi?node=mail0> Liens

Google Recherche Web 181 bloquée(s) Options

monitoring
Synthèse
IP inactives

Synthèse

- espace disque pour le mail: OK [N RRDtool](#)
- filtrage: OK [RRDtool](#)
- sendmail: temps de réponse normaux
- mail en attente: RAS [N RRDtool](#)
- imap: temps de réponse normaux [N](#)
- quarantaine: évolution
- quarantaine: contenu

Terminé Intranet local

```
stat(mail0,  
messaging,  
(disk,filtrage,sendmail,mailq,imap  
,quarantine,quarantine_detail),  
rien à signaler,  
à surveiller,  
problème,  
Oops !,  
)
```

Adresse <http://super/priv/index.cgi?node=filtrage>

Google Recherche Web 181 bloquée(s) Options

monitoring
Synthèse
IP inactives

Synthèse

- MIMEdefang: actif sur as3 [mimedefang-multiplexor: 3 match(es)] **N**
- MIMEdefang: actif sur asa [mimedefang-multiplexor: 4 match(es)] **N**
- spam: filtrage OK sur as3 [1110 spams tagged yesterday] **N**
- spam: filtrage OK sur asa [790 spams tagged yesterday] **N**
- attachements: filtrage OK sur as3 [2629 attachments removed yesterday] **N**
- attachements: filtrage OK sur asa [1659 attachments removed yesterday] **N**

Intranet local

```
stat(spam_report,  
spam,  
(./, '[report] mail spam'),  
filtrage OK,  
peu de spams filtrés hier,  
filtrage inopérant,  
Oops !,  
sur HN PO NA)
```

fini !