Nagios

Jacquelin Charbonnel - Albert Shih

CNRS - Ecole Mathrice 2009

Marseille, 16-20 Novembre 2009

Caractérisation

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

Fonctionnalités

- acquisition d'états
- déclenchement d'actions
  - actions de prévention et de récupération
  - notification via email, pager ou autre
- interface web
  - tableau de bord
  - pour administration (partielle)

Contexte

- logiciel libre
- historique
  - successeur de NetSaint
  - aujourd'hui version 3
- prérequis
  - Unix
  - Apache (recommandé)

Architecture

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

Objets manipulés par Nagios

- cf annexe1 pour une description exhaustive de tous les objets
- cibles du monitoring
  - host
  - service

```
define host {
  host_name                mail-serveur
  alias                    tonton
  address                  192.168.1.254

  check_command            check-host-alive
  check_interval           5
  retry_interval           1
  max_check_attempts       5
  check_period             24x7

  contact_groups           support
  notification_interval 0
  notification_period      24x7
  notification_options     d,u,r
}
```

```
define service {
  service_description   check-disk-sda1
  host_name             mail-server

  check_command         check-disk!/dev/sda1
  max_check_attempts    5
  check_interval        5
  retry_interval        3
  check_period          24x7

  notification_interval 0
  notification_period   24x7
  notification_options  w,c,r
  contact_groups        linux-admins
}
```

Autres objets

- divers
  - contact
  - timeperiod
  - command
- groupes
  - servicegroup
  - hostgroup
  - contactgroup

```
define contact {
  contact_name                    jdoe
  alias                           John Doe
  email                           jdoe@xx.fr

  host_notifications_enabled      1
  host_notification_period        24x7
  host_notification_options       d,u,r
  host_notification_commands      host-notify-by-email

  service_notifications_enabled   1
  service_notification_period     24x7
  service_notification_options    w,u,c,r
  service_notification_commands   notify-by-email
}
```

```
define timeperiod {
  timeperiod_name  repos
  alias            Periode de repos
  sunday           00:00-24:00
  monday           00:00-09:00,17:00-24:00
  tuesday          00:00-09:00,17:00-24:00
  wednesday        00:00-09:00,17:00-24:00
  thursday         00:00-09:00,17:00-24:00
  friday           00:00-09:00,17:00-24:00
  saturday         00:00-24:00
}
```

```
define command {
  command_name  check_pop
  command_line  /usr/local/nagios/libexec/check_pop \
                                        -H $HOSTADDRESS$
}
```

```
define host {
  name                    host-template
  register                0

  check_command           check-host-alive
  check_interval          5
  retry_interval          1
  max_check_attempts      5
  check_period            24x7
  contact_groups          support
  notification_interval   0
  notification_period     24x7
  notification_options    d,u,r
}

define host {
  use                     host-template

  host_name               mail-serveur
  alias                   tonton
  address                 192.168.1.254
}
```

```
define service {
  name                    service-template
  register                0

  max_check_attempts      5
  check_interval          5
  retry_interval          3
  check_period            24x7
  notification_interval   0
  notification_period     24x7
  notification_options    w,c,r
  contact_groups          linux-admins
}

define service {
  use                     service-template

  service_description     check-disk-sda1
  host_name               mail-server
  check_command           check-disk!/dev/sda1
}
```

Etat

- pour un host
  - ok
  - unreachable
    - parent dans le host
  - down
- pour un service
  - ok
  - warning
  - critical
  - unknown

Type d'état

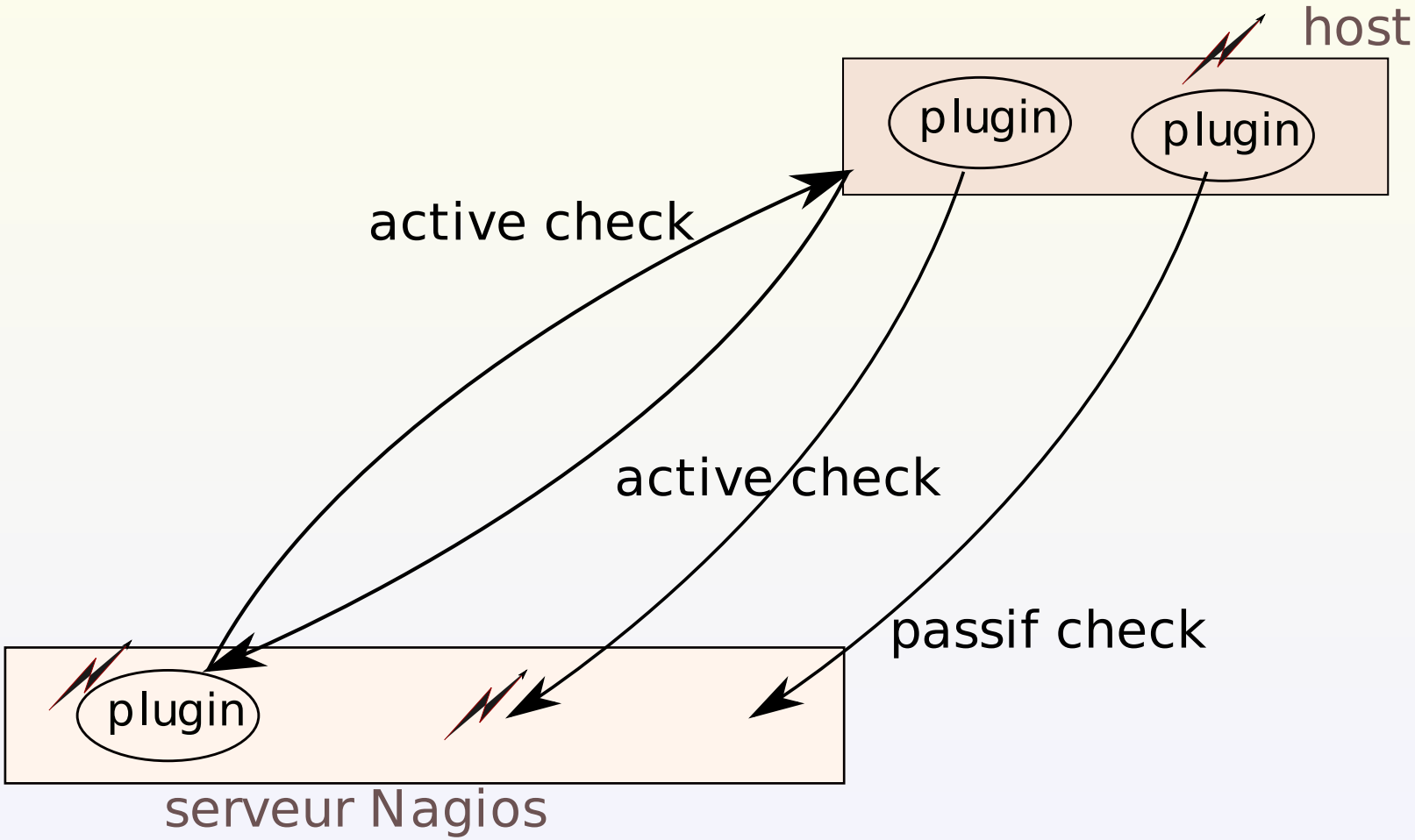
- 2 types d'état
  - soft
    - le problème a été détecté
    - aucune notification n'a encore été émise
    - possibilité d'agir pour éviter les alertes (handler)
  - hard
    - le problème est établi (stable)
    - les notifications sont en cours
    - possibilité d'agir pour réparer (handler)

Séquençage des types d'état

- détection d'un problème
  - (OK,hard) (CRIT,soft) (CRIT,soft) (CRIT,hard)
  - max_check_attempts (ici, c'est 2)
- retour à la normale (RECOVERY)
  - (CRIT,hard) (OK,hard)
  - (CRIT,soft) (OK,soft) (OK,hard)

Check

- active check
  - déclenché par Nagios
  - délégué à un plugin
- passive check
  - déclenchement externe indépendant de Nagios

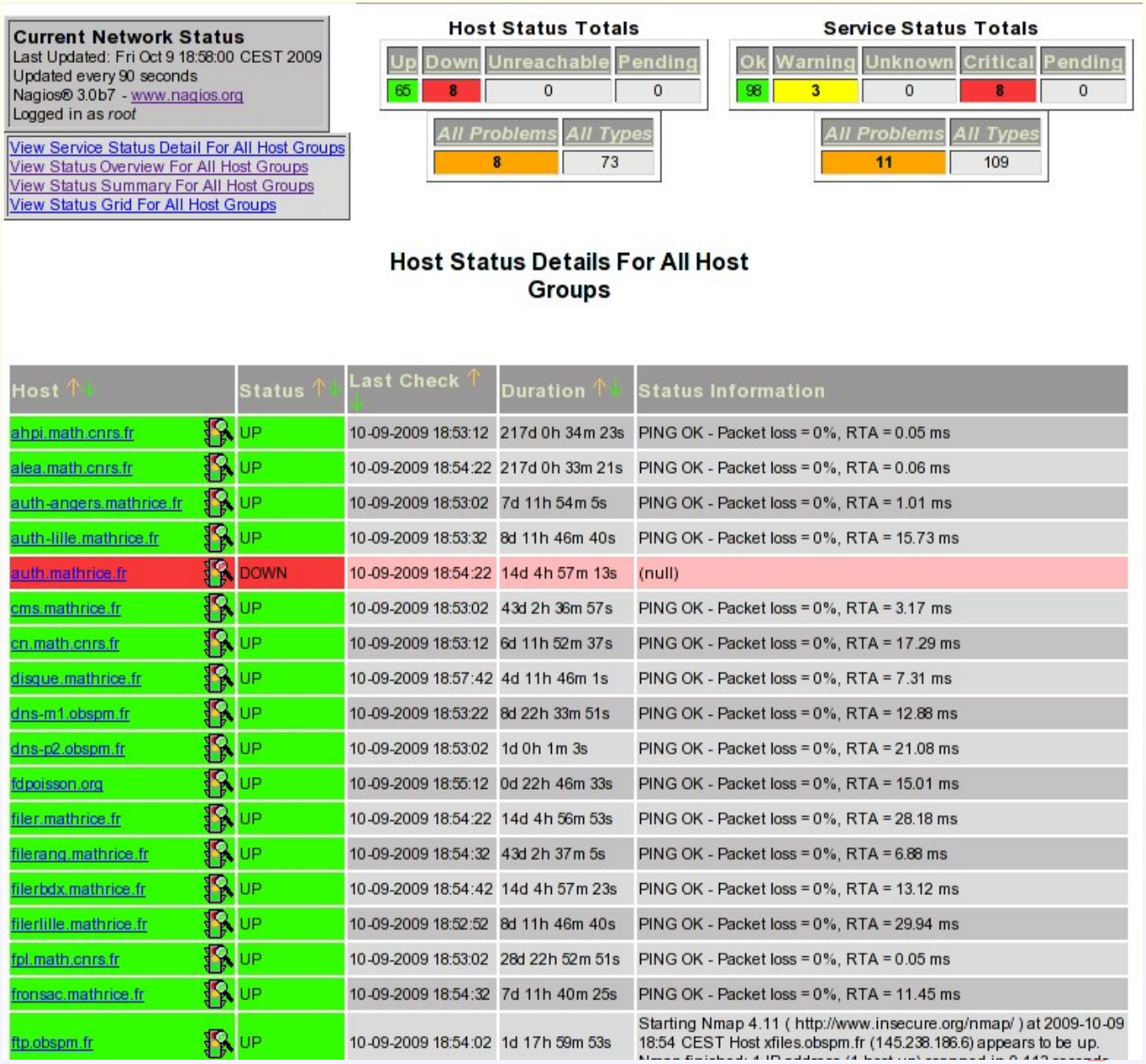

host
plugin
plugin
active check
active check
passif check
plugin
serveur Nagios

Active check

- service check
  - déclenché à interval régulier
    - check_interval et retry_interval définis pour le service
  - à la demande
    - via l'interface web
- host check
  - déclenché à interval régulier
    - check_interval et retry_interval définis pour le host
  - à la demande
    - lorsqu'un service de ce host change d'état
    - pour déterminer l'accessibilité d'un host fils
    - via l'interface web

```
define service {
  host_name                mon_host
  service_description      mon active check
  active_checks_enabled    1
  check_command            ma_commande
  check_interval           5
  retry_interval           3
  check_period             24x7
  ...
  }

define service {
  host_name                 mon_host
  service_description       mon passive check
  passive_checks_enabled    1
  ...
  }
```



Current Network Status
Last Updated: Fri Oct 9 18:58:00 CEST 2009
Updated every 90 seconds
Nagios® 3.0b7 - www.nagios.org
Logged in as *root*

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
65	8	0	0

All Problems	All Types
8	73

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
98	3	0	8	0

All Problems	All Types
11	109

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
ahpi.math.cnrs.fr	UP	10-09-2009 18:53:12	217d 0h 34m 23s	PING OK - Packet loss = 0%, RTA = 0.05 ms
alea.math.cnrs.fr	UP	10-09-2009 18:54:22	217d 0h 33m 21s	PING OK - Packet loss = 0%, RTA = 0.06 ms
auth-angers.mathrice.fr	UP	10-09-2009 18:53:02	7d 11h 54m 5s	PING OK - Packet loss = 0%, RTA = 1.01 ms
auth-lille.mathrice.fr	UP	10-09-2009 18:53:32	8d 11h 46m 40s	PING OK - Packet loss = 0%, RTA = 15.73 ms
auth.mathrice.fr	DOWN	10-09-2009 18:54:22	14d 4h 57m 13s	(null)
cms.mathrice.fr	UP	10-09-2009 18:53:02	43d 2h 36m 57s	PING OK - Packet loss = 0%, RTA = 3.17 ms
cn.math.cnrs.fr	UP	10-09-2009 18:53:12	6d 11h 52m 37s	PING OK - Packet loss = 0%, RTA = 17.29 ms
disque.mathrice.fr	UP	10-09-2009 18:57:42	4d 11h 46m 1s	PING OK - Packet loss = 0%, RTA = 7.31 ms
dns-m1.obspm.fr	UP	10-09-2009 18:53:22	8d 22h 33m 51s	PING OK - Packet loss = 0%, RTA = 12.88 ms
dns-p2.obspm.fr	UP	10-09-2009 18:53:02	1d 0h 1m 3s	PING OK - Packet loss = 0%, RTA = 21.08 ms
fdpoisson.org	UP	10-09-2009 18:55:12	0d 22h 46m 33s	PING OK - Packet loss = 0%, RTA = 15.01 ms
filer.mathrice.fr	UP	10-09-2009 18:54:22	14d 4h 56m 53s	PING OK - Packet loss = 0%, RTA = 28.18 ms
filerang.mathrice.fr	UP	10-09-2009 18:54:32	43d 2h 37m 5s	PING OK - Packet loss = 0%, RTA = 6.88 ms
filerbdx.mathrice.fr	UP	10-09-2009 18:54:42	14d 4h 57m 23s	PING OK - Packet loss = 0%, RTA = 13.12 ms
filerlille.mathrice.fr	UP	10-09-2009 18:52:52	8d 11h 46m 40s	PING OK - Packet loss = 0%, RTA = 29.94 ms
fpl.math.cnrs.fr	UP	10-09-2009 18:53:02	28d 22h 52m 51s	PING OK - Packet loss = 0%, RTA = 0.05 ms
fronsac.mathrice.fr	UP	10-09-2009 18:54:32	7d 11h 40m 25s	PING OK - Packet loss = 0%, RTA = 11.45 ms
ftp.obspm.fr	UP	10-09-2009 18:54:02	1d 17h 59m 53s	Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-10-09 18:54 CEST Host xfiles.obspm.fr (145.238.186.6) appears to be up.

Current Network Status
Last Updated: Fri Oct 9 18:59:59 CEST 2009
Updated every 90 seconds
Nagios® 3.0b7 - www.nagios.org
Logged in as *root*

View Service Status Detail For All Host Groups
View Host Status Detail For This Host Group
View Status Overview For This Host Group
View Status Summary For This Host Group
View Status Grid For This Host Group

Host Status Totals

Up	Down	Unreachable	Pending
43	4	0	0

All Problems	All Types
4	47

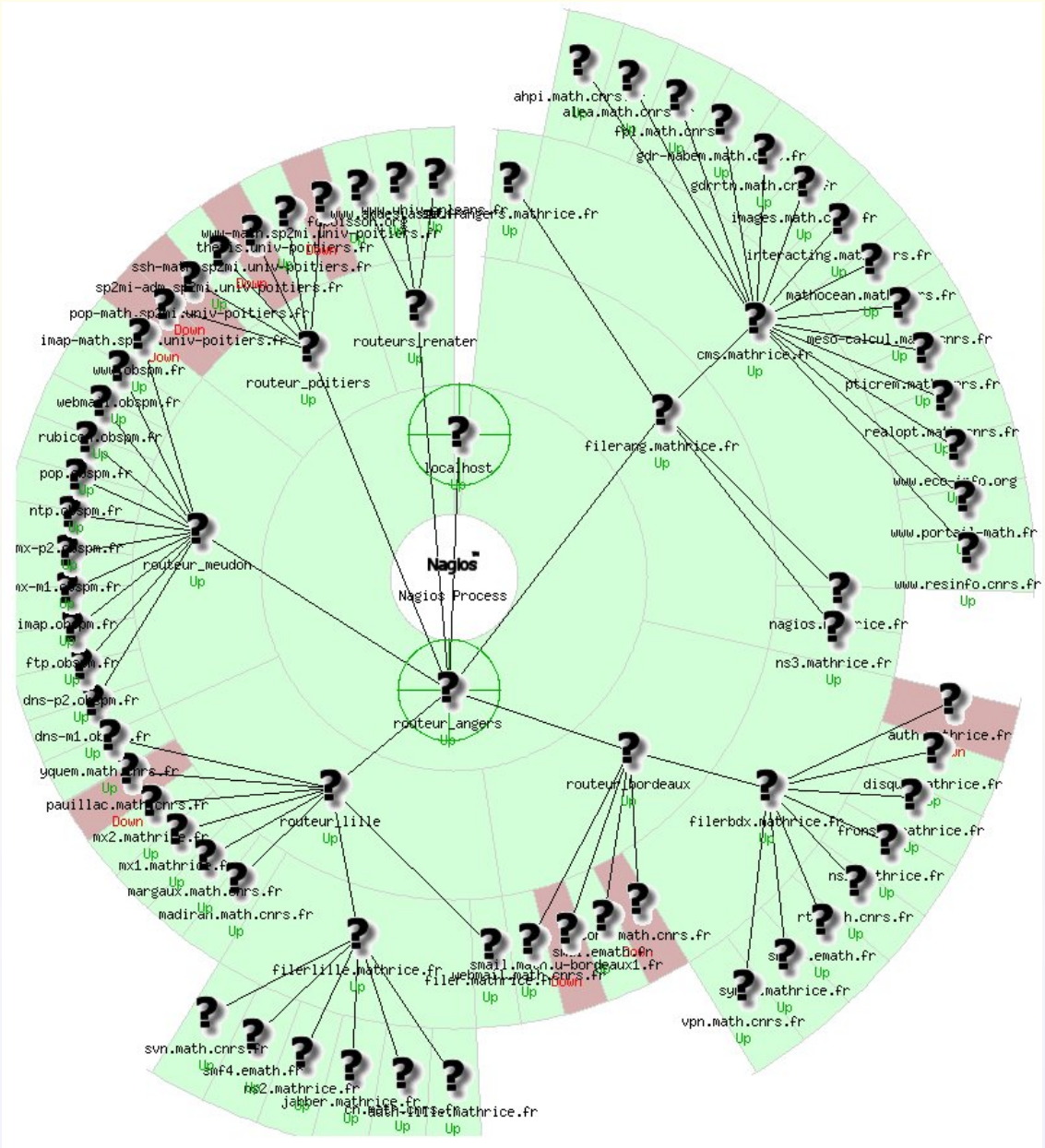
Service Status Totals

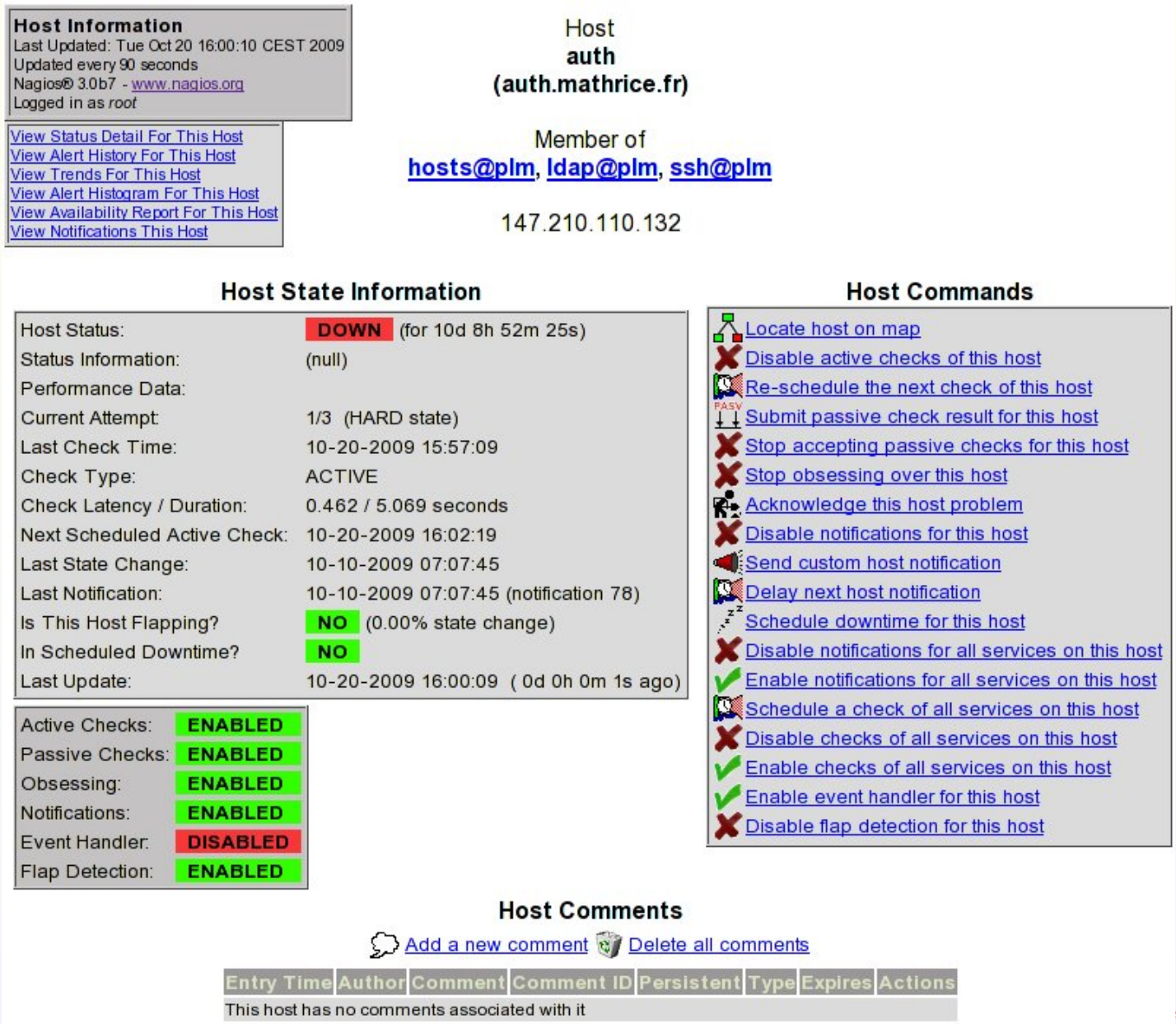
Ok	Warning	Unknown	Critical	Pending
60	2	0	7	0

All Problems	All Types
9	69

Service Status Details For Host Group 'hosts@plm'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ahpi.math.cnrs.fr	http vhost@plm	OK	10-09-2009 18:48:01	8d 11h 42m 51s	1/3	HTTP OK HTTP/1.1 200 OK - 0.088 second response time
alea.math.cnrs.fr	http vhost@plm	CRITICAL	10-09-2009 18:48:00	219d 4h 56m 56s	3/3	CRITICAL - pattern not found
auth-angers.mathrice.fr	ldap@plm	OK	10-09-2009 18:54:44	43d 2h 17m 58s	1/3	TCP OK - 0.061 second response time on port 389
	ssh@plm	OK	10-09-2009 18:48:36	7d 11h 56m 23s	1/3	SSH OK - OpenSSH_4.3 (protocol 2.0)
auth-lille.mathrice.fr	ldap@plm	OK	10-09-2009 18:49:42	8d 3h 40m 17s	1/3	TCP OK - 0.035 second response time on port 389
auth.mathrice.fr	ldap@plm	OK	10-09-2009 18:48:00	29d 12h 43m 23s	1/3	TCP OK - 0.055 second response time on port 389
	ssh@plm	CRITICAL	10-09-2009 18:57:53	234d 6h 41m 14s	1/3	CRITICAL - Socket timeout after 10 seconds
	tcp9009@plm	OK	10-09-2009 18:48:05	26d 12h 27m 33s	1/3	TCP OK - 0.016 second response time on port 9009
cms.mathrice.fr	http@plm	OK	10-09-2009 18:58:37	5d 20h 31m 23s	1/3	HTTP OK HTTP/1.1 200 OK - 27000 bytes in 0.133 seconds
	ssh@plm	OK	10-09-2009 18:48:05	43d 2h 27m 22s	1/3	SSH OK - OpenSSH_4.3 (protocol 2.0)
cn.math.cnrs.fr	http@plm	OK	10-09-2009 18:59:38	10d 4h 15m 29s	1/3	HTTP OK HTTP/1.1 200 OK - 6896 bytes in 0.066 seconds
	https@plm	OK	10-09-2009 18:54:39	11d 2h 51m 58s	1/3	TCP OK - 0.069 second response time on port 443
disque.mathrice.fr	http@plm	WARNING	10-09-2009 18:57:53	0d 4h 2m 6s	3/3	HTTP WARNING: HTTP/1.1 404 Not Found
	https@plm	OK	10-09-2009 18:51:46	37d 12h 53m 34s	1/3	TCP OK - 0.007 second response time on port 443
	ssh@plm	OK	10-09-2009 18:50:19	4d 11h 54m 40s	1/3	SSH OK - OpenSSH_5.1p1 FreeBSD-openssh-portable-5.1.p1,1 (protocol 2.0)
filer.mathrice.fr	ssh@plm	CRITICAL	10-09-2009 18:59:38	234d 6h 40m 20s	3/3	CRITICAL - Socket timeout after 10 seconds
filerang.mathrice.fr	http@plm	CRITICAL	10-09-2009 18:48:06	193d 1h 26m 37s	3/3	No route to host
	ssh22000@plm	CRITICAL	10-09-2009 18:57:53	193d 1h 19m 25s	3/3	No route to host
filerbdx.mathrice.fr	ssh@plm	OK	10-09-2009 18:54:39	16d 17h 50m 58s	1/3	SSH OK - OpenSSH_4.3 (protocol 2.0)


Nagios
Nagios Process
localhost
routeur_angers
routeur_meudon
routeur_poitiers
routeurs.renater
filerang.mathrice.fr
cms.mathrice.fr
routeur_lille
routeur_bordeaux
filerlille.mathrice.fr
filerbdx.mathrice.fr
ns3.mathrice.fr
vpn.math.cnrs.fr
svn.math.cnrs.fr
Up
Down



Host Information
Last Updated: Tue Oct 20 16:00:10 CEST 2009
Updated every 90 seconds
Nagios® 3.0b7 - www.nagios.org
Logged in as *root*

View Status Detail For This Host
View Alert History For This Host
View Trends For This Host
View Alert Histogram For This Host
View Availability Report For This Host
View Notifications This Host

Host
auth
(auth.mathrice.fr)

Member of
hosts@plm, **ldap@plm**, **ssh@plm**

147.210.110.132

Host State Information

Host Status:	DOWN (for 10d 8h 52m 25s)
Status Information:	(null)
Performance Data:	
Current Attempt:	1/3 (HARD state)
Last Check Time:	10-20-2009 15:57:09
Check Type:	ACTIVE
Check Latency / Duration:	0.462 / 5.069 seconds
Next Scheduled Active Check:	10-20-2009 16:02:19
Last State Change:	10-10-2009 07:07:45
Last Notification:	10-10-2009 07:07:45 (notification 78)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-20-2009 16:00:09 (0d 0h 0m 1s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

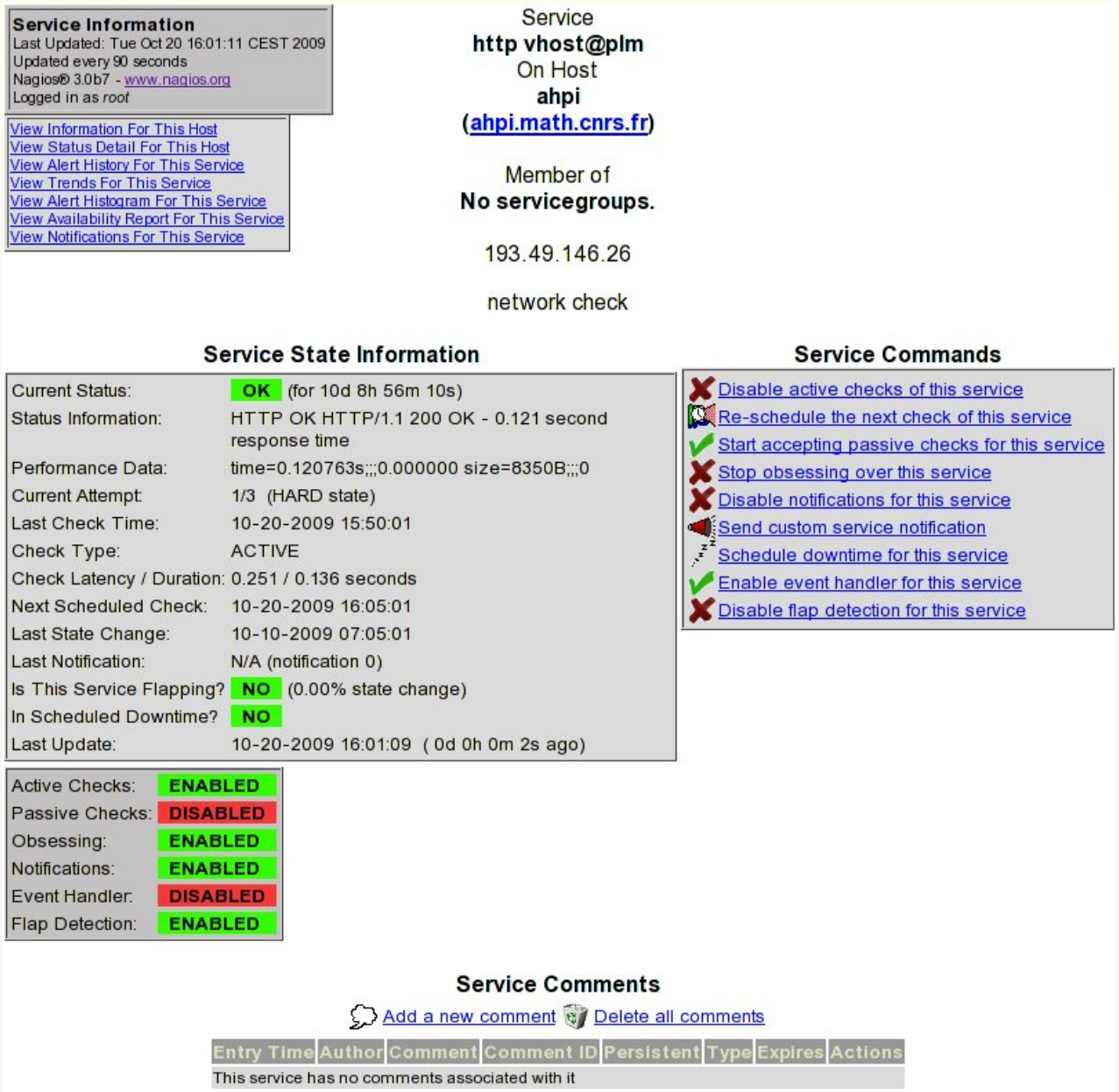
Host Commands

Locate host on map
Disable active checks of this host
Re-schedule the next check of this host
Submit passive check result for this host
Stop accepting passive checks for this host
Stop obsessing over this host
Acknowledge this host problem
Disable notifications for this host
Send custom host notification
Delay next host notification
Schedule downtime for this host
Disable notifications for all services on this host
Enable notifications for all services on this host
Schedule a check of all services on this host
Disable checks of all services on this host
Enable checks of all services on this host
Enable event handler for this host
Disable flap detection for this host

Host Comments

Add a new comment Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This host has no comments associated with it							



Service Information
Last Updated: Tue Oct 20 16:01:11 CEST 2009
Updated every 90 seconds
Nagios® 3.0b7 - www.nagios.org
Logged in as *root*

View Information For This Host
View Status Detail For This Host
View Alert History For This Service
View Trends For This Service
View Alert Histogram For This Service
View Availability Report For This Service
View Notifications For This Service

Service
http vhost@plm
On Host
ahpi
(ahpi.math.cnrs.fr)

Member of
No servicegroups.

193.49.146.26

network check

Service State Information

Current Status:	OK (for 10d 8h 56m 10s)
Status Information:	HTTP OK HTTP/1.1 200 OK - 0.121 second response time
Performance Data:	time=0.120763s;;;0.000000 size=8350B;;;0
Current Attempt:	1/3 (HARD state)
Last Check Time:	10-20-2009 15:50:01
Check Type:	ACTIVE
Check Latency / Duration:	0.251 / 0.136 seconds
Next Scheduled Check:	10-20-2009 16:05:01
Last State Change:	10-10-2009 07:05:01
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-20-2009 16:01:09 (0d 0h 0m 2s ago)

Service Commands

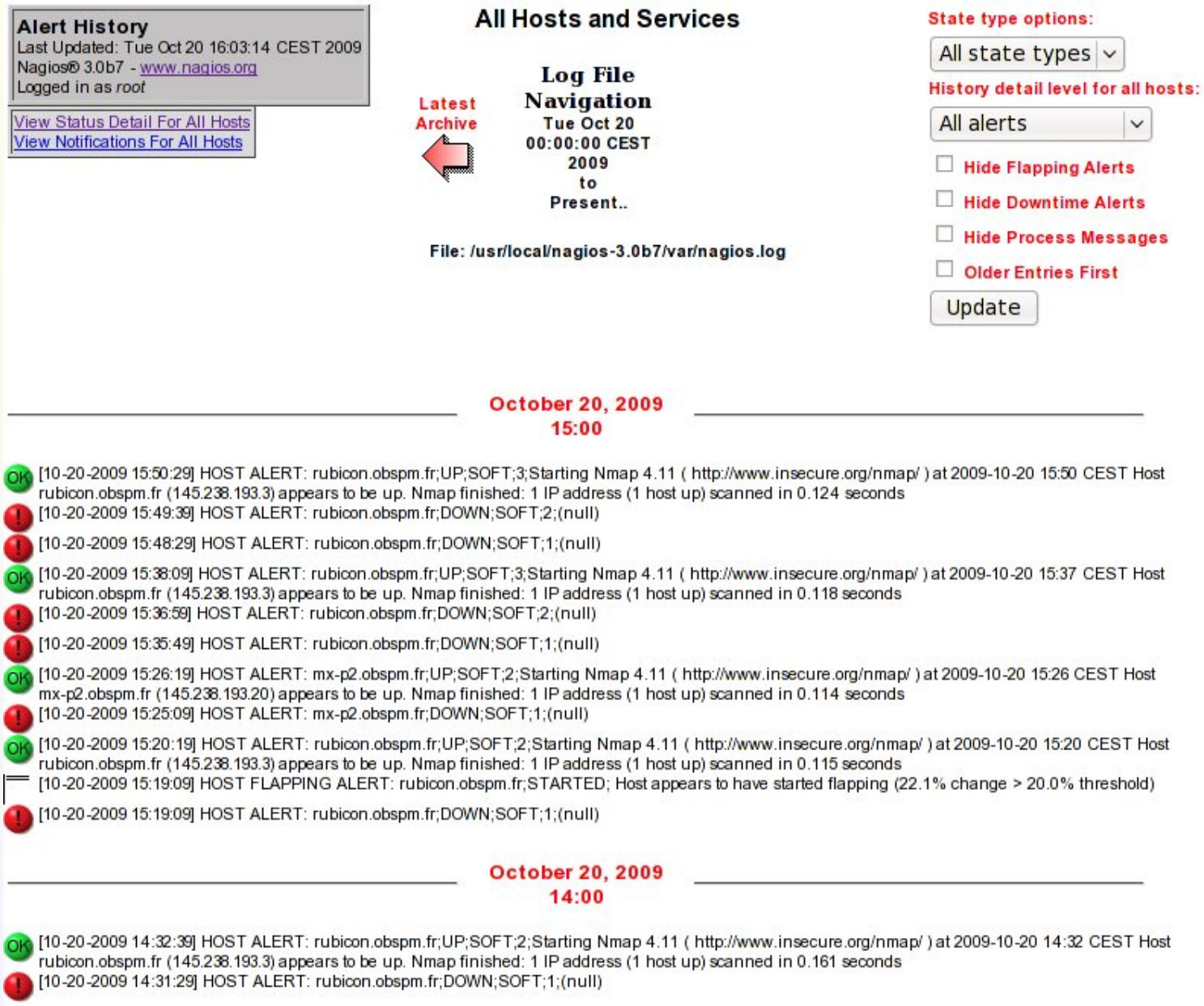
Disable active checks of this service
Re-schedule the next check of this service
Start accepting passive checks for this service
Stop obsessing over this service
Disable notifications for this service
Send custom service notification
Schedule downtime for this service
Enable event handler for this service
Disable flap detection for this service

Active Checks:	ENABLED
Passive Checks:	DISABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	DISABLED
Flap Detection:	ENABLED

Service Comments

Add a new comment Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This service has no comments associated with it							



Alert History
Last Updated: Tue Oct 20 16:03:14 CEST 2009
Nagios® 3.0b7 - www.nagios.org
Logged in as *root*

View Status Detail For All Hosts
View Notifications For All Hosts

All Hosts and Services

Latest Archive

Log File Navigation
Tue Oct 20 00:00:00 CEST 2009 to Present..

File: /usr/local/nagios-3.0b7/var/nagios.log

State type options:
All state types

History detail level for all hosts:
All alerts

- Hide Flapping Alerts
- Hide Downtime Alerts
- Hide Process Messages
- Older Entries First

Update

October 20, 2009 15:00

[10-20-2009 15:50:29] HOST ALERT: rubicon.obspm.fr;UP;SOFT;3;Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-10-20 15:50 CEST Host rubicon.obspm.fr (145.238.193.3) appears to be up. Nmap finished: 1 IP address (1 host up) scanned in 0.124 seconds
[10-20-2009 15:49:39] HOST ALERT: rubicon.obspm.fr;DOWN;SOFT;2;(null)
[10-20-2009 15:48:29] HOST ALERT: rubicon.obspm.fr;DOWN;SOFT;1;(null)
[10-20-2009 15:38:09] HOST ALERT: rubicon.obspm.fr;UP;SOFT;3;Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-10-20 15:37 CEST Host rubicon.obspm.fr (145.238.193.3) appears to be up. Nmap finished: 1 IP address (1 host up) scanned in 0.118 seconds
[10-20-2009 15:36:59] HOST ALERT: rubicon.obspm.fr;DOWN;SOFT;2;(null)
[10-20-2009 15:35:49] HOST ALERT: rubicon.obspm.fr;DOWN;SOFT;1;(null)
[10-20-2009 15:26:19] HOST ALERT: mx-p2.obspm.fr;UP;SOFT;2;Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-10-20 15:26 CEST Host mx-p2.obspm.fr (145.238.193.20) appears to be up. Nmap finished: 1 IP address (1 host up) scanned in 0.114 seconds
[10-20-2009 15:25:09] HOST ALERT: mx-p2.obspm.fr;DOWN;SOFT;1;(null)
[10-20-2009 15:20:19] HOST ALERT: rubicon.obspm.fr;UP;SOFT;2;Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-10-20 15:20 CEST Host rubicon.obspm.fr (145.238.193.3) appears to be up. Nmap finished: 1 IP address (1 host up) scanned in 0.115 seconds
[10-20-2009 15:19:09] HOST FLAPPING ALERT: rubicon.obspm.fr;STARTED; Host appears to have started flapping (22.1% change > 20.0% threshold)
[10-20-2009 15:19:09] HOST ALERT: rubicon.obspm.fr;DOWN;SOFT;1;(null)

October 20, 2009 14:00

[10-20-2009 14:32:39] HOST ALERT: rubicon.obspm.fr;UP;SOFT;2;Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-10-20 14:32 CEST Host rubicon.obspm.fr (145.238.193.3) appears to be up. Nmap finished: 1 IP address (1 host up) scanned in 0.161 seconds
[10-20-2009 14:31:29] HOST ALERT: rubicon.obspm.fr;DOWN;SOFT;1;(null)

Notification

- envoyée lors d'un changement d'état
- si le nouvel état est de type hard
- à chaque host et à chaque service est associé un contact ou contactgroup
  - ce sont les destinataires potentiels des alertes
  - encore faut-il passer les filtres
    - notification_options du host ou du service
    - notification_period du host ou du service
    - notification_options du contact
    - notification_period du contact

```
test d'1 service
si probleme
alors test du host
  si probleme
  alors envoi d'1 seule notification relative a ce host
  sinon envoi d'1 notification relative au service
```

```
cfg_file=/usr/local/nagios/etc/hosts.cfg
cfg_file=/usr/local/nagios/etc/services.cfg
cfg_file=/usr/local/nagios/etc/commands.cfg

cfg_dir=/usr/local/nagios/etc/commands
cfg_dir=/usr/local/nagios/etc/services
cfg_dir=/usr/local/nagios/etc/hosts

resource_file=/usr/local/nagios/etc/resource.cfg
status_file=/usr/local/nagios/var/status.dat

nagios_user=nagios
nagios_group=nagios

enable_notifications=1
execute_service_checks=1
accept_passive_service_checks=1
execute_host_checks=1
accept_passive_host_checks=1
enable_event_handlers=1
check_service_freshness=0
check_host_freshness=0

sleep_time=1
max_concurrent_checks=20
service_check_timeout=60
host_check_timeout=60
event_handler_timeout=60

enable_flap_detection=0
```

check_apt	check_flexlm	check_log	check_oracle	check_ssmtp
check_breeze	check_ftp	check_mailq	check_overcr	check_swap
check_by_ssh	check_http	check_mrtg	check_ping	check_tcp
check_clamd	check_icmp	check_mrtgtraf	check_pop	check_time
check_cluster	check_ide_smart	check_nagios	check_procs	check_udp
check_dhcp	check_ifoperstatus	check_nntp	check_real	check_ups
check_dig	check_ifstatus	check_nntps	check_rpc	check_users
check_disk	check_imap	check_nt	check_sensors	check_wave
check_disk_smb	check_ircd	check_ntp	check_simap	negate
check_dns	check_jabber	check_ntp_peer	check_smtp	urlize
check_dummy	check_ldap.pl	check_ntp_time	check_spop	utils.pm
check_file_age	check_load	check_nwstat	check_ssh	utils.sh

```
# ./check_tcp --help

This plugin tests TCP connections with the specified host (or unix socket).

Usage:check_tcp -H host -p port [-w <warning time>] [-c <critical time>]
        [-s <send string>] [-e <expect string>] [-q <quit string>]
[-m <maximum bytes>] [-d <delay>] [-t <timeout seconds>]
[-r <refuse state>] [-M <mismatch state>] [-v] [-4|-6] [-j]
[-D <days to cert expiry>] [-S <use SSL>] [-E]

# ./check_tcp -H cms.mathrice.fr -p 80
TCP OK - 0.002 second response time on port 80|time=0.002370s;;;0.000000;10.000000

# echo $?
0

# ./check_tcp -H cms.mathrice.fr -p 81
CRITICAL - Socket timeout after 10 seconds

# echo $?
2
```

```
# ./check_rpc --help

Check if a rpc service is registered and running using
      rpcinfo -H host -C rpc_command

Usage:
 check_rpc -H host -C rpc_command [-p port] [-c program_version] [-u|-t] [-v]
 check_rpc [-h | --help]
 check_rpc [-V | --version]

  <host>           The server providing the rpc service
  <rpc_command>    The program name (or number).
  <program_version> The version you want to check for (one or more)
                    Should prevent checks of unknown versions being syslogged
                    e.g. 2,3,6 to check v2, v3, and v6
  [-u | -t]        Test UDP or TCP
  [-v]             Verbose
  [-v -v]          Verbose - will print supported programs and numbers

# ./check_rpc -C nfs -H nfssrv.math
OK: RPC program nfs version 2 version 3 version 4 udp running

# echo $?
0
```

```
# check_http --help

This plugin tests the HTTP service on the specified host. It can test
normal (http) and secure (https) servers, follow redirects, search for
strings and regular expressions, check connection times, and report on
certificate expiration times.

Usage: check_http -H <vhost> | -I <IP-address> [-u <uri>] [-p <port>]
       [-w <warn time>] [-c <critical time>] [-t <timeout>] [-L]
       [-a auth] [-f <ok | warn | critcal | follow | sticky | stickyport>]
       [-e <expect>] [-s string] [-l] [-r <regex> | -R <case-insensitive regex>]
       [-P string] [-m <min_pg_size>:<max_pg_size>] [-4|-6] [-N] [-M <age>]
       [-A string] [-k string] [-S] [-C <age>] [-T <content-type>] [-j method]
NOTE: One or both of -H and -I must be specified

# check_http -I math.cnrs.fr
HTTP OK: HTTP/1.1 200 OK - 26999 bytes in 0.235 second response time | time=0.235475s;;;0.000000 size=26999B;;;0

# echo $?
0

# host math.cnrs.fr
math.cnrs.fr has address 193.49.146.26

# host 193.49.146.26
26.146.49.193.in-addr.arpa domain name pointer bonnezeaux.math.univ-angers.fr.

# host bonnezeaux.math.univ-angers.fr
bonnezeaux.math.univ-angers.fr has address 193.49.146.26
bonnezeaux.math.univ-angers.fr has IPv6 address 2001:660:7201:409::2600
```


http://www.math.cnrs.fr/
math.cnrs.fr : le domaine ...
math.cnrs.fr
Le domaine des laboratoires de mathématiques du CNRS
Des liens vers l'INSMI
Des annuaires
Groupe Calcul et autres ressources informatiques
Ressources documentaires
Aides à la coopération internationale
Le Café des Mathématiques
Images des Mathématiques
Institutions françaises
Institutions internationales
Unités et lieux de recherche
Groupements de recherche
Fédérations de recherche
Unités et groupements de service
http://bonnezeaux.math.univ-angers.fr/
Mathrice GDS CNRS 2754
Mathrice GDS CNRS 2754
Composante Angevine
Le CNRS | Université d'Angers | Mathrice | Larema |
Plateforme d'hébergement de sites web
Sites hébergés :
ahpi.math.cnrs.fr
alea.math.cnrs.fr
cethop.math.cnrs.fr
cmsmsa.mathrice.fr
ergodic2009.math.cnrs.fr
fpl.math.cnrs.fr [https]

```
# check_http --help

This plugin tests the HTTP service on the specified host. It can test
normal (http) and secure (https) servers, follow redirects, search for
strings and regular expressions, check connection times, and report on
certificate expiration times.

Usage: check_http -H <vhost> | -I <IP-address> [-u <uri>] [-p <port>]
       [-w <warn time>] [-c <critical time>] [-t <timeout>] [-L]
       [-a auth] [-f <ok | warn | critcal | follow | sticky | stickyport>]
       [-e <expect>] [-s string] [-l] [-r <regex> | -R <case-insensitive regex>]
       [-P string] [-m <min_pg_size>:<max_pg_size>] [-4|-6] [-N] [-M <age>]
       [-A string] [-k string] [-S] [-C <age>] [-T <content-type>] [-j method]
NOTE: One or both of -H and -I must be specified

# check_http -H bonnezeaux.math.univ-angers.fr -R "math.*matique"
HTTP CRITICAL: HTTP/1.1 200 OK - pattern not found - 27092 bytes in 3.817 second response time |
time=3.816504s;;;0.000000 size=27092B;;;0

# echo $?
2

# check_http -H math.cnrs.fr -R "math.*matique"
HTTP OK: HTTP/1.1 200 OK - 4749 bytes in 0.009 second response time |
time=0.008764s;;;0.000000 size=4749B;;;0

# echo $?
0
```

solution 1:

```
define command {
  command_name  check_vh_math_cnrs
  command_line  /plugins/check_http -I $HOSTADDRESS$ -H math.cnrs.fr -R "math.*matique"
}

define service {
  host_name             math.cnrs.fr
  service_description   check-vh-math-cnrs
  check_command         check_vh_math_cnrs
  ...
}
```

solution 2:

```
define command {
  command_name  check_vh
  command_line  /plugins/check_http -I $HOSTADDRESS$ -H $ARG1$ -R "$ARG2$"
}

define service {
  host_name             math.cnrs.fr
  service_description   check-vh-math-cnrs
  check_command         check_vh!math.cnrs.fr!math.*matique
  ...
}
```

```
# ./check_procs --help

Checks all processes and generates WARNING or CRITICAL states if the specified
metric is outside the required threshold ranges. The metric defaults to number
of processes.  Search filters can be applied to limit the processes to check.

Usage: check_procs -w <range> -c <range> [-m metric] [-s state] [-p ppid]
 [-u user] [-r rss] [-z vsz] [-P %cpu] [-a argument-array]
 [-C command] [-t timeout] [-v]

# ./check_procs -C crond -c 1:1;echo $?
PROCS OK: 1 process with command name 'crond'
0

# ./check_procs -C crond -c 1:1;echo $?
PROCS CRITICAL: 0 processes with command name 'crond'
2
```

```
# ./check_by_ssh --help

This plugin uses SSH to execute commands on a remote host

Usage: check_by_ssh -H <host> -C <command> [-fqv] [-1|-2] [-4|-6]
       [-S [lines]] [-E [lines]] [-t timeout] [-i identity]
       [-l user] [-n name] [-s servicelist] [-O outputfile]
       [-p port] [-o ssh-option]

# ./check_by_ssh -H nfssrv.math -C "check_procs -C crond -c 1:1"
PROCS OK: 1 process with command name 'crond'

# ./check_by_ssh -H nfssrv.math -C true ; echo $?
OK - check_by_ssh: Remote command 'true' returned status 0
0

# ./check_by_ssh -H nfssrv.math -C false ; echo $?
WARNING - check_by_ssh: Remote command 'false' returned status 1
1

# ./check_by_ssh -H nfssrv.math -C "exit 2" ; echo $?
CRITICAL - check_by_ssh: Remote command 'exit 2' returned status 2
2

# ./check_by_ssh -H nfssrv.math -C nimportequoi ; echo $?
Remote command execution failed: bash: nimportequoi: command not found
3
```

```
# ./check_dummy --help

This plugin will simply return the state corresponding to t
of the <state> argument with optional text

Usage: check_dummy <integer state> [optional text]

# ./check_dummy 0 "ma sortie de plugin" ; echo $?
OK: ma sortie de plugin
0
# ./check_dummy 2 "my plugin output" ; echo $?
CRITICAL: my plugin output
2
```

```
# ./negate --help

Negates the status of a plugin (returns OK for CRITICAL and vice-versa).
Additional switches can be used to control which state becomes what.

Usage:negate [-t timeout] [-Towcu STATE] [-s] <definition of wrapped plugin>

 ./negate ./check_dummy 0 "ma sortie de plugin" ; echo $?
OK: ma sortie de plugin
2
# ./negate ./check_dummy 1 "my plugin output" ; echo $?
WARNING: my plugin output
1
# ./negate ./check_dummy 2 "my plugin output" ; echo $?
CRITICAL: my plugin output
0
# ./negate ./check_dummy 3 "my plugin output" ; echo $?
UNKNOWN: my plugin output
3
```

Principe du plugin

- programme autonome
- doit renvoyer
  - une ligne de texte caractérisant l'état courant
  - un état
    - ok (0)
    - warning (1)
    - critical (2)
    - unknown (3)
- doit traiter l'option –help
- écrire un plugin
  - faire un programme C, Perl, shell...
  - qui écrit 1 ligne sur stdout
  - qui renvoit un code de retour compris entre 0 et 3

```
# df /
Filesystem  1024-blocks   Used   Available Capacity Mounted on
/dev/...     1460048    1174552   210132     85%     /

# df / |tail -1|awk '{print $4}'|sed 's/%//'
85

# cat check_root_size.sh
#!/bin/bash

n=$(df / |tail -1|awk '{print $4}'|sed 's/%//')

if (( n==100 )) ; then
  echo "/ is critical" ; exit 2
elif (( n>95 )) ; then
  echo "/ is warning" ; exit 1
elif (( n<=95 )) ; then
  echo "/ is OK" ; exit 0
else
  echo "unknown" ; exit 3
fi
```

Macros

- $HOSTNAME$
- $HOSTADDRESS$
- $HOSTSTATE$
- $SERVICEDESC$
- $SERVICESTATE$
- $LASTSERVICESTATE$
- etc, au total plusieurs dizaines de macros
- cf annexe2 pour une description de toutes les macros

```
# 'notify-host-by-email' command definition
define command{
        command_name    notify-host-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios *****\n\n\
Notification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\n\
Address: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | \
/bin/mail -s "* $NOTIFICATIONTYPE$ \ Host Alert: $HOSTNAME$ is $HOSTSTATE$ *" $CONTACTEMAIL$
        }

# 'notify-service-by-email' command definition
define command{
        command_name    notify-service-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios *****\n\n \
Notification Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\n \
Address: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\n\
Additional Info:\n\n$SERVICEOUTPUT$" | /bin/mail -s \
"* $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ *" \
 $CONTACTEMAIL$
        }

# 'check-host-alive' command definition
define command{
        command_name    check-host-alive
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100%
        }
```

handler

- programme externe
  - déclenché par Nagios
  - destiné à résoudre un pb avant d'alerter
- ne renvoie rien à Nagios

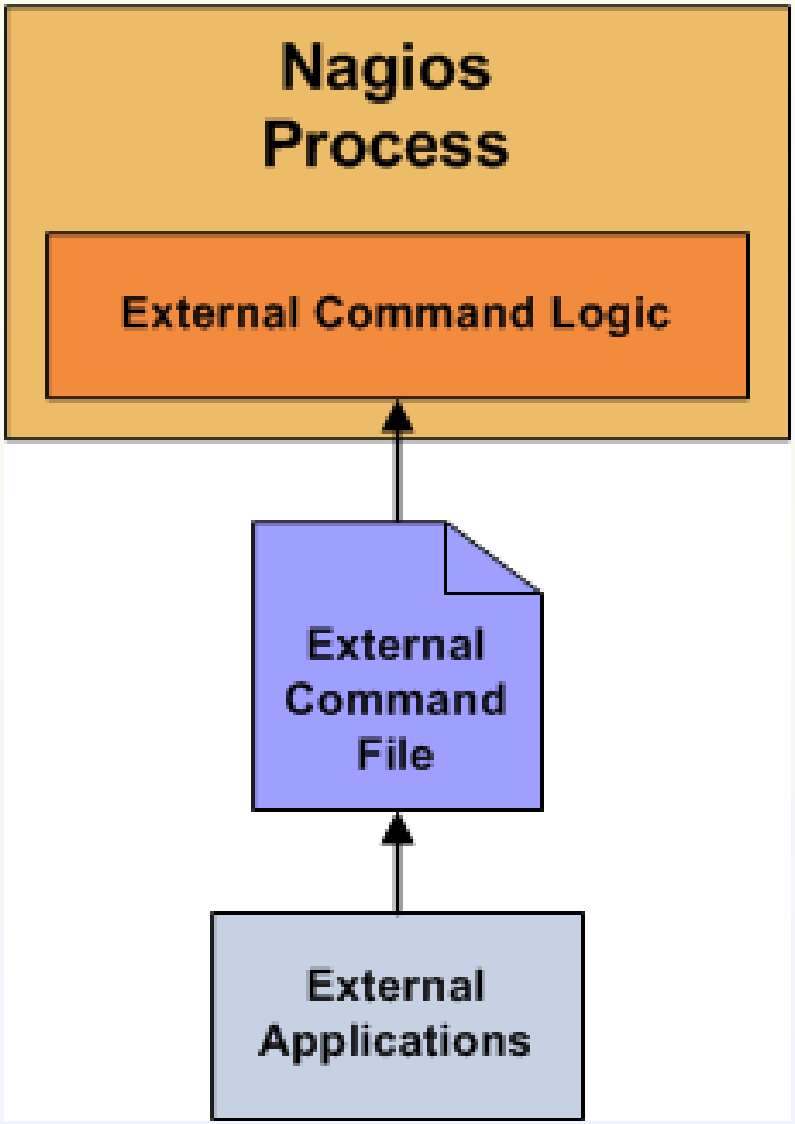
```
#!/usr/local/bin/bash
# /handler.sh

service_attempt=$1
case "$service_attempt" in
  1)
    # tentative simple pour résoudre le pb
    exit 0
  2)
    # examen plus poussé pour tenter de résoudre
    exit 0
  *)
    # on tente le tout pour le tout
    exit 0
esac

--

define command {
  command_name  exemple_handler
  command_line  /usr/local/nagios/libexec/handler.sh $SERVICEATTEMPT$
}
```

Commandes externes



```
# echo "[time] command_id;command_arguments" > /var/rw/nagios.cmd
```

time au format time_t

```
# ll /var/rw/nagios.cmd
prw-rw---- 1 nagios nagcmd 0 Oct  9 09:52 /var/rw/nagios.cmd
```

- action sur le tableau de bord
  - ADD_HOST_COMMENT
  - ADD_SVC_COMMENT
- action sur les notifications
  - CHANGE_CONTACT_HOST_NOTIFICATION_TIMEPERIOD
  - CHANGE_CONTACT_SVC_NOTIFICATION_TIMEPERIOD
  - DISABLE_NOTIFICATIONS
- action sur les commandes
  - CHANGE_HOST_CHECK_COMMAND
  - CHANGE_HOST_EVENT_HANDLER
  - DISABLE_EVENT_HANDLERS
- action sur le séquençage
  - CHANGE_MAX_SVC_CHECK_ATTEMPTS
  - CHANGE_RETRY_SVC_CHECK_INTERVAL
- action sur la logique de monitoring
  - DISABLE_FLAP_DETECTION
  - DISABLE_PASSIVE_SVC_CHECKS

Monitoring adaptatif

- le comportement du monitoring peut être modifié "à la volée"
  - check command (et ses arguments)
  - check interval
  - max check attempts
  - check timeperiod
  - event handler command (et ses arguments)

Envoyer :

```
[<timestamp>] PROCESS_SERVICE_CHECK_RESULT;<host>;<service>;<code>;<output>
```

dans le pipe Nagios

Exemple :

```
# echo "[1255138503] PROCESS_SERVICE_CHECK_RESULT;mailhost;smtp;0;OK"
                                        > /var/rw/nagios.cmd
```

```
define service{
  host_name                backup-server
  service_description      Backup Job

  active_checks_enabled    0
  passive_checks_enabled   1
  check_freshness          1

  freshness_threshold      93600    ; 26 hours threshold

                          ; this command is run only if
                          ; the service results are "stale"
  check_command            no-backup-report

  ...other options...
  }
```

Flapping détection

- Flapping = changements d'état trop fréquent
- Si la détection est activée
  - lorsque le host/service "bagotte"
    - envoi d'une notification "flapping start"
    - blocage des notifications pour ce host/service
  - lorsque le comportement se stabilise
    - envoi d'une notification "flapping stop"
    - déblocage des notifications pour ce host/service
- Activation
  - enable_flap_detection à 1 dans nagios.cfg
  - flap_detection_enabled à 1 dans le host/service

Services volatiles

- normalement, le rythme des notifications est indépendant du rythme des checks
  - quand un service passe dans un état non OK, 1ère notification
  - tq qu'il reste dans cet état, les notifications sont réémises suivant notification_interval
- service volatile
  - notification envoyée à chaque fois qu'un check est non OK ("notification_interval" ignoré)
- exemple
  - tester quotidiennement le contenu d'un log

Dépendance de hosts et de services

- objectif
  - augmenter la pertinence des notifications
    - en supprimant les notifications sans intérêt
  - optimiser la charge du serveur nagios (et des machines monitorées)
    - en supprimant les checks inutiles

Dépendance de hosts

- mise en oeuvre
  - définir un host master (host_name)
  - définir un host slave (dependent_host_name)
- définir les états du master pour lesquels l'état du slave n'a plus d'intérêt
  - notification_failure_criteria
    - liste d'états
    - si le master est dans l'un de ces états, les notifications pour le slave ne sont plus émises
- exemple
  - 1 master host "serveur mysql"
  - 1 slaves host "serveur SPIP"

Dépendance de services

- mise en oeuvre
  - définir un service master (host_name et service_description)
  - définir un service slave (dependent_host_name et dependent_service_description)
  - définir les états du master pour lesquels l'état du slave n'a plus d'intérêt
- exemple
  - 1 service master http
  - n services slaves "virtual_host"

Dépendance de services

- execution_failure_criteria
  - liste d'états
  - si le master est dans l'un de ces états, le slave n'est plus testé
- notification_failure_criteria
  - liste d'états
  - si le master est dans l'un de ces états, les notifications pour le slave ne sont plus émises

```
define servicedependency{
  host_name                       www
  service_description             http
  dependent_host_name             www
  dependent_service_description vh A
  execution_failure_criteria      c
  notification_failure_criteria c
  }
```

Principe de l'escalade d'alertes

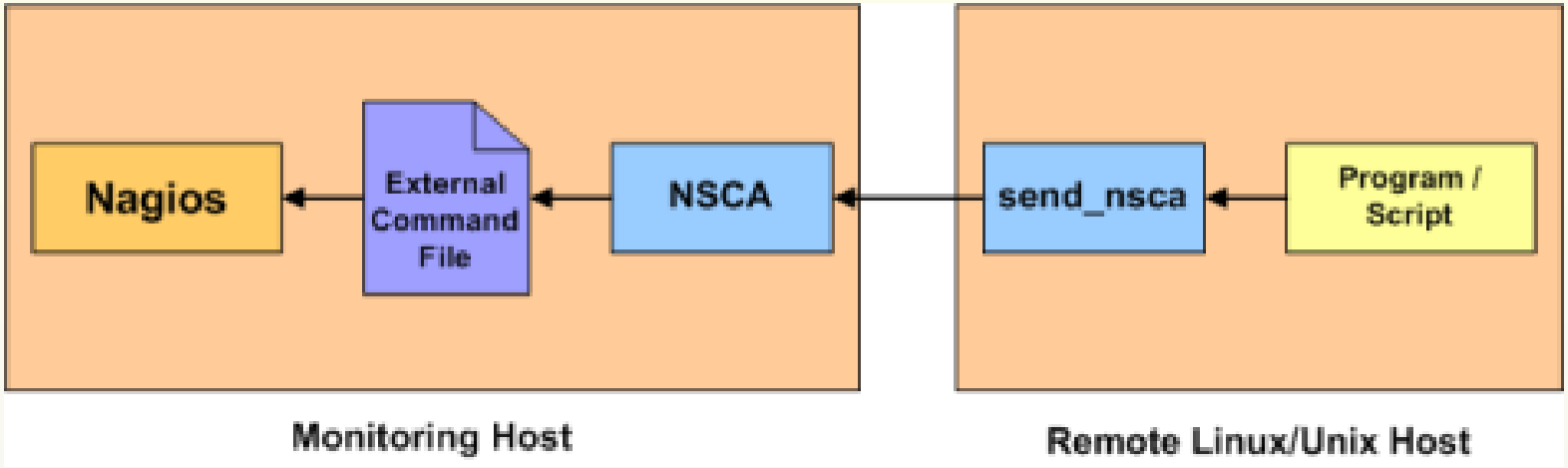
- si un problème persiste après un certain nombre de notifications
- alors on change
  - de destinataire
  - la période de réexpédition des notifications

```
define hostescalation {
  host_name               router-34
  first_notification      5
  last_notification       8
  notification_interval 60
  contact_groups          all-router-admins
  }
```

```
define serviceescalation {
  host_name               webserver
  service_description     HTTP
  first_notification      3
  last_notification       5
  notification_interval 90
  contact_groups          nt-admins,managers
  }

define serviceescalation {
  host_name               webserver
  service_description     HTTP
  first_notification      6
  last_notification       10
  notification_interval   60
  contact_groups          nt-admins,managers,everyone
  }
```

NSCA


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

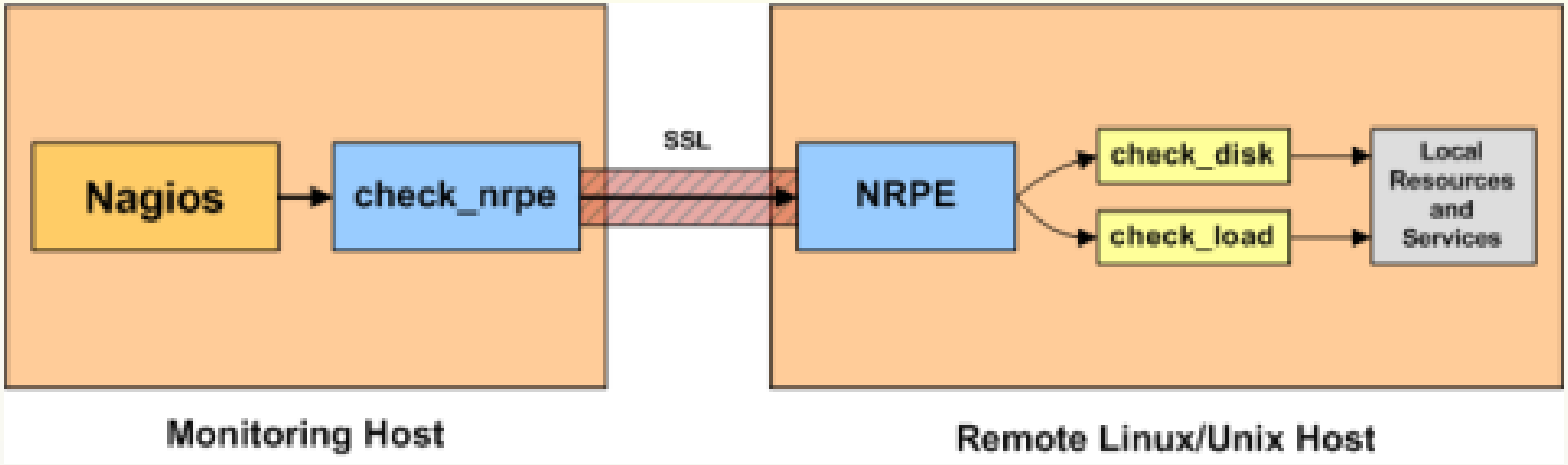
```
Usage: send_nsca -H <host_address> [-p port] [-to to_sec] [-d delim] [-c config_file]

Options:
 <host_address> = The IP address of the host running the NSCA daemon
 [port]         = The port on which the daemon is running - default is 5667
 [to_sec]       = Number of seconds before connection attempt times out.
                  (default timeout is 10 seconds)
 [delim]        = Delimiter to use when parsing input (defaults to a tab)
 [config_file]  = Name of config file to use


Service Checks:
<host_name>[tab]<svc_description>[tab]<return_code>[tab]<plugin_output>[newline]

Host Checks:
<host_name>[tab]<return_code>[tab]<plugin_output>[newline]
```

NRPE


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

Conclusion

- Les plus
  - robuste, peu de bug
  - stable
  - prévu pour supporter la charge et passer l'échelle
  - bien documenté
  - flexible
- Les moins
  - pas d'archives exploitables
  - pas de représentations graphiques valables
    - couplage avec RRDtool (PNP4Nagios, etc.)
  - trop stable ?
    - beaucoup de back-end, add-on, etc.
    - Icinga (fork)
  - configuration verbeuse
    - beaucoup de front-end
    - m4

Définition des macros m4

```
changequote([[,]])

define(m4HOST,[[
define host {
        host_name    $1
ifelse($2,,[[dnl]],[[dnl
        use         translit($2,[[[()]]])]])
        alias ifelse($3,,$1,$3)
        address     syscmd(gethostip -d ifelse($4,,$1,$4)) dnl
ifelse($5,,
        [[dnl
                ifdef([[m4HOST_PARENT]],[[dnl
        parents         translit(m4HOST_PARENT,[[[()]]])]]) dnl
        ]],[[dnl
        parents      translit($5,[[[()]]])]])
ifelse($6,,[[dnl]],[[dnl
        hostgroups  translit($6,[[[()]]])]])
ifdef([[m4HOST_CHECK_COMMAND]],[[dnl
        check_command         m4HOST_CHECK_COMMAND]])
ifdef([[m4CONTACT_GROUPS]],[[dnl
        contact_groups         +translit(m4CONTACT_GROUPS,[[[()]]])]])
ifdef([[m4CONTACTS]],[[dnl
        contacts         +translit(m4CONTACTS,[[[()]]])]])
}
]])

define(m4SERVICE,[[
define service {
        service_description  [[$1]]
ifelse($2,,[[dnl]],[[dnl
        use         translit($2,[[[()]]])]])
ifdef([[m4CONTACT_GROUPS]],[[dnl
        contact_groups       +translit(m4CONTACT_GROUPS,[[[()]]])]])
ifdef([[m4CONTACTS]],[[dnl
        contacts         +translit(m4CONTACTS,[[[()]]])]])
ifelse($3,,[[dnl]],[[dnl
        host_name       translit([[$3]],[[[()]]])]])
ifelse($4,,[[dnl]],[[dnl
       hostgroup_name       translit([[$4]],[[[()]]])]])
ifelse($5,,[[dnl]],[[dnl
       check_command       translit([[$5]],[[[()]]])]])
ifdef([[m4SERVICE_GROUPS]],[[dnl
        servicegroups   translit(m4SERVICE_GROUPS,[[[()]]])]])
}
]])
```

Définition des templates

```
####################
# host templates

# regular hosts
define host {
        name                            regular_host
        use                             basehost
        register                        0

        check_command                   check-host-alive
}

####################
# service templates

# regular services
define service {
        name                            regular_service
        register                        0

        normal_check_interval           15
        retry_check_interval            2
        max_check_attempts              3
}

# relaxed services
define service {
        name                            relaxed_service
        register                        0

        normal_check_interval           60
        retry_check_interval            5
        max_check_attempts              3
}
```

Déclaration des groupes de hosts et services

```
######################
# host groups

define hostgroup{
        hostgroup_name linux_grp
}
define hostgroup{
        hostgroup_name web_grp
}
```

Pour au final définir les ressources en 1 ligne

```
define([[m4CONTACT_GROUPS]],admin_contact)

####################
# hosts

define([[m4HOST_CHECK_COMMAND]],check_host_alive)

dnl m4HOST(1hostname,[2use],[3alias],[4address],[5parents],[6hostgroups+])

m4HOST(alceste,regular_host,,,,(linux_grp,web_grp,ssh_grp))
m4HOST(tonton,regular_host,,,,(linux_grp,mail_grp))
m4HOST(ldap,regular_host,,,,(linux_grp,ldap_grp))
m4HOST(svn,regular_host,,,,(linux_grp,web_grp,svn_grp))
m4HOST(laremagw,regular_host,,,,(linux_grp))

####################
# services

define([[m4SERVICE_GROUPS]],larema_srv)

dnl m4SERVICE(1service,[2use],[3host]+,[4hostgroup+],5check_command)

m4SERVICE(fs,relaxed_service,,linux,check-df!--crit 1000 --warn 5000)
m4SERVICE(ssh,normal_service,,ssh,check_ssh)
```

Références

- le site : http://www.nagios.org
- site collaboratif sur Nagios : http://www.nagiosexchange.org
- site collaboratif sur les plugins : http://nagiosplugins.org
- communauté Nagios francophone : http://www.nagios-fr.org
- fiche plume sur Nagios : http://www.projet-plume.org/fr/fiche/nagios
- http://demo.icinga.org