



# Availability Management

## **Nagios overview**



# Agenda

## ■ Introduction

- Objectives
- Functionalities
- Requirement.

## ■ Architecture & Operation

- Operation Description
- WEB portal

## ■ Plugins and extensions

- Plugins description
- Useful extensions
- Extension example



# INTRODUCTION



## Objectives: Availability Management

- Availability Management is a process of the Service Delivery (ITIL specifications). Its goal is to ensure that the required level of Availability is provided. The measurement and monitoring of IT Availability is a key activity to ensure Availability levels are being met consistently. Availability Management should look continuously to optimise the Availability of the IT Infrastructure, services and supporting organisation.
- In a Network Management environment, monitoring services needed are for example:
  - Routers status
  - Routers environment (CPU, Memory, Temperature...)
  - Links status (interconnexion, access)
  - Links health (traffic evolution, errors level, instability...)
  - Routing protocol status (BGP, MPLS...)
  - ...
- The functionalities needed are:
  - Extended monitoring capabilities, including custom programs for non-standard elements
  - Powerful analysis and notification when an incident is detected
  - Easy to use configuration interface
  - Friendly GUI for service status display

## Nagios functionalities

- Nagios® is an open source tool specially developed to monitor host and service and designed to inform you of network incidents before your clients, end-users or managers do. It has been designed to run under the Linux operating system, but works fine under most \*NIX variants as well
- Initially developed for servers and application monitoring, it is now widely used to monitor networks availability. It is possible with the development of specific plugins around Nagios process.
- Nagios works with a set of "plugins" to provide local and remote service status. The monitoring daemon runs intermittent checks on hosts and services you specify using external "plugins" which return status information to Nagios.
- When incidents are detected, the daemon send notifications out to administrative contacts in a variety of different ways (email, instant message, SMS, etc.). Current status information, historical logs, and reports can all be accessed via a Web browser.
- Custom "plugins" are relatively easy to develop
- Different methods are provided for remote resource discovery
- Nagios is freely available from <http://www.nagios.org>

# Nagios functionalities

- Nagios tool provide monitoring facilities (polling elements at regular intervals and generating events depending on polling return status. Nagios can be considered as a scheduler, which execute plugins, analyse results and obtain a status about each element concerned.
- Nagios can be configured to monitor anything that you can write a script for (Perl scripts, Shell, C programs, ...).
- Nagios comes with loads of plugins for just about every normal known service such as SNMP, DNS, SSH, HTTP, NFS, FTP, etc, etc.
- The advantages of Nagios against other manufacturer products are:
  - It is a free product, running on Linux OS
  - It is an easy to use product, including all functions needed to perform availability monitoring
  - Extensions (plugins) are simple to develop, using well known languages
  - It is scalable, and it is possible to deploy a hierarchy of Nagios servers to provide consolidated views of network and / or system availability (Hypervisor)
- The platform shall nevertheless be integrated in an operational environment with all its constraints:
  - Automatic or semi-automatic configuration of multiple services and instances
  - Attractive GUI for incidents identification, reporting, and relation with Incident Management process
  - Operators alarm (visual, audio or through pager for on-call FTE)

# Requirements

## ■ Other things you will need to get Nagios working are:

- Nagios Plugins (from Nagios download URL)
- GD - Graphics Libraries
- JPEG Lib Sources
- PNG Lib Sources
- FPing (Fast Ping), this is optional but useful.
- For SNMP monitoring you will need:
  - net-snmp-tools, and
  - net-snmp-utils

## ■ MySQL database for storing:

- Elements status logs





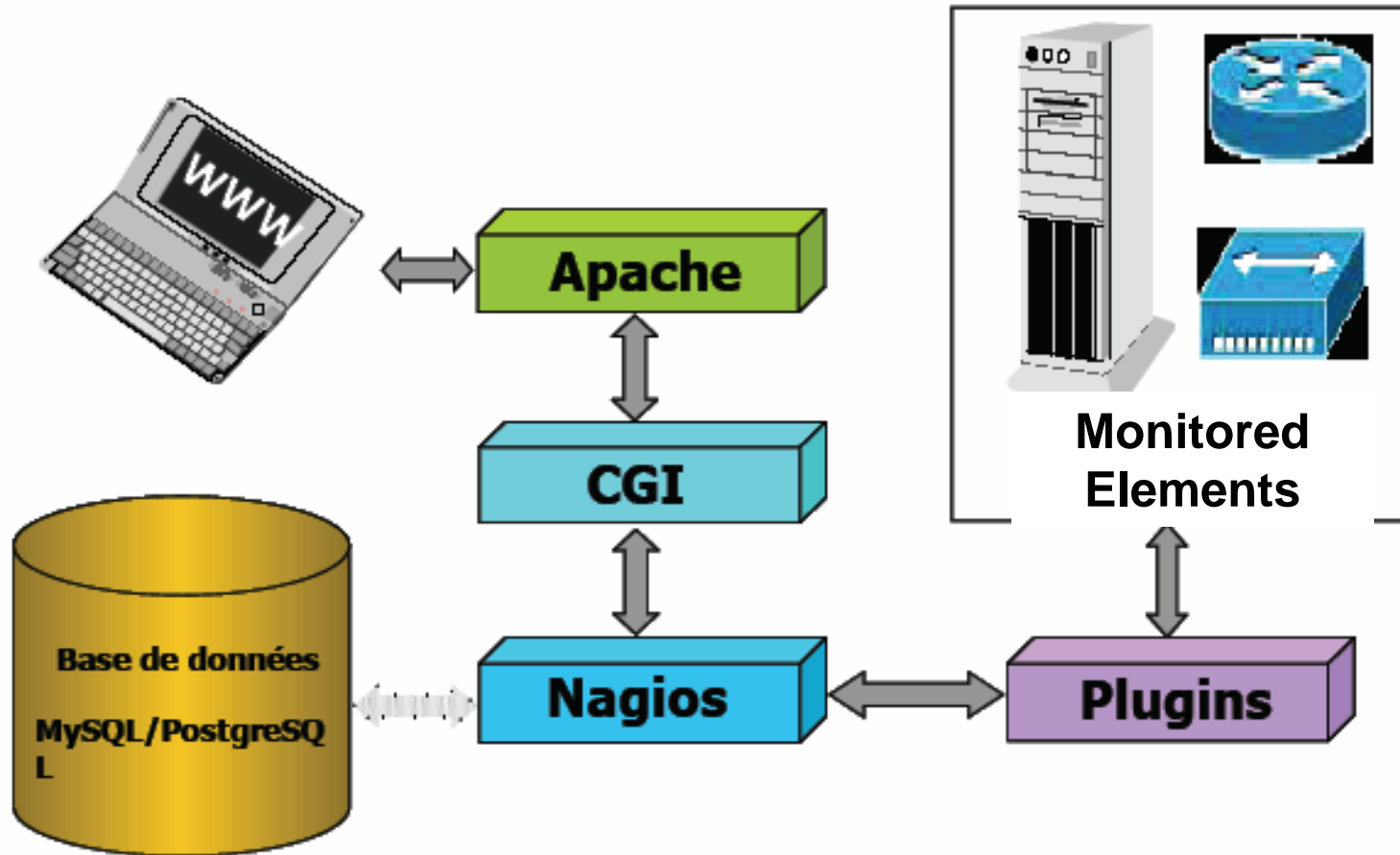
**ARCHITECTURE  
&  
OPERATION**



# Architecture

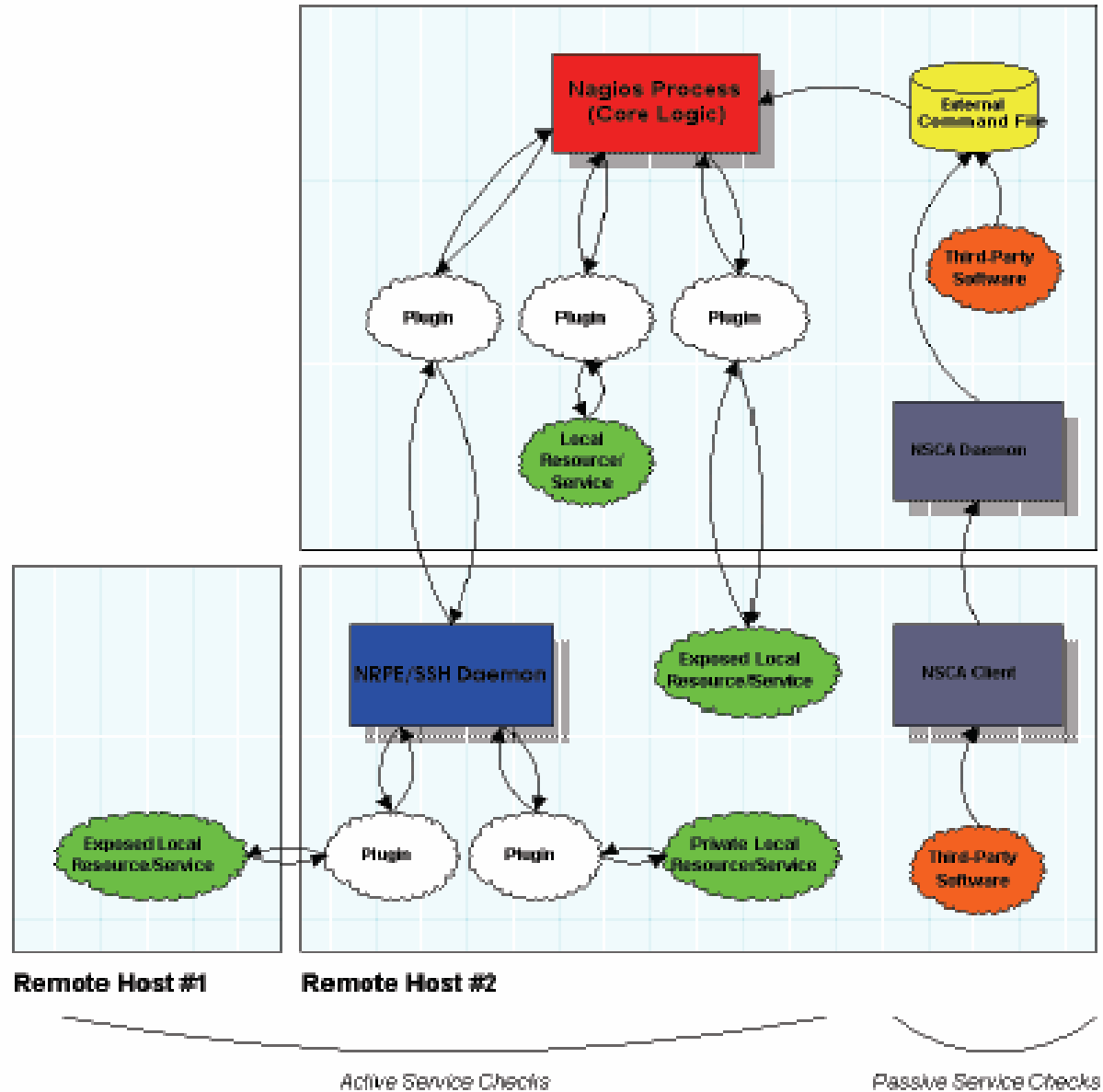
- Nagios is built on a server/agents architecture.  
Usually, on a network, a Nagios server is running on a host, and plugins are running on all the remote hosts that need to be monitored. These plugins send information to the server, which displays them in a GUI.
- Nagios is composed of three parts:
  - A scheduler: this is the server part of Nagios.  
At regular interval, the scheduler checks the plugins, and according to their results do some actions.
  - A GUI: the interface of Nagios (with the configuration, the alerts, ...). It is displayed in web pages generated by CGI.  
It can be state buttons (green,OK/red,Error), sounds, MRTG graphs, ...
  - The plugins. They are configurable by the user. They check a service and return a result to the Nagios server.
- A soft alert is raised when a plugin returns a warning or an error.  
Then on the GUI, a green button turns to red, and a sound is emitted.  
When this soft alert is raised many times (the number is configurable), a hard alert is raised, and the Nagios server sends notifications: email, SMS, ...

# Nagios Architecture (internal)



# Nagios architecture (external)

- Local host
  - Nagios process
  - Plugins
  - NCSA daemon
  
- Remote host
  - NCSA client
  - NRPE/SSH daemon
  - Plugins



# Web Interface: tactical overview

The screenshot displays the Nagios web interface in a browser window. The interface is organized into several sections:

- General:** Includes links for Home, Documentation, Monitoring, Tactical Overview, Status Beta II, Status Overview, Status Summary, Status Grid, Status Map, 3D Status Map, Service Problems, and Network Outages.
- Monitoring Performance:** Shows Check Execution Time (0 / 60 / 3.642 sec), Check Latency (0 / 1 / 0.007 sec), # Active Checks (137), and # Passive Checks (0).
- Network Health:** Displays Host Health and Service Health with corresponding status bars.
- Tactical Monitoring Overview:** Provides a summary of the monitoring system, including the last update time (Sun Jul 15 14:02:26 EDT 2001) and a note about monitoring services in warning.
- Network Outages:** Shows 2 Outages.
- Hosts:** A table showing the status of monitored hosts: 1 Down, 4 Unreachable, 28 Up, and 0 Pending.
- Services:** A table showing the status of monitored services: 14 Critical, 2 Warning, 0 Unknown, 103 OK, and 18 Pending.
- Monitoring Features:** A table detailing the status of various monitoring features:
 

Feature	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Flap Detection	All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping	OK	OK	All Services Enabled All Hosts Enabled	All Services Enabled



# Web Interface: services overview

The screenshot shows the Nagios web interface in a Mozilla browser window. The browser address bar shows `http://starfield.rmpdp.com/nagios/`. The interface includes a left-hand navigation menu with sections for General, Monitoring, Reporting, and Configuration. The main content area displays 'Current Network Status' (last updated Feb 5 17:08:03 GMT 2004), 'Host Status Totals' (14 Up, 0 Down, 0 Unreachable, 0 Pending), and 'Service Status Totals' (66 Ok, 0 Warning, 0 Unknown, 0 Critical, 0 Pending). Below these are three service overview tables for 'cdn-machines', 'uk-machines', and 'zaroff-machines'. The 'cdn-machines' table lists 3 hosts, 'uk-machines' lists 10 hosts, and 'zaroff-machines' lists 2 hosts. All hosts shown are in an 'UP' status with 'OK' service levels.

**Current Network Status**  
 Last Updated: Thu Feb 5 17:08:03 GMT 2004  
 Updated every 60 seconds  
 Nagios © - [www.nagios.org](http://www.nagios.org)  
 Logged in as *rmckenzi*

**Host Status Totals**

Up	Down	Unreachable	Pending
14	0	0	0
<i>All Problems</i>		<i>All Types</i>	
0		14	

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
66	0	0	0	0
<i>All Problems</i>		<i>All Types</i>		
0		66		

**Service Overview For All Host Groups**

**cdn-machines (cdn-machines)**

Host	Status	Services	Actions
<a href="#">chezpat.rmpdp.com</a>	UP	3 OK	
<a href="#">gumbymk2.clones.ca</a>	UP	4 OK	
<a href="#">pinetree-adsl.pinetree.org</a>	UP	4 OK	

**uk-machines (uk-machines)**

Host	Status	Services	Actions
<a href="#">adsl.rmpdp.com</a>	UP	1 OK	
<a href="#">camera.uk.rmpdp.com</a>	UP	4 OK	
<a href="#">ca-gp.uk.rmpdp.com</a>	UP	1 OK	
<a href="#">rob-uk.uk.rmpdp.com</a>	UP	2 OK	
<a href="#">router.uk.rmpdp.com</a>	UP	4 OK	
<a href="#">shengli.uk.rmpdp.com</a>	UP	2 OK	
<a href="#">starfield.rmpdp.com</a>	UP	14 OK	
<a href="#">yuki-uk.uk.rmpdp.com</a>	UP	1 OK	

**us-machines (us-machines)**

Host	Status	Services	Actions
<a href="#">thehostedbox.com</a>	UP	14 OK	

**zaroff-machines (zaroff-machines)**

Host	Status	Services	Actions
<a href="#">icslowa.com</a>	UP	6 OK	
<a href="#">zaroff.net</a>	UP	6 OK	

# Web Interface: services status detail

The screenshot displays the Nagios web interface in a Mozilla browser window. The page title is "RPMDDP - Nagios - Mozilla <2>". The address bar shows "http://starfield.rmpdp.com/nagios/". The interface is divided into several sections:

- Current Network Status:** Last Updated: Thu Feb 5 17:08:35 GMT 2004. Updated every 60 seconds. Nagios® - [www.nagios.org](http://www.nagios.org). Logged in as *rmckenzi*.
- Host Status Totals:**

Up	Down	Unreachable	Pending
1	0	0	0
All Problems		All Types	
0		1	
- Service Status Totals:**

Ok	Warning	Unknown	Critical	Pending
14	0	0	0	0
All Problems		All Types		
0		14		
- Service Status Details For Host 'thehostedbox.com':**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
thehostedbox.com	DISK_BOOT	OK	2004-02-05 17:05:48	2d 13h 0m 34s	1/4	DISK OK [243894 kB (87%) free on /dev/hda1]
	DISK_ROOT	OK	2004-02-05 17:05:47	2d 11h 49m 24s	1/4	DISK OK [22110484 kB (41%) free on /dev/hda3]
	DNS	OK	2004-02-05 17:05:49	10d 8h 47m 24s	1/4	DNS ok - 0 seconds response time, Address(es) is/are 64.236.24.20
	HTTP	OK	2004-02-05 17:05:49	3d 14h 10m 44s	1/4	HTTP ok: HTTP/1.1 200 OK - 0.562 second response time
	IMAP	OK	2004-02-05 17:05:50	2d 11h 49m 24s	1/4	IMAP OK - 0.304 second response time on port 143 [ CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS AUTH=LOGIN] thehostedbox.com IMAP4rev1 2001.315r at Thu, 5 Feb 2004 17:05:54 +0000 (GMT)]
	LOAD	OK	2004-02-05 17:05:48	1d 13h 45m 44s	1/4	OK - load average: 0.20, 0.61, 0.58
	MEMORY	OK	2004-02-05 17:05:48	2d 13h 0m 34s	1/4	Status: OK - 71% memory free.
	MYSQL	OK	2004-02-05 17:05:48	2d 11h 49m 34s	1/4	Uptime: 1969461 Threads: 4 Questions: 908865 Slow queries: 37 Opens: 19007 Flush tables: 1 Open tables: 64 Queries per second avg: 0.461
	PING	OK	2004-02-05 17:05:45	5d 1h 13m 54s	1/4	PING OK - Packet loss = 0%, RTA = 133.47 ms
	SMTP	OK	2004-02-05 17:05:47	8d 7h 34m 14s	1/4	SMTP OK - 0 second response time
	SSH	OK	2004-02-05 17:05:50	10d 8h 47m 24s	1/4	SSH OK - OpenSSH_3.5p1 (protocol 2.0)
	TOTAL PROCESSES	OK	2004-02-05 17:05:47	2d 13h 0m 24s	1/4	OK - 99 processes running
	USERS	OK	2004-02-05 17:05:47	5d 14h 16m 4s	1/4	USERS OK - 0 users currently logged in
	ZOMBIE_PROCS	OK	2004-02-05 17:05:48	2d 13h 0m 24s	1/4	OK - 0 processes running with STATE = Z

At the bottom of the table, it says "14 Matching Service Entries Displayed".

The left sidebar contains navigation menus for General, Monitoring, Reporting, and Configuration.

# Web Interface: services status detail

Current Service Status - Mozilla Firefox

Echier Edition Affichage Aller à Marque-pages Outils ?

**Current Network Status**  
 Last Updated: Fri Sep 2 16:23:32 CEST 2005  
 Updated every 90 seconds  
 Nagios® - [www.nagios.org](http://www.nagios.org)  
 Logged in as *adm-nagios*

[View History For This Host](#)  
[View Notifications For This Host](#)  
[View Service Status Detail For All Hosts](#)

**Host Status Totals**

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
5	0	0	1	0

All Problems	All Types
1	6

**Service Status Details For Host 'infobiovi'**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
infobiovi	BGPstatus	CRITICAL	09-02-2005 16:19:04	0d 0h 44m 27s	4/4	BGP to CNG-2_65025 is DOWN
	CPU	OK	09-02-2005 16:22:30	10d 5h 46m 30s	1/4	5 Minute Avg CPU Usage is 3%
	Istatus	OK	09-02-2005 16:19:04	6d 4h 21m 20s	1/4	OK: host '194.57.241.5', interfaces up: 49, down: 0, dormant: 0, excluded: 0, unused: 0
	Interfaces	OK	09-02-2005 16:20:33	7d 3h 41m 46s	1/4	OK: Les liens "Infobiovi_Vlan23, Infobiovi_Vlan22, Infobiovi_Vlan30, Infobiovi_Vlan40, Infobiovi_Vlan50, Infobiovi_Vlan90, Infobiovi_Vlan1 , Infobiovi_Vlan10, Infobiovi_Vlan20, Infobiovi_Vlan21 , Infobiovi_Vlan121, Infobiovi_Vlan2, Infobiovi_Vlan140" sont Up
	OSPFstatus	OK	09-02-2005 16:21:03	80d 4h 28m 50s	1/4	Links to infobio,infobiovp are Up
	PING	OK	09-02-2005 16:22:31	1d 9h 28m 13s	1/4	PING OK - Packet loss = 20%, RTA = 9.10 ms

6 Matching Service Entries Displayed

Terminé

# Web Interface: services status detail

Extended Information - Mozilla Firefox

Eichier Edition Affichage Aller à Marque-pages Outils ?

**Service Information**  
 Last Updated: Fri Sep 2 16:24:29 CEST 2005  
 Updated every 90 seconds  
 Nagios® - [www.nagios.org](http://www.nagios.org)  
 Logged in as *adm-nagios*

[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 This Service](#)

Service  
**BGPstatus**  
 On Host  
**infobiovi**  
**(infobiovi)**

194.57.241.5  
 Voir la Weathermap  
 ( Voir la Weathermap )

**Service State Information**

Current Status:	<b>CRITICAL</b>
Status Information:	BGP to CNG-2_65025 is DOWN
Current Attempt:	4/4
State Type:	HARD
Last Check Type:	ACTIVE
Last Check Time:	09-02-2005 16:24:04
Status Data Age:	0d 0h 0m 26s
Next Scheduled Active Check:	09-02-2005 16:29:04
Latency:	< 1 second
Check Duration:	1 second
Last State Change:	09-02-2005 15:39:05
Current State Duration:	0d 0h 45m 25s
Last Service Notification:	N/A
Current Notification Number:	0
Is This Service Flapping?	N/A
Percent State Change:	N/A
In Scheduled Downtime?	<b>NO</b>
Last Update:	09-02-2005 16:24:25

Service Checks: **ENABLED**  
 Passive Checks: **ENABLED**  
 Service Notifications: **DISABLED**  
 Event Handler: **ENABLED**  
 Flap Detection: **ENABLED**

**Service Commands**

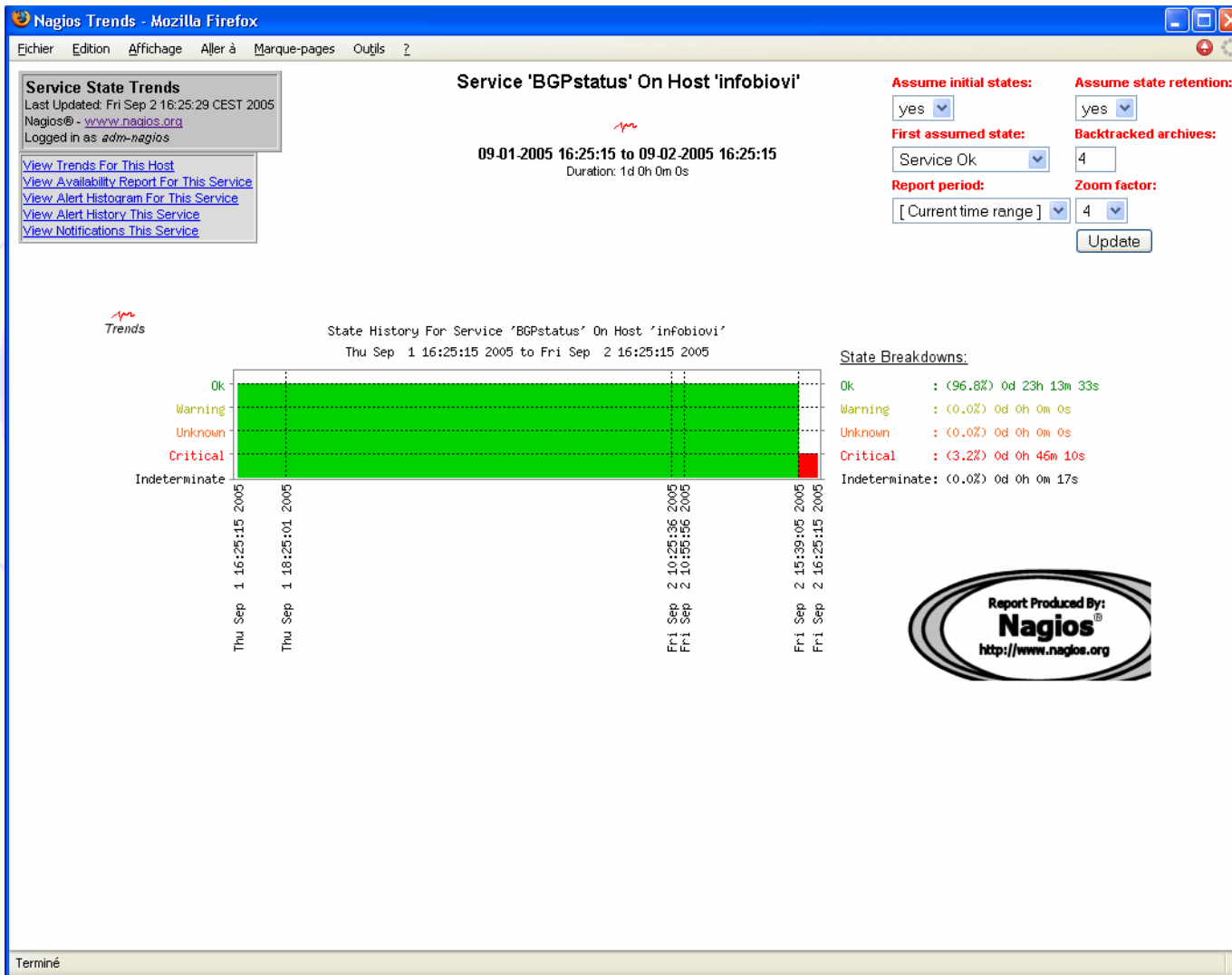
- [Disable checks of this service](#)
- [Re-schedule the next check of this service](#)
- [Submit passive check result for this service](#)
- [Stop accepting passive checks for this service](#)
- [Acknowledge this service problem](#)
- [Enable notifications for this service](#)
- [Schedule downtime for this service](#)
- [Disable event handler for this service](#)
- [Disable flap detection for this service](#)

**Service Comments**

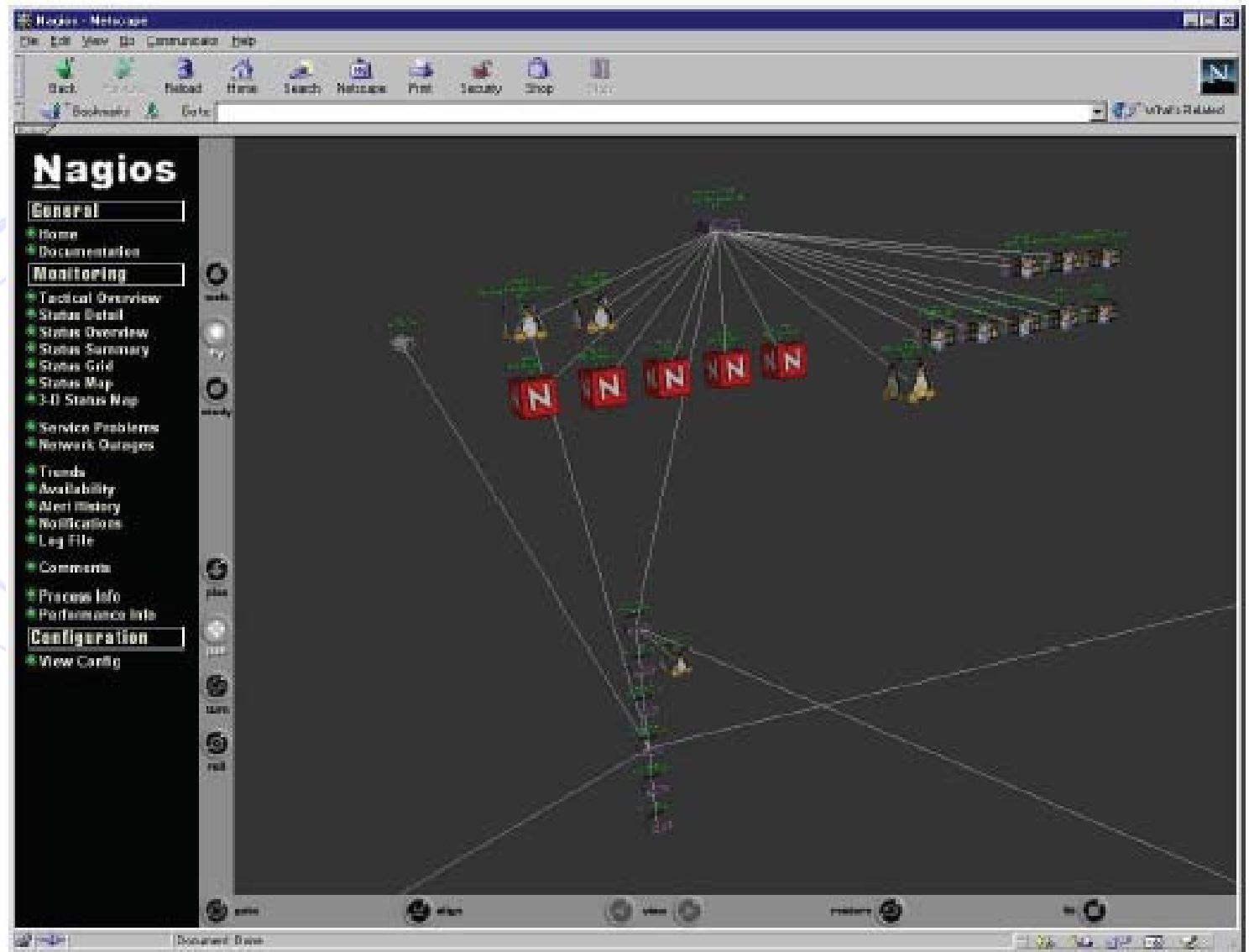
Terminé



# Web Interface: services status detail



# Web Interface: 3D status map



# Configuration Files

- **nagios.cfg**
  - Main configuration file
  - Monitored elements configuration
- **resource.cfg**
  - User defined elements configuration file
- **cgi.cfg**
  - Display options for CGI
- **host, hostgroup and hostextinfo**
  - Information concerning monitored equipments
- **service, servicextinfo**
  - Information concerning monitored services
- **host and service dependency**
  - Dependencies between hosts and between services
- **host escalation, host group escalation, service escalation**
  - Escalation notification

# Configuration Files

- **contact**
  - Nagios users. To access Nagios interface, it is necessary to be registered in this contact file
- **contactgroup**
  - User Groups. Notifications and display rights are settled in this file
- **timeperiod**
  - Use to configure period of time for elements monitoring and users notifications.
- **command**
  - Set of commands used to control services, equipments, events management and notifications



## Sample configuration files

Hosts.cfg :

=====

```
define host{
```

```
    notifications_enabled      1 ; Host notifications are enabled
    event_handler_enabled      1 ; Host event handler is enabled
    flap_detection_enabled     1 ; Flap detection is enabled
    process_perf_data          1 ; Process performance data
    retain_status_information   1 ; Retain status information
```

```
across
```

```
program restarts
```

```
    retain_nonstatus_information 1 ; Retain non-status information
```

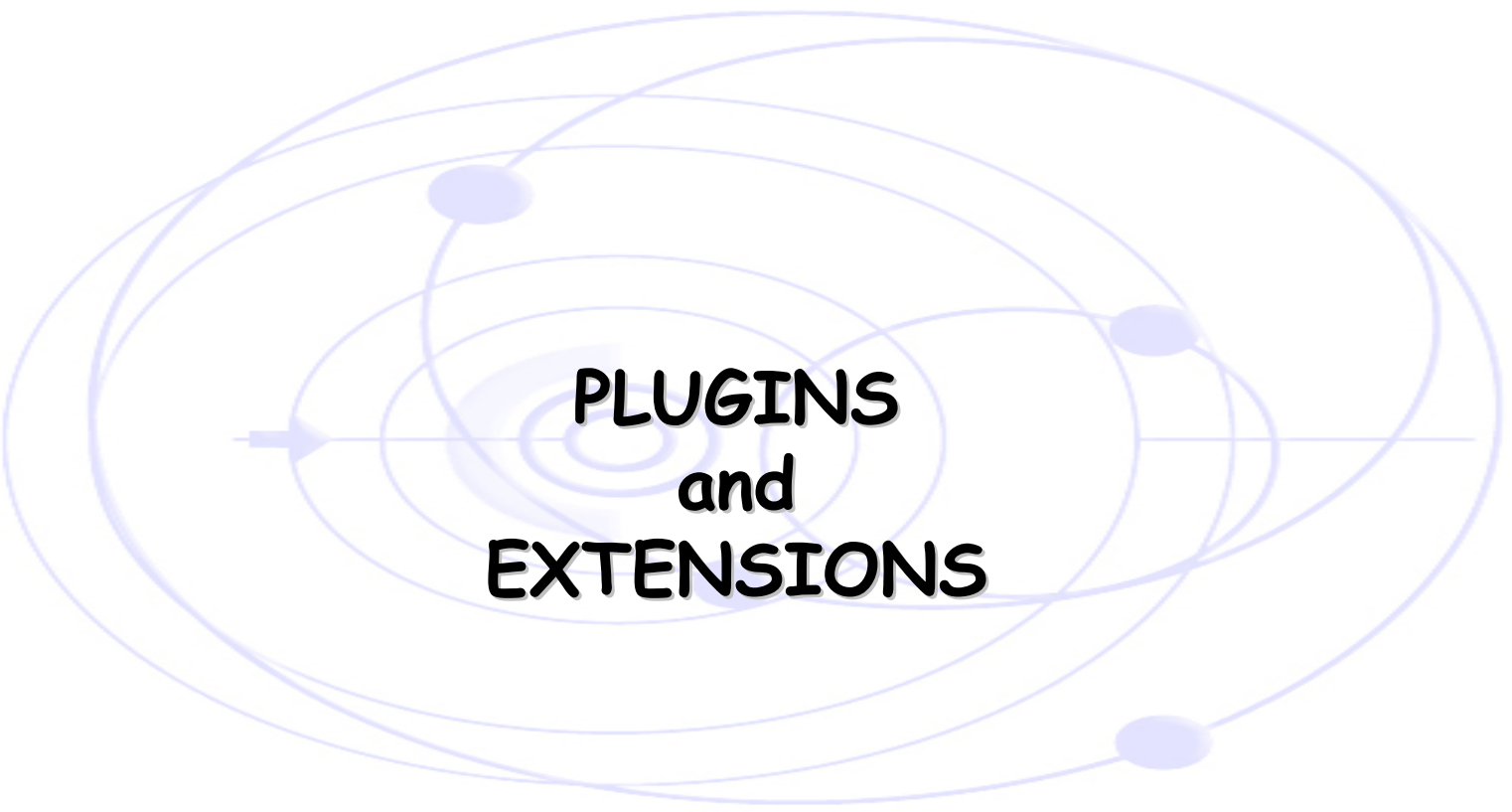
```
across program restarts
```

```
# 'novell1' host definition
```

```
define host{
```

```
    use                               generic-host ; Name of host template to
    use
```

```
    host_name                         novell1
    alias                             Novell Server #1
    address                           192.168.1.2
    check_command                      check-host-alive
    max_check_attempts                 10
    notification_interval              120
    notification_period                24x7
    notification_options               d,u,r
}
```



# PLUGINS and EXTENSIONS

# Plugins and Extensions

- Developments on Nagios can be found at <http://www.nagiosexchange.org/>
- AddOn projects are freely available. They cover subjects on:
  - Charts,
  - Communications,
  - Configuration,
  - Development,
  - DownTimes,
  - FrontEnds,
  - Notificatons,
  - Misc
- Plugins have been developed on:
  - Networking,
  - SNMP,
  - Hardware,
  - Linux,
  - Solaris,
  - Windows, ...

# PLUGINS

- A plugin is a small program (in Perl, C, java, python, ...) that checks a service (a daemon, some free space on a disk, ...). It must return a value and a small line of text (Nagios will only grab the first line of text).

Output should be in the format: *METRIC STATUS: information text/performance data*

The allowed METRIC STATUS are 0 (OK), 1 (WARNING), 2 (CRITICAL) or 3 (UNKNOWN)

- The warning and critical **thresholds** are parameters, set by the user, passed as arguments to the plugin.
- A plugin can also return **performance data** in the format: "label1=value1 label2=value2 ..."  
These data are stored by Nagios and may be later displayed with **MRTG**  
(<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>)
- The plugins can be run:
  - **Locally**, on the Nagios server.  
But such a plugin can check remote hosts, for example *check\_ping* which pings remote hosts to check if they are running.
  - **Remotely**, through a remote Nagios server, with ssh, with snmp, with NRPE (Nagios Remote Plugin Executor), or with NSCA (Nagios Service Check Acceptor).  
It means that the plugin either waits for a verification request from the Nagios server before sending its result, or executes itself and sends the result to the Nagios server.



## Sample Plugin: Check\_Cisco-Ping (beginning)

```
#!/usr/bin/perl

# check_cisco_command - telnet's to a Cisco router to run a command

# License Information:
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#

use strict;

use Getopt::Long;

use vars qw($opt_d $opt_u $opt_p $opt_P $opt_h $opt_H $opt_V $opt_v
            $debug $username $password $hostname $state $error $PROGNAME
            @command_output $session $command $opt_r $tmp_var_loss
            $tmp_var_latency
            $opt_c $opt_w $info $answer $opt_m $metric $warning_rta $warning_pl
            $timeout $router $critical_rta $critical_pl $opt_t $vrf $stats);

use lib "utils.pm";
use utils qw(%ERRORS &print_revision &support &usage );

use Net::Telnet::Cisco;

sub print_help ();
sub print_usage ();

$ENV{'PATH'}='';
$ENV{'BASH_ENV'}='';
$ENV{'ENV'}='';
```

## Other useful developments

### ■ Alarm resiliency

- Nagios gives an immediate status of the monitored elements, it has no memory (except in log). It is useful to keep trace of an incident until it has been checked and acknowledged by an operator.

### ■ Network Interfaces discovery

- Within big networks, it is useful to « compare » real configuration with database configuration. An external program can check every day (auto-discovery) the real network configuration versus Nagios database.
- If differences appears, notify network administrator of the change.

### ■ Semi-automatic configuration

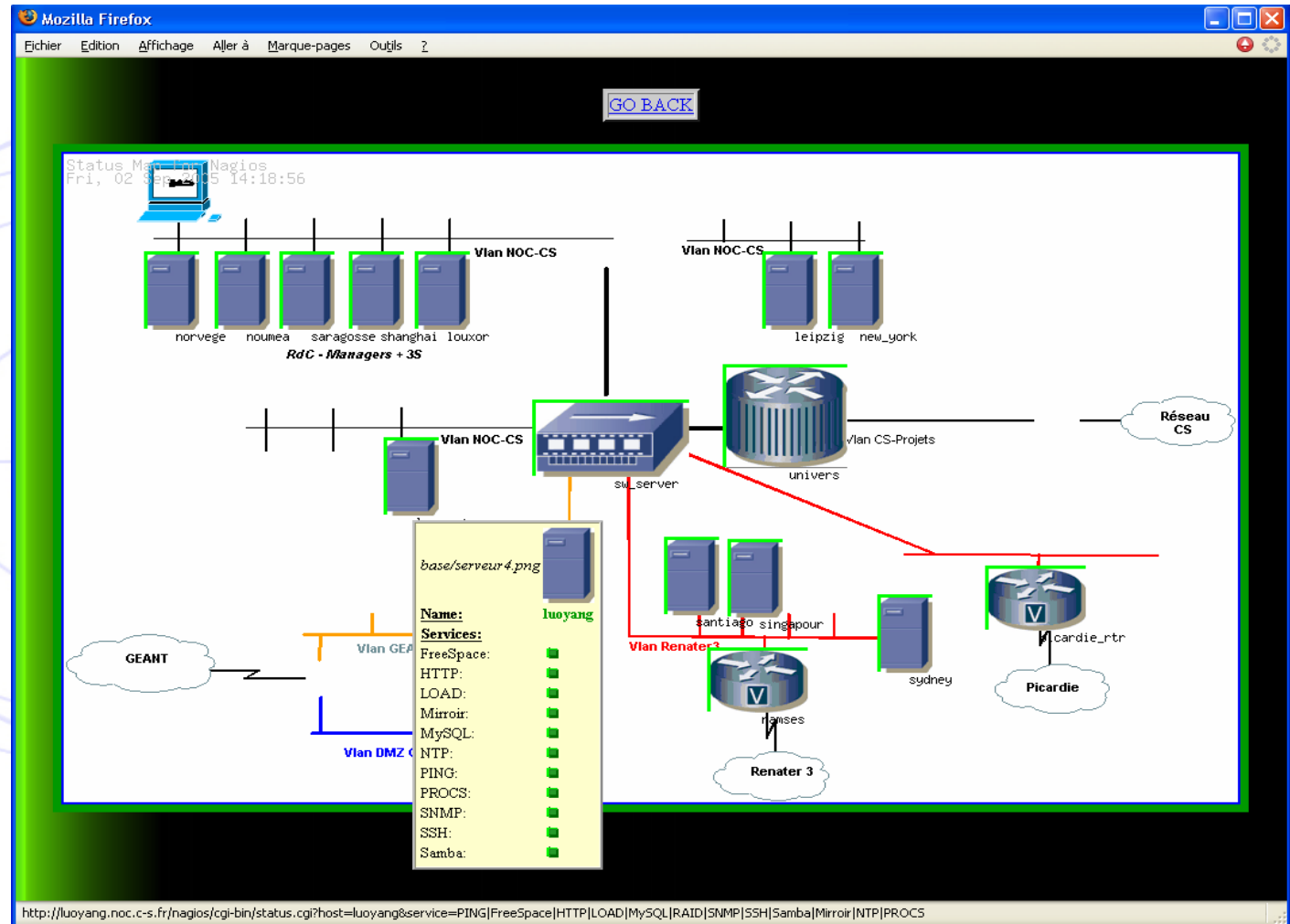
- For each new element, multiple identified checking have to be configured and started
- Semi-automatic configuration tool will write Nagios configuration files based on higher level network description files



# BBMAP interfacing Nagios

## ■ BBMAP (Big Brother MAP)

- BBMAP gives a graphical view of Nagios elements.
- Elements on the map are "clickable" and give access to underlying status details
- It is easier to modify than Nagios maps (2D and 3)
- It is logically separated from Nagios (security enhancement):
  - Nagios is for administrator
  - BBMAP is for users





# BBMAP interfacing Nagios and WeatherMap

Mozilla Firefox

Fichier Edition Affichage Aller à Marque-pages Outils ?

[GO BACK](#)

Status Map for Nagios  
Fr Tue Nov 23 06:24:33 GMT 2004

**base/switch\_router\_33x29.png**

**Name:** infobiovi

**Services:**

- BGPstatus: ❌
- CPU: ✅
- IFstatus: ✅
- Interfaces: ✅
- OSPFstatus: ✅
- PING: ✅

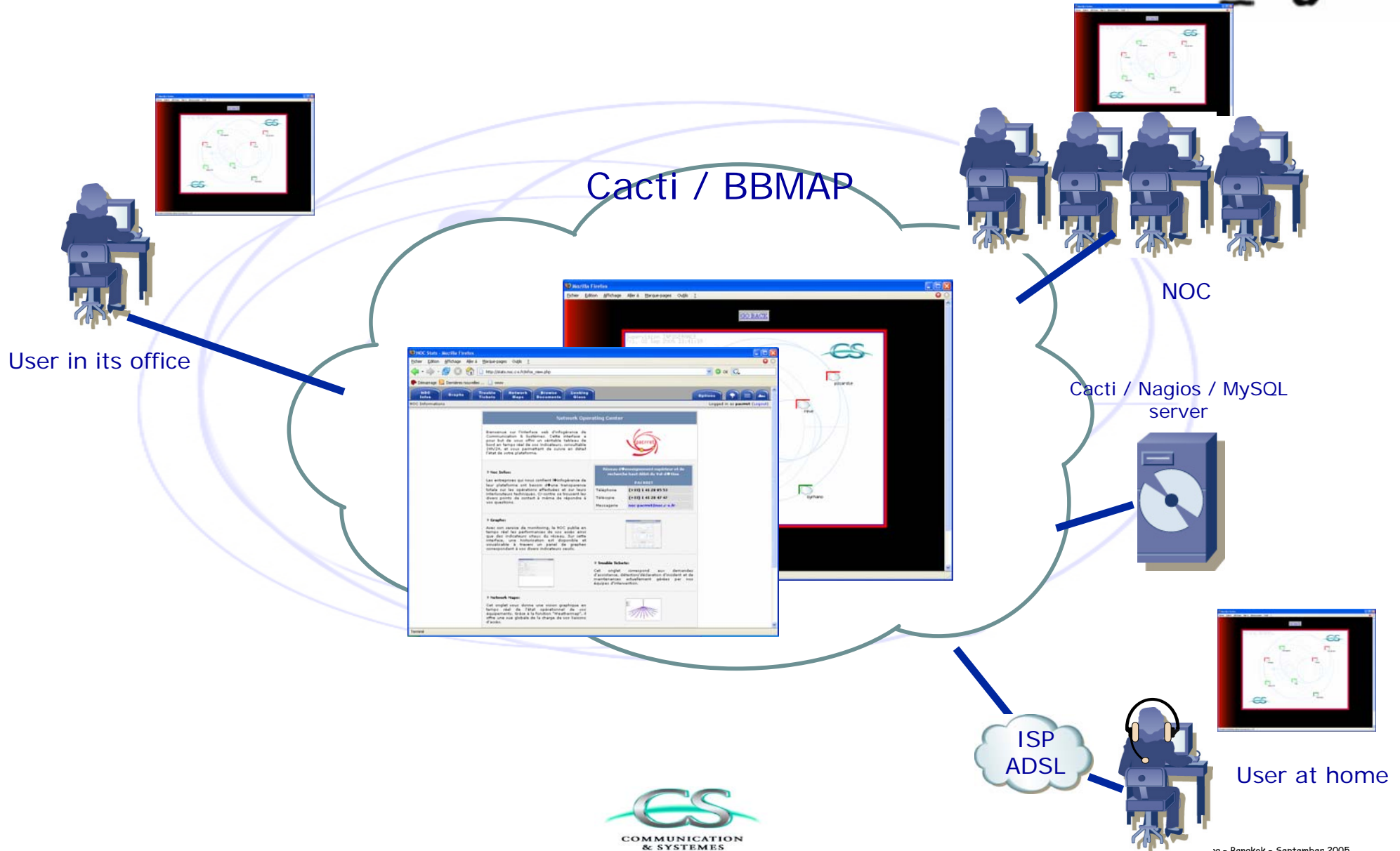
**Legend:**

- <0.005%
- <0.01%
- <0.05%
- <0.1%
- <0.5%
- <1%
- <2%
- <5%
- <10%
- <30%
- <60%
- <70%
- <80%
- <90%
- <100%

http://luoyang.noc.c-s.fr/nagios/cgi-bin/status.cgi?host=infobiovi&service=CPU|IFstatus|Interfaces|OSPFstatus|BGPstatus|PING|STATUS



# Cacti and BMAP consolidation



# References

- **Nagios source program**
  - <http://www.nagios.org/download/>
- **Nagios Extra developments**
  - <http://www.nagiosexchange.org/>
- **Official plugins**
  - <http://nagiosplug.sourceforge.net/>
- **Conferences**
  - <http://www.nagios.org/propaganda/conferences/>



**THE END**

Thank you for your attention