



Nagios®

- Surveillance des services réseaux
- Surveillance des ressources serveurs
- Surveillance des services applicatifs
- Notification d'informations
- Interface Web
- Licence GNU/GPL

1

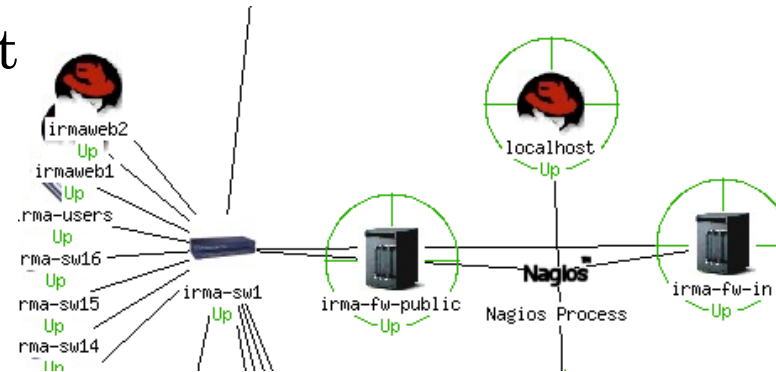
PLAN

- Présentation de l'outil
 - Fonctionnement du moteur (ordonnanceur)
 - Interface WEB de consultation
 - Des plugins
- Les fichiers de configuration
- Les plugins de Nagios – Les plugins « perso »

Supervision à l'IRMA

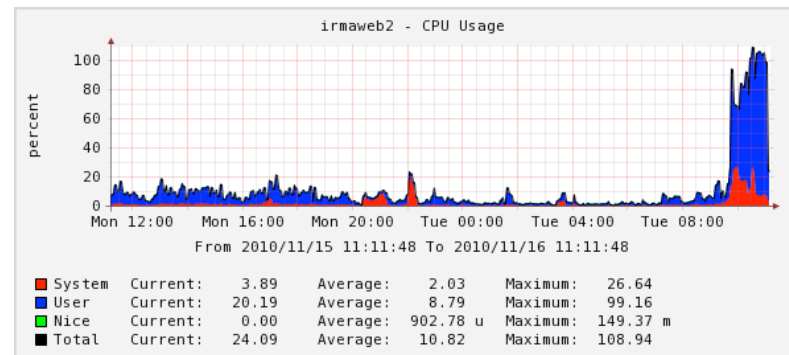
○ Nagios (tableau de bord)

- Vue globale des serveurs, services, équipements...
- Alertes dysfonctionnement
- Log des problèmes
- ...



○ Cacti (historique)

- Historique d'activité (cpu, disques, réseau, printer...)
- Optimisation ressources
- Gestion consommables
- ...



HISTORIQUE DE NAGIOS

- *Mars 1999* : Création de Netsaint
- *Mars 2002* : Dernière version de Netsaint –
Abandon du projet
- *Mai 2002* : Première version de Nagios –
Suite de Netsaint
- *Février 2004* : Sortie de la version 1.2 Nagios stable
- *Février 2006* : Sortie de la version 2.0 Nagios stable
- *Octobre 2009* : Version 3
- *Actuellement* : Version 3.3.1
- Et... « fork » du projet pour créer Icinga
- Et aussi... Centreon – surcouche de configuration

<http://www.nagios.org/>

AVANTAGES ET INCONVÉNIENTS - NAGIOS

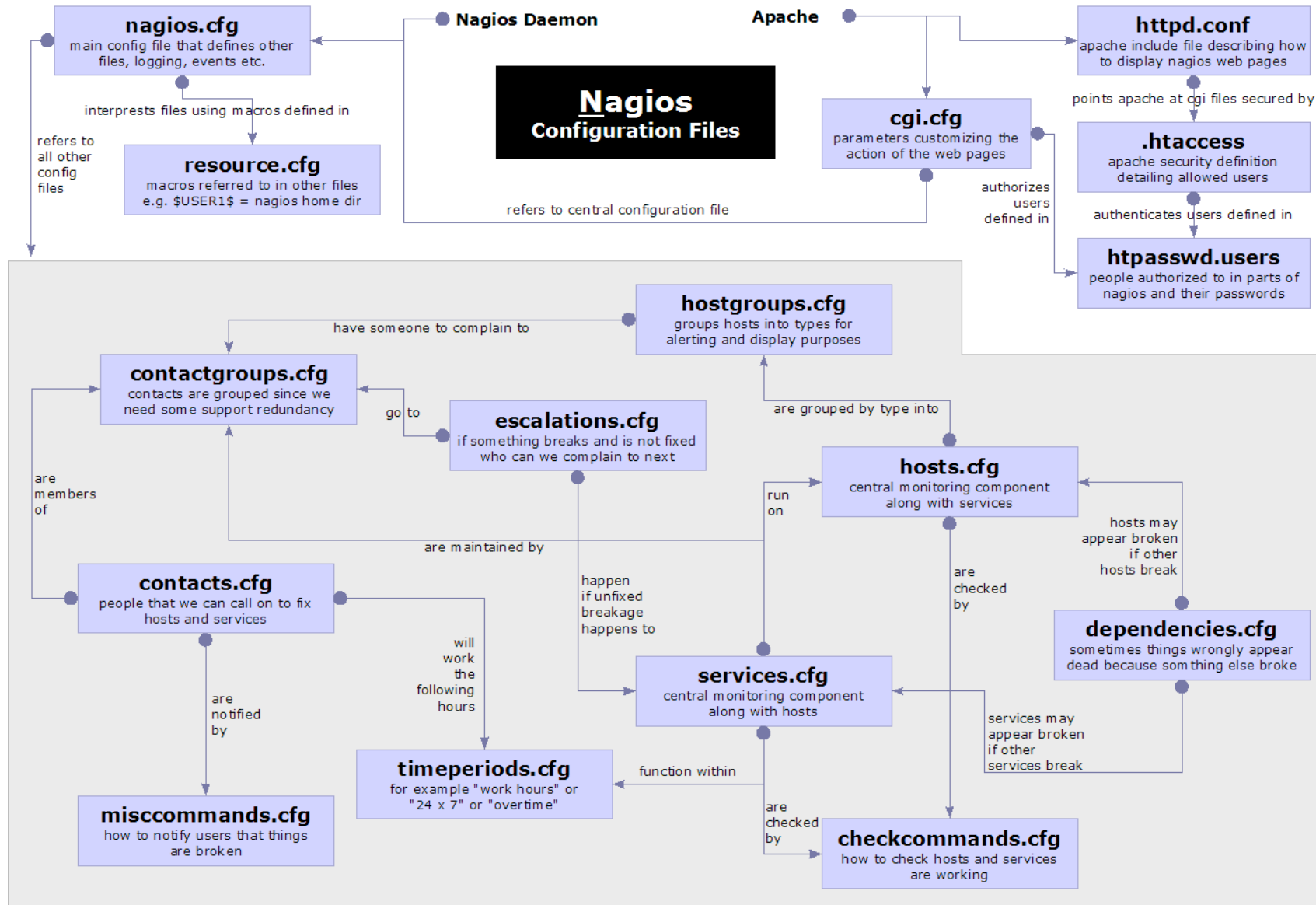
○ **Avantages:**

- Logiciel libre
- Information constante et en temps réel sur l'état du parc informatique
- Richesse des plugins (nagios.org et nagiosexchange.org et ses propres plugins)
- Possibilité d'analyse grâce à l'édition de rapports

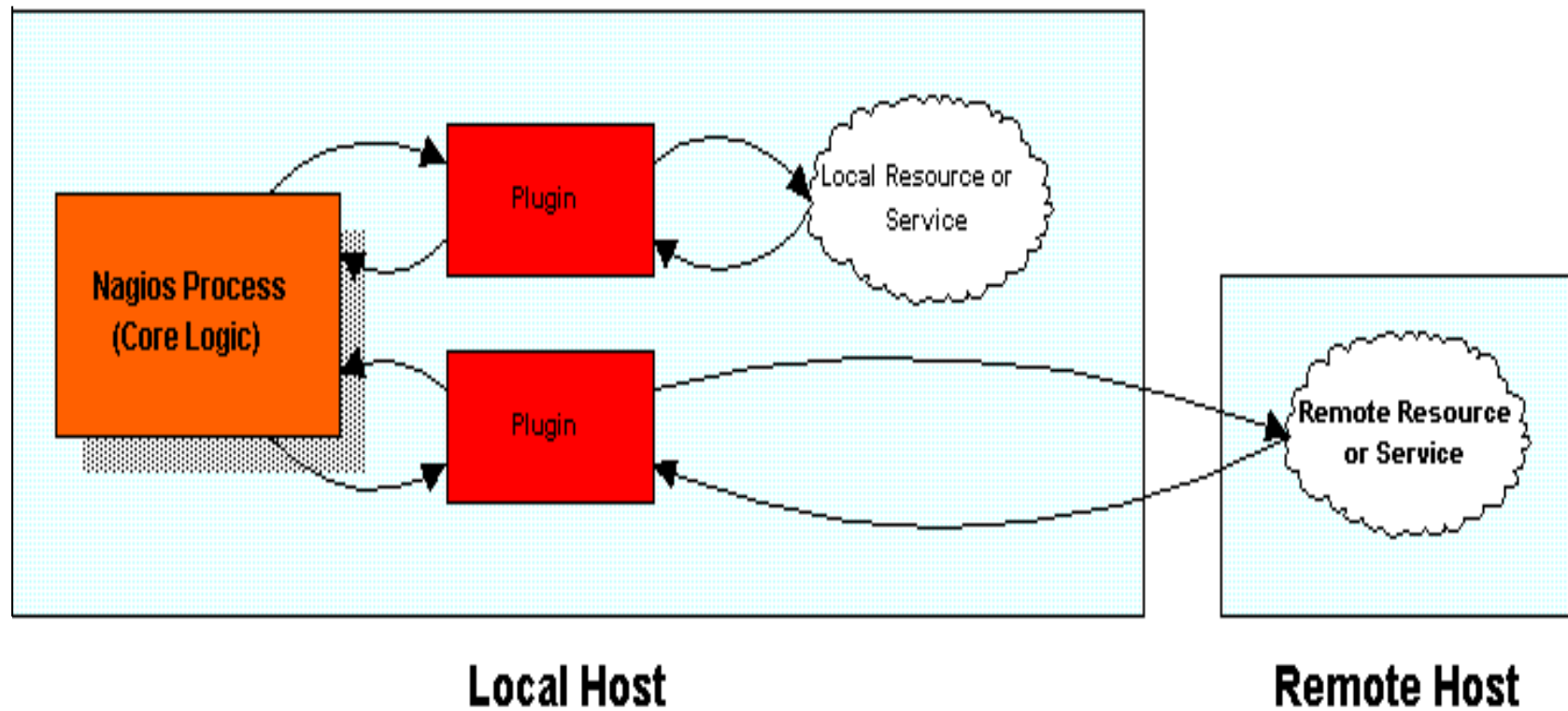
○ **Inconvénients**

- Interface complexe et pas très intuitive
- Configuration fastidieuse, nombre important de fichiers de configuration
- Configuration de bout en bout

DÉPENDANCE ET CONFIGURATION !!!



FONCTIONNEMENT



FONCTIONNEMENT

Quelques plugins par catégorie:

○ **Equipement**

- **Etat** (up/down...)
- Test de **l'espace disque** disponible
- **Charge du système** en temps réel
- **Consommables** (toner, bandes...)
- Monitoring de **température**
- Monitoring **services** dhcp, http, flexlm, smtp, mysql, ssh...
- ... et tout ce qui peut être supervisé 😊

FONCTIONNEMENT

Quelques plugins par catégorie:

○ Réseaux - protocoles

- Vérifie si un **hôte** est **vivant** sur le réseau (ICMP)
- Taux de transfert d'un **routeur** ou **switch**
- Test des réseaux **NetWare**
- Test de la couche **Transport** (UDP/TCP...)
- **plugin** sur base snmp...
- ...

FONCTIONNEMENT

Quelques plugins par catégorie:

○ Applicatifs

- **Encapsulation** de requête en utilisant **SSH** comme support
- Ou typique :
 - nagios lui-même,
 - flexlm,
 - mysql,
 - backup... etc.

FONCTIONNEMENT

Quelques plugins par catégorie:

○ Services

- Vérification de « **serveurs/services** » :
 - DNS
 - FTP
 - Pop/Imap
 - NFS
 - NTP
 - HTTP
 - Lpd/ipp
 - MySQL ou autre...
 - ...

INTERFACE – TACTICAL OVERVIEW

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends
- Alerts
 - History
 - Summary
 - Histogram
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Tactical Monitoring Overview
 Last Updated: Mon Nov 8 11:59:37 CET 2010
 Updated every 90 seconds
 Nagios® Core™ 3.2.0 - www.nagios.org
 Logged in as nagiosadmin

Monitoring Performance

Service Check Execution Time: 0.01 / 10.12 / 2.205 sec
 Service Check Latency: 0.00 / 0.50 / 0.212 sec
 Host Check Execution Time: 3.02 / 4.06 / 4.000 sec
 Host Check Latency: 0.02 / 0.35 / 0.200 sec
 # Active Host / Service Checks: 50 / 103
 # Passive Host / Service Checks: 0 / 0

Network Outages
 0 Outages

Network Health

Host Health:

Service Health:

Hosts

1 Down | 0 Unreachable | 49 Up | 0 Pending

1 Unhandled Problems

Services

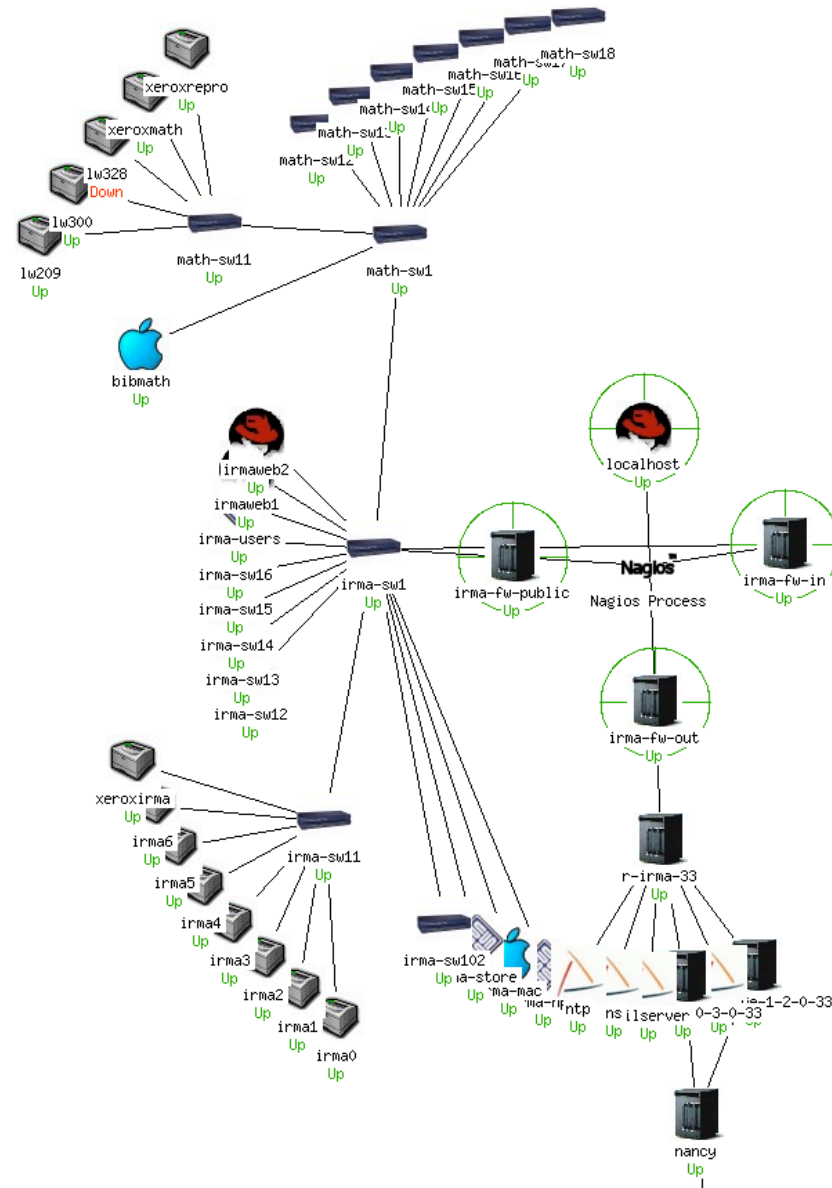
4 Critical | 0 Warning | 0 Unknown | 99 Ok | 0 Pending

4 on Problem Hosts

Monitoring Features

| Flap Detection | Notifications | Event Handlers | Active Checks | Passive Checks |
|---|--|--|--|--|
| Enabled All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping | Enabled 11 Services Disabled All Hosts Enabled | Enabled All Services Enabled All Hosts Enabled | Enabled All Services Enabled All Hosts Enabled | Enabled All Services Enabled All Hosts Enabled |

INTERFACE - MAP



INTERFACE - HOSTS

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts**
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends
- Alerts
 - History
 - Summary
 - Histogram
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Current Network Status
 Last Updated: Mon Nov 8 12:09:20 CET 2010
 Updated every 90 seconds
 Nagios® Core™ 3.2.0 - www.nagios.org
 Logged in as nagiosadmin

[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 |
|---------------------|------|------------------|---------|
| 49 | 1 | 0 | 0 |
| All Problems | | All Types | |
| 1 | | 50 | |

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|---------------------|---------|------------------|----------|---------|
| 99 | 0 | 0 | 4 | 0 |
| All Problems | | All Types | | |
| 4 | | 103 | | |

Host Status Details For All Host Groups

| Host ↑↓ | Status ↑↓ | Last Check ↑↓ | Duration ↑↓ | Status Information |
|---------------------|-----------|---------------------|-----------------|---|
| ibmath | UP | 11-08-2010 12:08:56 | 54d 2h 27m 40s | PING OK - Paquets perdus = 0%, RTA = 1.36 ms |
| cro-rc1-qa-1-2-0-33 | UP | 11-08-2010 12:09:06 | 18d 17h 37m 54s | PING OK - Paquets perdus = 0%, RTA = 12.44 ms |
| irma-fw-in | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 0.94 ms |
| irma-fw-out | UP | 11-08-2010 12:09:06 | 54d 2h 27m 40s | PING OK - Paquets perdus = 0%, RTA = 0.17 ms |
| irma-fw-public | UP | 11-08-2010 12:09:06 | 54d 2h 27m 40s | PING OK - Paquets perdus = 0%, RTA = 0.21 ms |
| irma-hwc | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 0.20 ms |
| irma-mac | UP | 11-08-2010 12:09:06 | 54d 2h 27m 50s | PING OK - Paquets perdus = 0%, RTA = 0.16 ms |
| irma-store | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 2.19 ms |
| irma-sw1 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 40s | PING OK - Paquets perdus = 0%, RTA = 0.73 ms |
| irma-sw102 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 2.01 ms |
| irma-sw11 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 40s | PING OK - Paquets perdus = 0%, RTA = 2.73 ms |
| irma-sw12 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 1.95 ms |
| irma-sw13 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 1.93 ms |
| irma-sw14 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 1.45 ms |
| irma-sw15 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 1.54 ms |
| irma-sw16 | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 2.20 ms |
| irma-users | UP | 11-08-2010 12:09:06 | 54d 2h 27m 30s | PING OK - Paquets perdus = 0%, RTA = 0.50 ms |
| irma0 | UP | 11-08-2010 12:06:46 | 1d 11h 51m 54s | PING OK - Paquets perdus = 0%, RTA = 0.94 ms |
| irma1 | UP | 11-08-2010 12:04:16 | 0d 11h 52m 44s | PING OK - Paquets perdus = 0%, RTA = 0.32 ms |
| irma2 | UP | 11-08-2010 12:04:26 | 0d 11h 52m 34s | PING OK - Paquets perdus = 0%, RTA = 0.84 ms |
| irma3 | UP | 11-08-2010 12:04:26 | 0d 11h 52m 34s | PING OK - Paquets perdus = 0%, RTA = 0.63 ms |

INTERFACE - SERVICES

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts
- Services**
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends
- Alerts
 - History
 - Summary
 - Histogram
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Current Network Status
 Last Updated: Mon Nov 8 12:11:15 CET 2010
 Updated every 90 seconds
 Nagios® Core™ 3.2.0 - 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 |
|----|------|-------------|---------|
| 49 | 1 | 0 | 0 |

[All Problems](#) [All Types](#)

| | |
|---|----|
| 1 | 50 |
|---|----|

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|----|---------|---------|----------|---------|
| 99 | 0 | 0 | 4 | 0 |

[All Problems](#) [All Types](#)

| | |
|---|-----|
| 4 | 103 |
|---|-----|

Service Status Details For All Hosts

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---------------------|-------------------|--------|---------------------|-----------------|---------|--|
| bibmath | HTTP | OK | 11-08-2010 12:10:05 | 13d 18h 31m 50s | 1/4 | HTTP OK HTTP/1.1 200 OK - 3257 bytes in 2.280 seconds |
| | PING | OK | 11-08-2010 12:07:06 | 0d 10h 4m 9s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.32 ms |
| cro-rc1-ge-1-2-0-33 | PING | OK | 11-08-2010 12:08:07 | 0d 0h 8m 8s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.57 ms |
| irma-fw-in | PING | OK | 11-08-2010 12:10:07 | 41d 10h 17m 46s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 10.18 ms |
| | SSH | OK | 11-08-2010 12:10:05 | 67d 19h 18m 39s | 1/4 | SSH OK - OpenSSH_4.5p1 (protocole 2.0) |
| irma-fw-out | PING | OK | 11-08-2010 12:10:07 | 54d 17h 4m 20s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.25 ms |
| irma-fw-public | PING | OK | 11-08-2010 12:10:07 | 54d 20h 9m 58s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.35 ms |
| irma-hpc | PING | OK | 11-08-2010 12:10:08 | 54d 20h 9m 27s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.45 ms |
| | SSH | OK | 11-08-2010 12:10:05 | 56d 8h 42m 44s | 1/4 | SSH OK - Sun_SSH_1.1.3 (protocole 2.0) |
| irma-mac | PING | OK | 11-08-2010 12:10:08 | 54d 2h 26m 21s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.18 ms |
| irma-store | PING | OK | 11-08-2010 12:10:07 | 38d 10h 11m 18s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 4.55 ms |
| | SSH | OK | 11-08-2010 12:10:05 | 60d 22h 42m 26s | 1/4 | SSH OK - Sun_SSH_1.1.3 (protocole 2.0) |
| irma-sw1 | PING | OK | 11-08-2010 12:10:07 | 67d 19h 18m 41s | 1/3 | PING OK - Paquets perdus = 0%, RTA = 1.05 ms |
| | Uptime | OK | 11-08-2010 12:10:05 | 68d 20h 22m 22s | 1/3 | SNMP OK - Timeticks: (1373910543) 159 days, 0:25:05.43 |
| irma-sw102 | PING | OK | 11-08-2010 12:10:07 | 54d 20h 9m 39s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 0.64 ms |
| irma-sw11 | PING | OK | 11-08-2010 12:10:07 | 39d 0h 2m 30s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 2.44 ms |
| irma-sw12 | PING | OK | 11-08-2010 12:10:07 | 54d 17h 4m 26s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 1.47 ms |
| irma-sw13 | PING | OK | 11-08-2010 12:10:07 | 54d 20h 9m 39s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 2.48 ms |
| irma-sw14 | PING | OK | 11-08-2010 12:10:07 | 54d 2h 26m 1s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 9.48 ms |
| irma-sw15 | PING | OK | 11-08-2010 12:10:07 | 29d 14h 0m 6s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 1.95 ms |
| irma-sw16 | PING | OK | 11-08-2010 12:10:08 | 10d 18h 22m 47s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 1.82 ms |
| | SSH | OK | 11-08-2010 12:10:05 | 33d 18h 28m 2s | 1/4 | SSH OK - OpenSSH_4.3 (protocole 2.0) |
| irma0 | PING | OK | 11-08-2010 12:07:06 | 1d 11h 54m 9s | 1/4 | PING OK - Paquets perdus = 0%, RTA = 1.27 ms |
| | Printer_ieldirect | OK | 11-08-2010 12:10:04 | 0d 2h 31m 11s | 1/3 | Imprimante ok - ("Mode veille activ") |

INTERFACE – HOST GROUPS SUMMARY

Current Network Status
 Last Updated: Mon Nov 8 12:12:26 CET 2010
 Updated every 90 seconds
 Nagios® Core™ 3.2.0 - www.nagios.org
 Logged in as *nagiosadmin*

[View Service Status Detail For All Host Groups](#)
[View Host Status Detail For All Host Groups](#)
[View Status Overview For All Host Groups](#)
[View Status Grid For All Host Groups](#)

Host Status Totals

| Up | Down | Unreachable | Pending |
|----|------|-------------|---------|
| 49 | 1 | 0 | 0 |

| All Problems | All Types |
|--------------|-----------|
| 1 | 50 |

Service Status Totals

| Ok | Warning | Unknown | Critical | Pending |
|----|---------|---------|----------|---------|
| 99 | 0 | 0 | 4 | 0 |

| All Problems | All Types |
|--------------|-----------|
| 4 | 103 |

Status Summary For All Host Groups

| Host Group | Host Status Summary | Service Status Summary |
|---|---------------------|--|
| irma Servers (irma-servers) | 9 UP | 18 OK |
| Linux Servers (linux-servers) | 1 UP | 8 OK |
| Network Printers (network-printers) | 12 UP 1 DOWN | 45 OK 4 CRITICAL : 4 on Problem Hosts |
| Network Switches (switches) | 17 UP | 18 OK |

INSTALLATION

- Système Unix
(portage sur d'autres systèmes possible)
- Compilateur C, si compilation des sources
ou installation des packages
- Net-snmp
- Serveur Apache + PHP pour une interface web
- Un réseau configuré ☺



FICHIERS DE CONFIGURATION

18

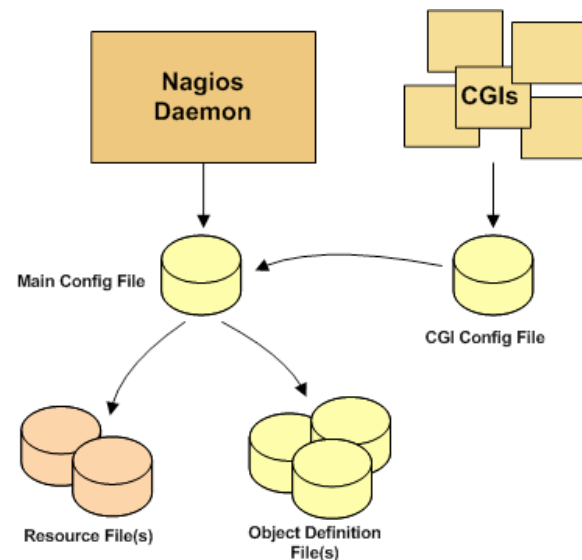
PREMIÈRE ÉTAPE : ANALYSE

- Cartographie du SI
- Quel objet – service est à superviser
- Grouper :
 - Entités logiques d'objets
 - Relations et interactions entre les objets
 - Déterminer les seuils d'alertes
 - Qui alerter...
- Créer/modifier les fichiers de configuration 😊

CONFIGURATION DE NAGIOS

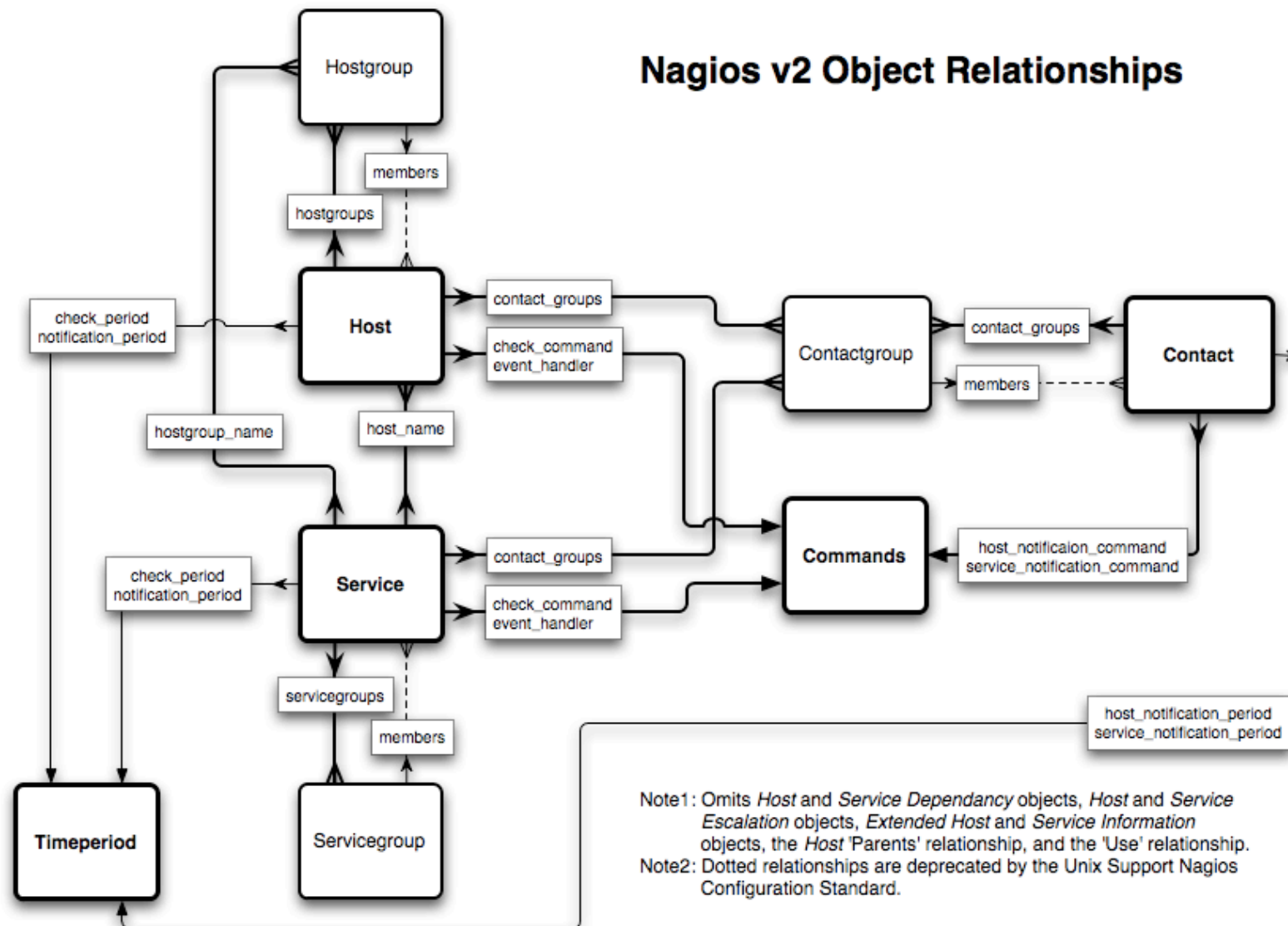
- Un « certain » nombre de fichiers de configuration:
 - nagios.cfg fichier de configuration principal
 - resources.cfg \$USERS macros (paths, users, passwd)
 - Fichier contact.cfg
 - Fichier contactgroups.cfg
 - Fichier host.cfg
 - Fichier hostgroups.cfg
 - Fichier services.cfg
 - Fichier timeperiods.cfg
 - Fichier command.cfg
 - Fichier checkcommand.cfg
 - Fichier dependencies.cfg
 - Fichier escalations.cfg

Et tout autre fichier nécessaire à votre organisation...



OBJET ET RELATION ...

Nagios v2 Object Relationships



FICHER DE CONFIGURATION : STRUCTURE

- Fichier = collection d'objet
- Commentaire = ';' ou '#'
- Objet :
 - *define object_definition*
 {
 name object_name
 use template_name
 propriété1 valeur
 propriété2 valeur
 ...
 }

FICHER NAGIOS/CONTACTS.CFG.

- Un contact définit une personne à prévenir dans les cas ou un « reporting » est demandé.
- On définit
 - le nom du contact (identifiant pour faire référence à ce contact dans les autres fichiers)
 - son alias
 - les périodes de notification par défaut
 - Les méthodes de notification par défaut
 - les éléments nécessaires pour communiquer avec ce contact

```
define contact
{
    contact_name nagios_adm
    alias nagios administrator
    service_notification_period 24x7
    host_notification_period 24x7
    service_notification_options w,u,c,r
    host_notification_options d,u,r
    service_notification_commands
        notify-by-email
    email nagios@sprv.cnrs.fr
}
```

FICHER NAGIOS/CONTACTGROUPS.CFG.

- Un groupe de contacts permet de regrouper un ou plusieurs contacts pour émettre des notifications.
- On définira pour chaque groupe créé :
 - un nom de groupe (qui permettra d'identifier le groupe dans les autres fichiers)
 - un alias
 - les membres du groupe (définis dans contact.cfg)

```
define contactgroup
{
    contactgroup_name GrContact1
    alias Groupe Numéro 1
    members root, nagios, robert
}
```


FICHER NAGIOS/HOSTS.CFG.

- Une définition d'hôte s'applique à un serveur "physique", une station de travail, un périphérique, un équipement, qui se trouve sur votre réseau.
- On le définit par:
 - le modèle à utiliser
 - le nom de la machine (pour y faire référence dans les fichiers de configuration)
 - un alias
 - l'adresse IP de la machine
 - la commande à exécuter pour vérifier l'accessibilité de la machine (définie dans nagios/checkcommands.cfg)
 - les paramètres de notification

```
define host
{
    use linux_server
    host_name www
    alias server web
    address 1.2.3.4
    check_command commande1
    max_check_attempts 20
    notification_interval 60

    notification_period 24x7
    notification_options d,u,r
}
```

FICHER NAGIOS/HOSTGROUPS.CFG

- Un groupe d'hôtes permet de regrouper un ou plusieurs hôtes pour simplifier les notifications.
- On définira ici pour chaque groupe créé :
 - un nom de groupe (permettant d'identifier le groupe dans les autres fichiers)
 - un alias
 - les groupes de contacts à y associer
 - une liste de machines à associer au groupe

```
define hostgroup
{
    hostgroup_name GrMachine1
    alias Groupe 1 de machines
    contact_groups GrContact1
    members host1, host2, host3
}
```

FICHER NAGIOS/SERVICES.CFG

- Un service identifie une ressource ou un service à surveiller sur une machine
- On définit:
 - le modèle à utiliser
 - l'identifiant de la machine concernée
 - le nom du service voulu
 - les paramètres liés à l'exécution de la vérification du service
 - le groupe de contact concerné par les notifications
 - les paramètres de notification
 - la commande à exécuter pour vérifier le bon fonctionnement du service (avec ses arguments)

```
define service
{
    use generic-service
    host_name Machine1
    service_description PING
    check_period 24x7
    max_check_attempts 3
    normal_check_interval 5
    retry_check_interval 1
    contact_groups GrContact1
    notification_interval 240
    notification_period 24x7
    notification_options c,r
    check_command check_ping
    100.0,20%!500.0,60%
}
```

LES OPTIONS

- Intervalles de temps : minutes
- Options de notification
 - Pour un **service** :
 - **w** = envoi de la notification pour un état WARNING
 - **u** = envoi de la notification pour un état UNKNOWN
 - **r** = envoi de la notification pour le retour à la normale
 - **n** (none)
 - Pour un **hôte** :
 - **d** = envoi de la notification pour un état DOWN
 - **u** = envoi de la notification pour un état UNREACHABLE
 - **r** = envoi de la notification pour le retour à la normale
 - **n** (none)

FICHER NAGIOS/TIMEPERIOD.CFG

- Définit une tranche horaire pour connaître la disponibilité d'un objet

```
define timeperiod
{
    timeperiod_name nonworkhours
    alias Non-Work Hours
    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
}
```

FICHER NAGIOS/CHECKCOMMAND.CFG

- Associe le nom d'une commande à un script avec ses paramètres

- define command

```
{  
  command_name    check_temperature  
  command_line    $USER1$/check_temperature  
                  $HOSTADDRESS$ $ARG1$ $ARG2$  
  
}
```

FICHER NAGIOS/DEPENDENCIES.CFG

- Définit la dépendance entre host ou service
- Supprime les cascades d'alertes
- Si un service ou un host tombe, les alertes des host et services qui en dépendent ne sont pas envoyés

FICHER NAGIOS/DEPENDENCIES.CFG

- define servicedependency
{
 dependent_host_name host_name
 dependent_service_description service_description
 host_name host_name
 service_description service_description
 execution_failure_criteria [o,w,u,c,n]
 notification_failure_criteria [o,w,u,c,n]
}
- define hostdependency
{
 dependent_host_name host_name
 host_name host_name
 notification_failure_criteria [o,d,u,n]
}

FICHER NAGIOS/ESCALATIONS.CFG

- Permet de définir une cascade d'alerte si un service ou un host vient à tomber
- Fonctionnalité optionnelle

FICHIER NAGIOS/ESCALATIONS.CFG

- define serviceescalation

```
{  
host_name host_name  
service_description service_description  
contact_groups contactgroup_name  
first_notification      #  
last_notification      #  
notification_interval  #  
}
```

- define hostescalation

```
{  
host_name host_name  
contact_groups contactgroup_name  
first_notification      #  
last_notification      #  
notification_interval  #  
}
```

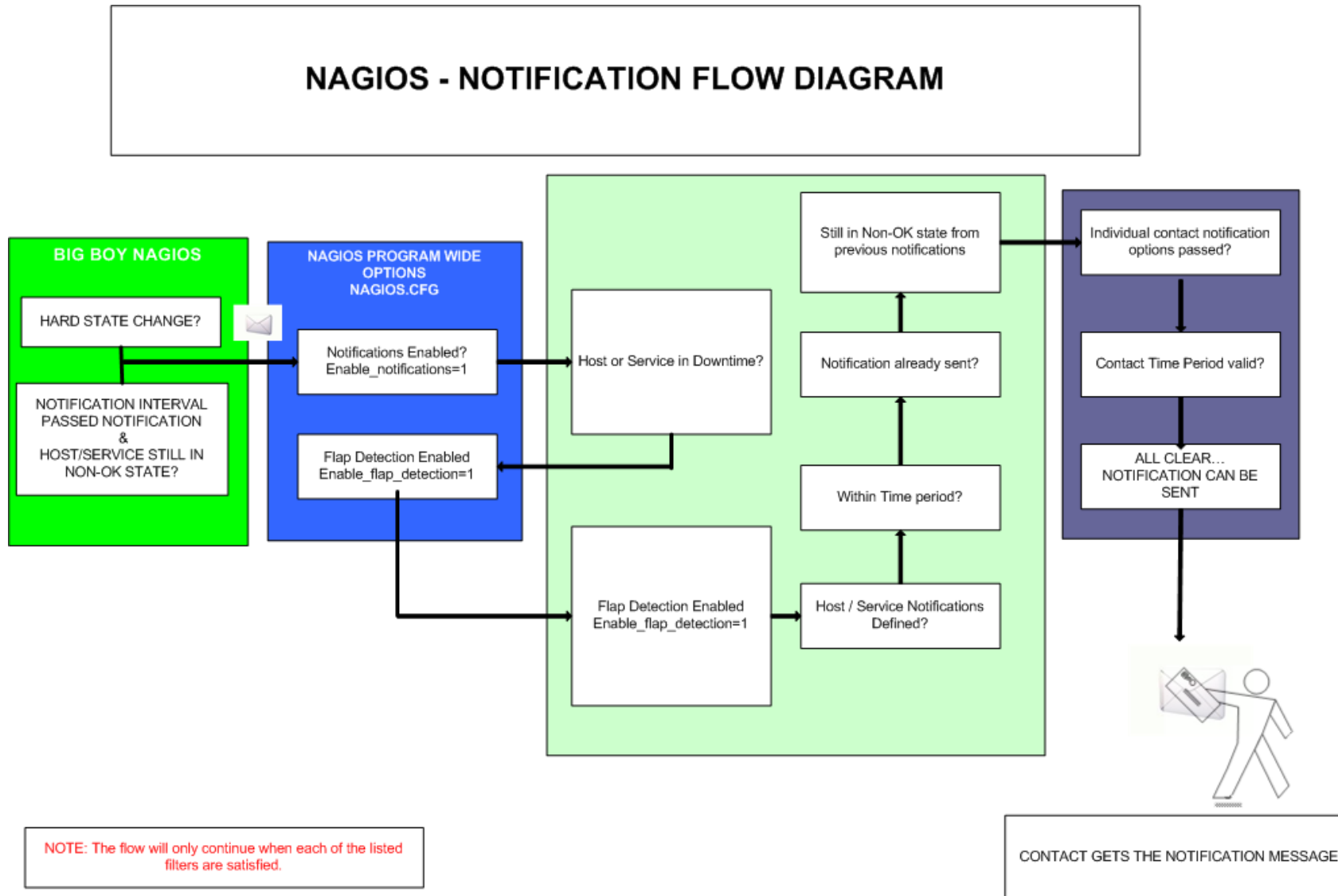
FICHER NAGIOS/ESCALATIONS.CFG

- Permet de définir une cascade d'alerte pour un groupe d'host si un des hosts du groupe vient à tomber
- Fonctionnalité optionnelle

```
Define hostgroupescalation
{
    hostgroup_name
        hostgroup_name
    contact_groups
        contactgroup_name
    first_notification      #
    last_notification      #
    notification_interval  #
}
```

NOTIFICATIONS – DIAG.

NAGIOS - NOTIFICATION FLOW DIAGRAM



LES PLUGINS NAGIOS

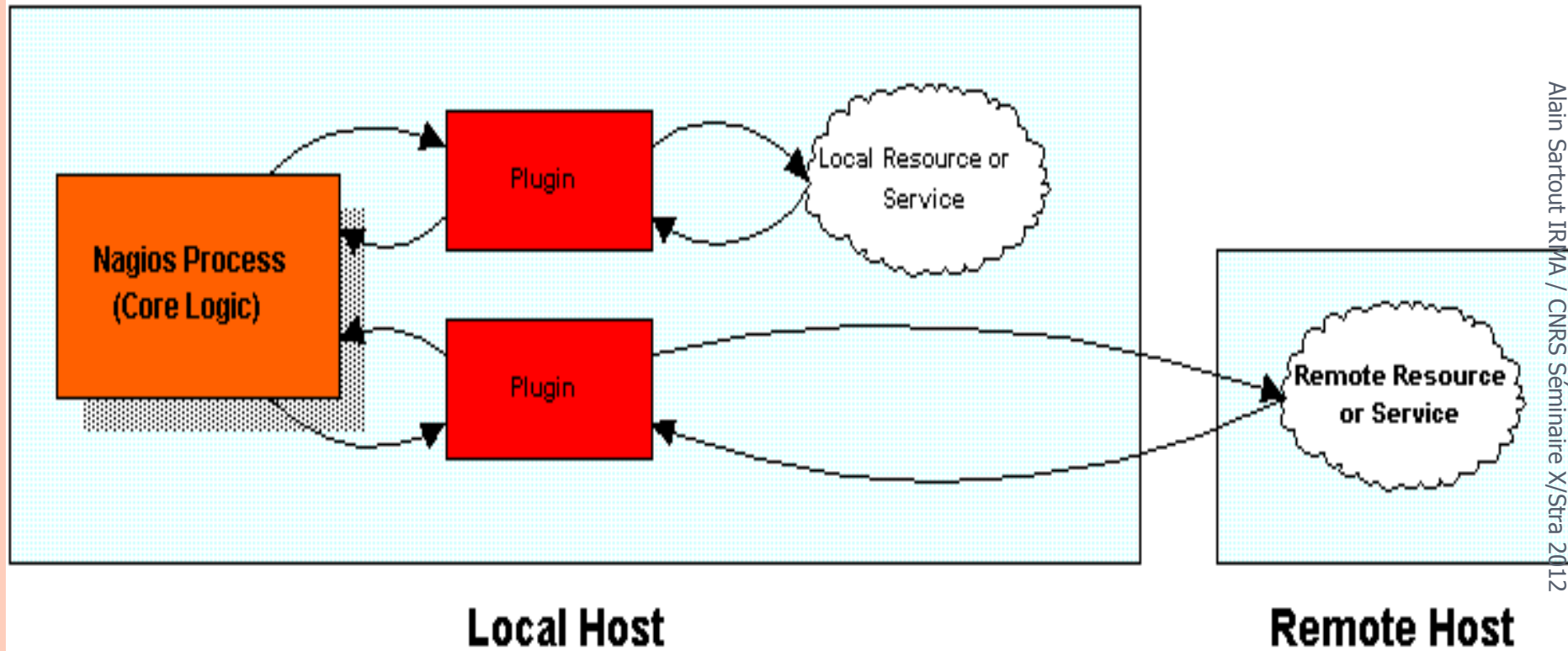


37

LES PLUGINS NAGIOS : PRÉSENTATION

- Pas de mécanisme interne dans Nagios pour vérifier l'état d'un hôte, un service, etc...
- Utilisation de programmes externes appelés plugins
- Les plugins permettent de contrôler une ressource ou un service local ou distant

LES PLUGINS NAGIOS : PRÉSENTATION



Alain Sartout IRIMA / CNRS Séminaire X/Stra 2012

LES PLUGINS NAGIOS : PRÉSENTATION

- Programmes exécutables ou scripts (perl, shell, etc...)
- Nagios teste la valeur retournée par le plugin pour savoir l'état de la ressource ou du service contrôlé
- N'importe qui peut développer son propre plugin afin de surveiller un service spécifique

LES PLUGINS NAGIOS : DÉVELOPPEMENT

- Peu importe le langage de programmation : C, shell, perl, ...
- Doit renvoyer une valeur entre 0 et 3 :
- Doit afficher un message court sur la sortie standard (1 ligne, max 80 caractères)

| Valeur | Statut |
|---------------|---------------|
| 0 | OK |
| 1 | Warning |
| 2 | Critical |
| 3 | Unknown |

PLUGINS : collection standard

- check_by_ssh
- check_disk
- check_disk_smb
- check_dns
- check_dummy
- check_flexlm
- check_ftp
- check_http
- check_imap
- check_ircd
- check_load
- check_log
- check_mailq
- check_mrtg
- check_mtrgtraf
- check_nagios
- check_nntp
- check_ntp
- check_nwstat
- check_overcr
- check_ping
- check_pop
- check_procs
- check_real
- check_rpc
- check_sensors
- check_smtp
- check_ssh
- check_swap
- check_tcp
- check_time
- check_udp
- check_users

PLUGIN : EXEMPLE

```
#!/bin/bash
# This script pings a host and compares
# critical and warning tresholds against
# avg rtt (ms)
# Syntax: nagios_check_ping.sh HOST CRITICAL
WARNING
# Example: nagios_check_ping.sh www.sunet.se
10 20

if [ ! -n "$1" ]
then
    echo "UNKNOWN: Missing argument HOSTNA
ME..."
    exit 3
fi

if [ ! -n "$2" ]
then
    echo "UNKNOWN: Missing argument WARNIN
G..."
    exit 3
fi

if [ ! -n "$3" ]
then
    echo "UNKNOWN: Missing argument CRITICA
L..."
    exit 3
fi
```

```
AVG=`ping -n -c 5 $1 | awk -F '/' ^rtt/ { print $5 } |
awk -F '!' '{ print $1; }`

if [ ! -n "$AVG" ]
then
    echo "CRITICAL: Error pinging"
    exit 2
elif [ $AVG -le "$2" ]
then
    SC="OK"
    EX=0
elif [ $AVG -le "$3" ]
then
    SC="WARNING"
    EX=1
else
    SC="CRITICAL"
    EX=2
fi

echo "$SC: Average response time is $AVG ms"
exit $EX
```

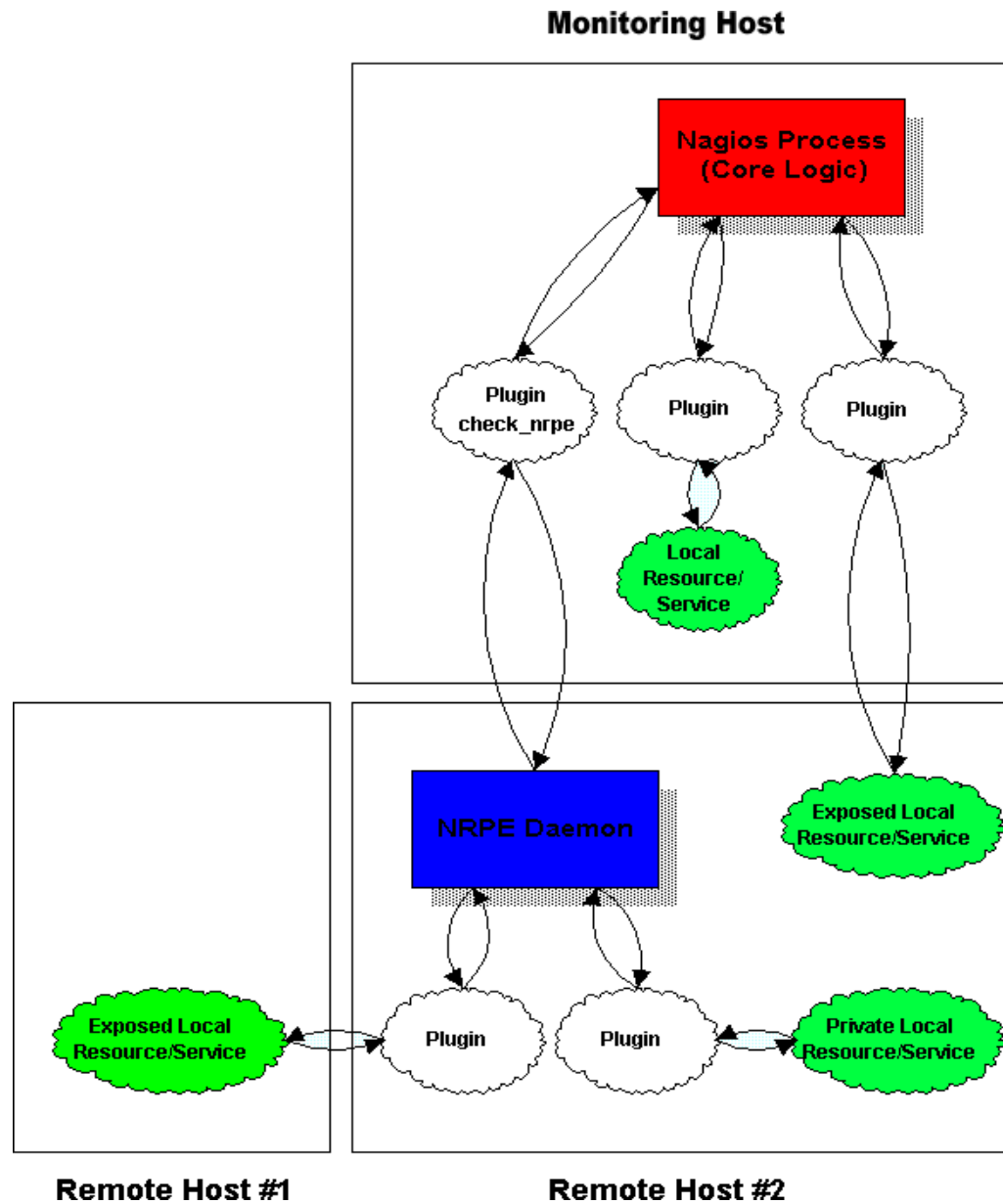
LES PLUGINS NAGIOS : EXÉCUTION À DISTANCE

- Utilisation de l'addon NRPE (Nagios Remote Plugin Executor)
- NRPE comprend un agent *nrpe* qui tourne sur la machine distante et un plugin *check_nrpe* sur la machine Nagios
- Le plugin *check_nrpe* fait une requête à l'agent en demandant l'exécution d'un plugin sur la machine où tourne l'agent

LES PLUGINS NAGIOS : EXÉCUTION À DISTANCE

- L'agent exécute le plugin demandé et renvoie le résultat au plugin `check_nrpe` de la machine Nagios
- Le plugin `check_nrpe` renvoie la sortie du plugin distant et le code de retour à Nagios comme si c'était le sien
- Équivalent : nagios « slave »

LES PLUGINS NAGIOS : EXÉCUTION À DISTANCE



LES PLUGINS NAGIOS : CONFIGURATION DE NAGIOS

- Dans les fichiers *services.cfg* et *hosts.cfg*, on indique la commande à utiliser pour contrôler un service ou une machine
- Ces commandes sont définies dans le fichier *checkcommands.cfg*. C'est dans ce fichier qu'est indiquée la ligne de commande à exécuter

MODIFICATION ET VÉRIFICATION

- Vérifier la syntaxe des fichiers de configuration
 - *nagios3 -v /etc/nagios3/nagios.cfg*
- Redémarrer le service nagios si modification d'un fichier de configuration
 - *service nagios3 restart*
- Accéder à l'interface web de nagios
 - *http://serveur.domaine.local/nagios3/*

