



Programme Opérations de registre avancées

NAGIOS



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Introduction

- Outil de mesure fondamental en matière de supervision active de la disponibilité des périphériques et des services.
- Il s'agit probablement du logiciel de supervision de réseau libre le plus utilisé.
- Nagios possède une interface réseau.
 - Il utilise des CGI en langage C offrant une rapidité et une extensibilité supérieures.
- Il peut prendre en charge des milliers de périphériques et de services.

Installation

Sous Debian/Ubuntu

```
# apt-get install nagios3
```

- Les fichiers sont installés ici :

```
/etc/nagios3
```

```
/etc/nagios3/conf.d
```

```
/etc/nagios-plugins/conf
```

```
/usr/share/nagios3/htdocs/images/logos
```

```
/usr/sbin/nagios3
```

```
/usr/sbin/nagios3stats
```

Adresse de l'interface web de Nagios :

<http://localhost/nagios3/>

Présentation générale

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
 - Unhandled
- Host Problems
 - Unhandled
- Network Outages

Show Host:

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

Reporting

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

Configuration

- View Config

Tactical Monitoring Overview

Last Updated: Thu Sep 3 15:37:09 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

Monitoring Performance

Service Check Execution Time: 0.01 / 4.07 / 0.115 sec
Service Check Latency: 0.02 / 0.25 / 0.117 sec
Host Check Execution Time: 0.01 / 0.13 / 0.018 sec
Host Check Latency: 0.01 / 0.28 / 0.137 sec
Active Host / Service Checks: 41 / 46
Passive Host / Service Checks: 0 / 0

Network Outages

0 Outages

Network Health

Host Health: ██████████
Service Health: ██████████

Hosts

0 Down	0 Unreachable	41 Up	0 Pending
--------	---------------	-------	-----------

Services

0 Critical	0 Warning	0 Unknown	46 Ok	0 Pending
------------	-----------	-----------	-------	-----------

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 All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled

Détail des services

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail**
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map

Service Problems

- Unhandled
- Host Problems
- Unhandled
- Network Outages

Show Host:

Comments

- Downtime

Process Info

- Performance Info
- Scheduling Queue

Reporting

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

Configuration

- View Config

Current Network Status

Last Updated: Thu Sep 3 14:46:07 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
41	0	0	0
All Problems		All Types	
0		41	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0
All Problems		All Types		
0		46		

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
DNS-ROOT	SSH	OK	2009-09-03 14:43:51	43d 0h 55m 19s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
ISP-DNS	SSH	OK	2009-09-03 14:41:21	16d 3h 57m 24s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
ISP-RTR	SSH	OK	2009-09-03 14:43:57	43d 5h 35m 13s	1/4	SSH OK - Cisco-1.25 (protocol 2.0)
NOC-TLD1	SSH	OK	2009-09-03 14:41:27	1d 0h 1m 59s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD2	SSH	OK	2009-09-03 14:44:04	1d 22h 44m 22s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD3	SSH	OK	2009-09-03 14:41:34	1d 22h 40m 58s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD4	SSH	OK	2009-09-03 14:44:10	1d 22h 44m 16s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD5	SSH	OK	2009-09-03 14:41:40	1d 22h 41m 46s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD6	SSH	OK	2009-09-03 14:44:17	1d 22h 44m 9s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD7	SSH	OK	2009-09-03 14:41:47	1d 22h 41m 39s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD8	SSH	OK	2009-09-03 14:44:23	1d 22h 44m 3s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD1	SSH	OK	2009-09-03 14:41:53	1d 0h 1m 33s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD2	SSH	OK	2009-09-03 14:44:30	1d 22h 43m 56s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD3	SSH	OK	2009-09-03 14:42:00	1d 22h 41m 26s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD4	SSH	OK	2009-09-03 14:44:36	1d 22h 43m 50s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD5	SSH	OK	2009-09-03 14:42:06	1d 22h 41m 20s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD6	SSH	OK	2009-09-03 14:44:43	1d 22h 43m 43s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)

Détail des hôtes

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail**
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Service Map
- 3-D Status Map

- Service Problems
 - Unhandled
- Host Problems
 - Unhandled
- Network Outages

Show Host:

- Comments
- Downtime

- Process Info
- Performance Info
- Scheduling Queue

Reporting

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

Configuration

- View Config

Current Network Status

Last Updated: Thu Sep 3 14:55:18 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as *guest*

[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
41	0	0	0
All Problems		All Types	
0		41	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0
All Problems		All Types		
0		46		

Host Status Details For All Host Groups

Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
DNS-ROOT	UP	2009-09-03 14:51:41	43d 1h 7m 0s	PING OK - Packet loss = 0%, RTA = 0.33 ms
ISP-DNS	UP	2009-09-03 14:51:41	16d 4h 11m 25s	PING OK - Packet loss = 0%, RTA = 0.29 ms
ISP-RTR	UP	2009-09-03 14:51:51	43d 5h 47m 40s	PING OK - Packet loss = 0%, RTA = 1.24 ms
NOG-TLD1	UP	2009-09-03 14:52:01	1d 0h 10m 56s	PING OK - Packet loss = 0%, RTA = 4.02 ms
NOG-TLD2	UP	2009-09-03 14:52:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.23 ms
NOG-TLD3	UP	2009-09-03 14:52:11	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 2.62 ms
NOG-TLD4	UP	2009-09-03 14:52:21	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.09 ms
NOG-TLD5	UP	2009-09-03 14:52:31	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 5.20 ms
NOG-TLD6	UP	2009-09-03 14:52:31	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 10.49 ms
NOG-TLD7	UP	2009-09-03 14:52:41	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 1.05 ms
NOG-TLD8	UP	2009-09-03 14:52:51	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 1.00 ms
NS1-TLD1	UP	2009-09-03 14:53:01	1d 0h 10m 26s	PING OK - Packet loss = 0%, RTA = 10.19 ms
NS1-TLD2	UP	2009-09-03 14:53:01	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 5.06 ms
NS1-TLD3	UP	2009-09-03 14:53:11	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.03 ms
NS1-TLD4	UP	2009-09-03 14:53:21	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.15 ms
NS1-TLD5	UP	2009-09-03 14:53:21	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 1.12 ms
NS1-TLD6	UP	2009-09-03 14:53:31	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.06 ms
NS1-TLD7	UP	2009-09-03 14:53:41	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 1.11 ms
NS1-TLD8	UP	2009-09-03 14:53:51	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.18 ms
TLD1-RTR	UP	2009-09-03 14:53:51	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 2.22 ms
TLD2-RTR	UP	2009-09-03 14:54:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.38 ms

Vue d'ensemble des groupes d'hôtes

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map

Service Problems

- Unhandled

Host Problems

- Unhandled

Network Outages

Show Host:

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Reporting

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

Configuration

- View Config

Current Network Status

Last Updated: Thu Sep 3 14:55:28 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

[View Service Status Detail For All Host Groups](#)
[View Host Status Detail 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
41	0	0	0
All Problems		All Types	
0		41	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0
All Problems		All Types		
0		46		

Service Overview For All Host Groups

TRTI TLD1 Servers, Virtual Machines, Routers (TLD1)

Host	Status	Services	Actions
NOC-TLD1	UP	1 OK	
NS1-TLD1	UP	1 OK	
TLD1-RTR	UP	1 OK	
TRTI-TLD1	UP	1 OK	

TRTI TLD2 Servers, Virtual Machines, Routers (TLD2)

Host	Status	Services	Actions
NOC-TLD2	UP	1 OK	
NS1-TLD2	UP	1 OK	
TLD2-RTR	UP	1 OK	
TRTI-TLD2	UP	1 OK	

TRTI TLD3 Servers, Virtual Machines, Routers (TLD3)

Host	Status	Services	Actions
NOC-TLD3	UP	1 OK	
NS1-TLD3	UP	1 OK	
TLD3-RTR	UP	1 OK	
TRTI-TLD3	UP	1 OK	

TRTI TLD4 Servers, Virtual Machines, Routers (TLD4)

Host	Status	Services	Actions
NOC-TLD4	UP	1 OK	
NS1-TLD4	UP	1 OK	
TLD4-RTR	UP	1 OK	
TRTI-TLD4	UP	1 OK	

TRTI TLD5 Servers, Virtual Machines, Routers (TLD5)

Host	Status	Services	Actions
NOC-TLD5	UP	1 OK	
NS1-TLD5	UP	1 OK	
TLD5-RTR	UP	1 OK	
TRTI-TLD5	UP	1 OK	

TRTI TLD6 Servers, Virtual Machines, Routers (TLD6)

Host	Status	Services	Actions
NOC-TLD6	UP	1 OK	
NS1-TLD6	UP	1 OK	
TLD6-RTR	UP	1 OK	
TRTI-TLD6	UP	1 OK	

TRTI TLD7 Servers, Virtual Machines, Routers (TLD7)

Host	Status	Services	Actions
NOC-TLD7	UP	1 OK	
NS1-TLD7	UP	1 OK	

TRTI TLD8 Servers, Virtual Machines, Routers (TLD8)

Host	Status	Services	Actions
NOC-TLD8	UP	1 OK	
NS1-TLD8	UP	1 OK	

TRTI Management Virtual Machines (VM-mgmt)

Host	Status	Services	Actions
DNS-ROOT	UP	1 OK	
ISP-DNS	UP	1 OK	

Vue d'ensemble des groupes de services

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
 - Unhandled
- Host Problems
 - Unhandled
- Network Outages

Show Host:

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

Reporting

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

Configuration

- View Config

Current Network Status

Last Updated: Fri Sep 4 13:29:20 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

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

Host Status Totals

Up	Down	Unreachable	Pending
41	0	0	0
All Problems		All Types	
0		41	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
53	0	0	1	0
All Problems		All Types		
1		54		

Service Overview For All Service Groups

TLD Servers running Nagios (NAGIOS)

Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	  
NS1-TLD2	UP	1 OK	  
NS1-TLD3	UP	1 OK	  
NS1-TLD4	UP	1 OK	  
NS1-TLD5	UP	1 OK	  
NS1-TLD6	UP	1 OK	  
NS1-TLD7	UP	1 OK	  
NS1-TLD8	UP	1 OK	  

TLD Servers running SSH (SSH)

Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	  
NS1-TLD2	UP	1 CRITICAL	  
NS1-TLD3	UP	1 OK	  
NS1-TLD4	UP	1 OK	  
NS1-TLD5	UP	1 OK	  
NS1-TLD6	UP	1 OK	  
NS1-TLD7	UP	1 OK	  
NS1-TLD8	UP	1 OK	  

nsr@apricot 2010

Schéma en grappe de l'arborescence

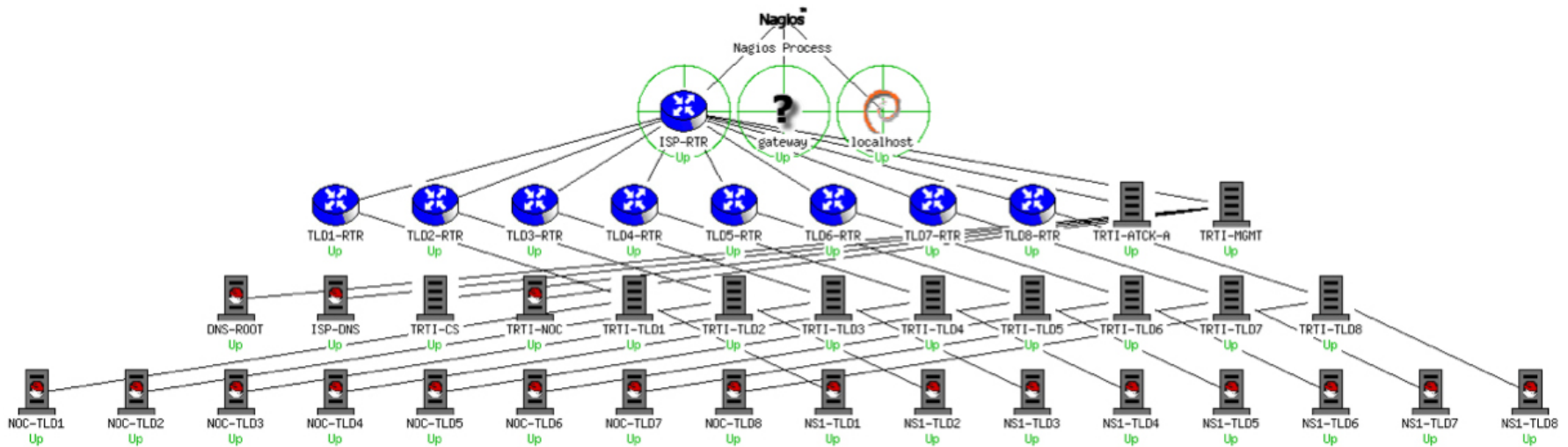
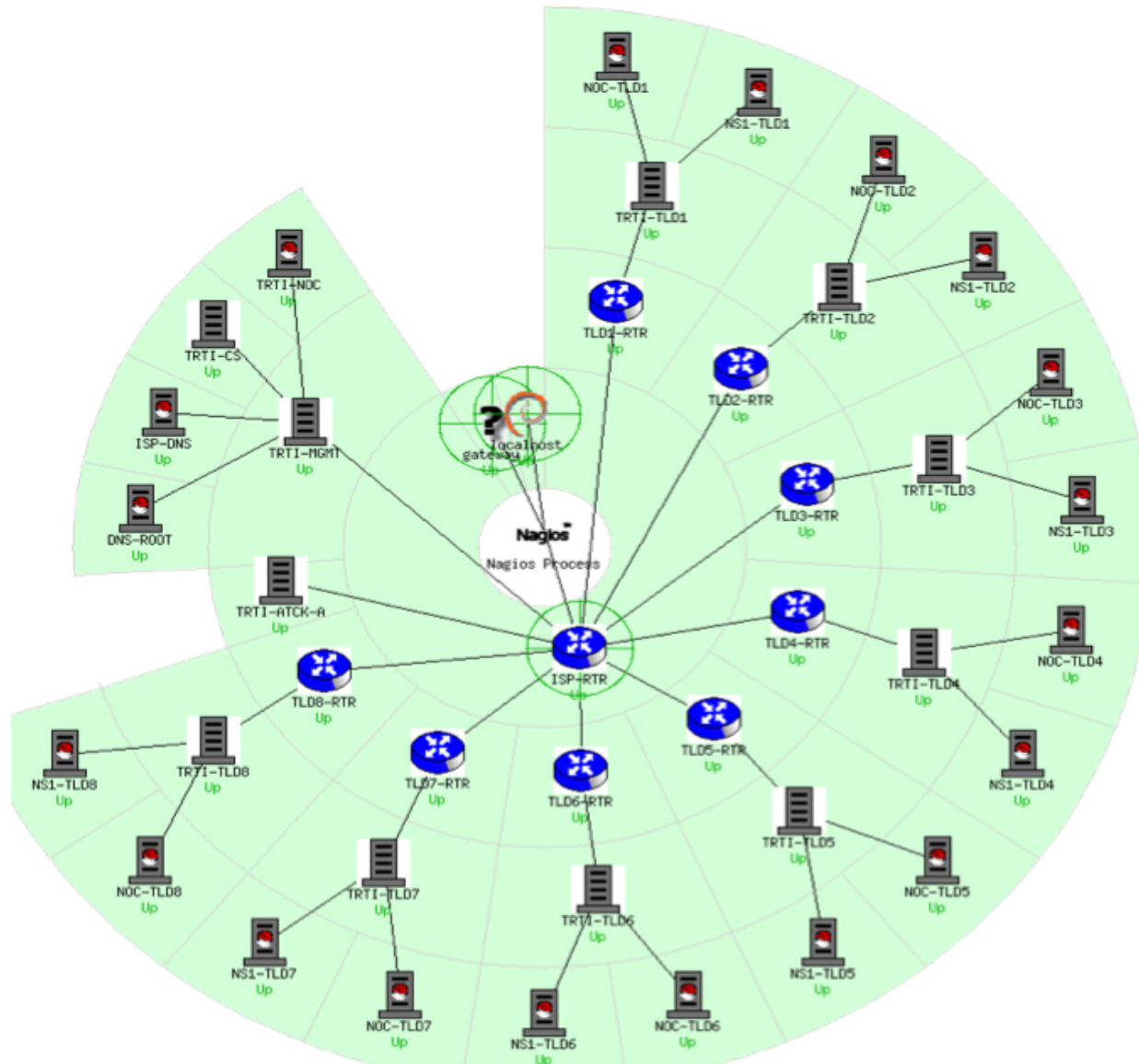
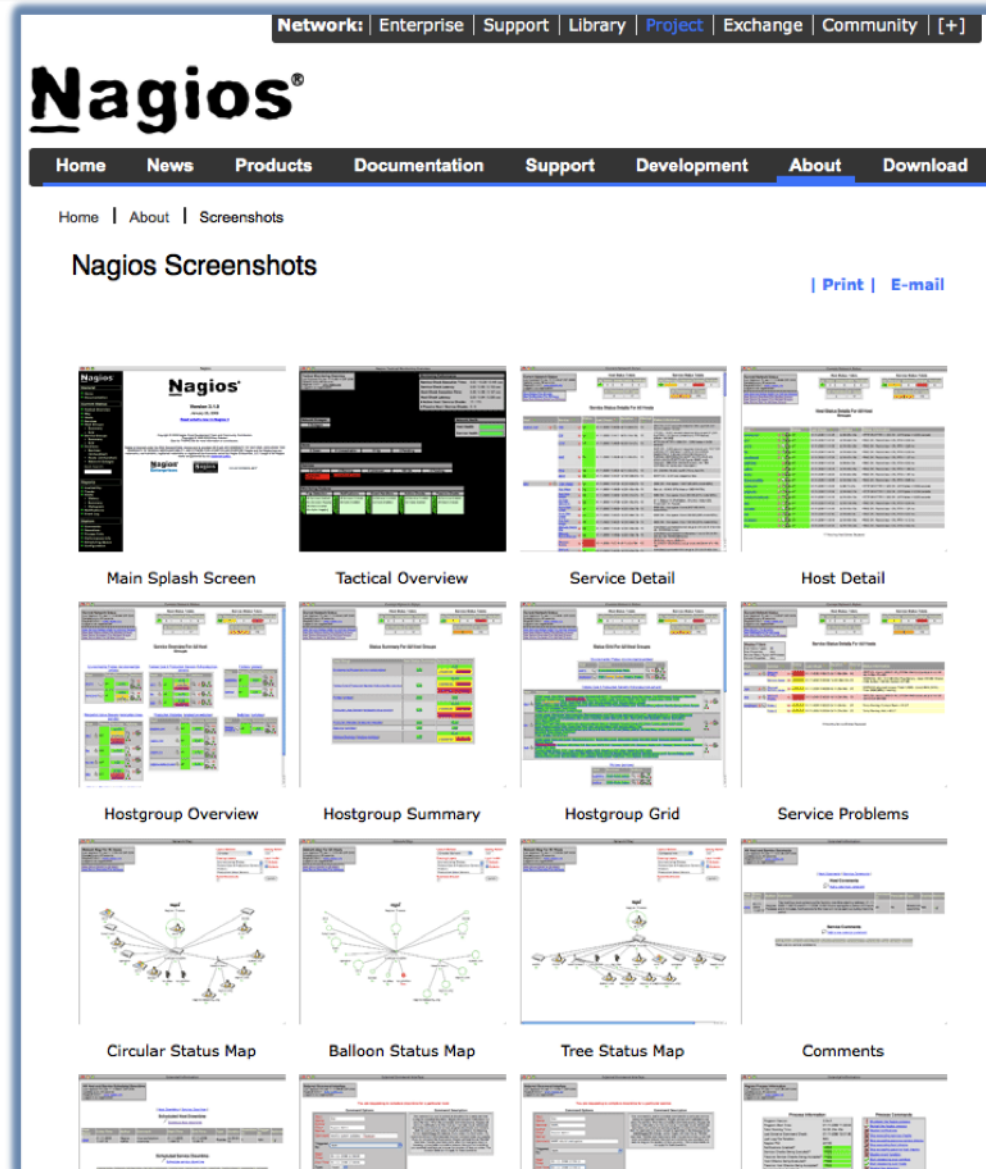


Schéma circulaire



Autres captures d'écran



Bien d'autres captures d'écran Nagios à l'adresse :

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

Fonctions

- La vérification des disponibilités est déléguée aux plugins :
 - l'architecture du produit est suffisamment simple pour permettre d'écrire facilement de nouveaux plugins dans le langage de votre choix
 - il existe un nombre considérable de plugins.
- Nagios s'appuie sur des vérifications et des embranchements parallèles.
 - La version 3 de Nagios s'accomplit mieux de ces tâches.

Fonctions (suite)

- Fonctions de vérification intelligentes : Nagios s'efforce de répartir la charge de supervision du serveur (grands sites) ainsi que la charge imposée aux périphériques supervisés.
- Configuration sous la forme de fichiers texte simples pouvant être très détaillés et reposant sur des modèles.
- Nagios lit sa configuration à partir de tout un répertoire. Vous restez maître de la définition des différents fichiers.

Fonctions (suite)

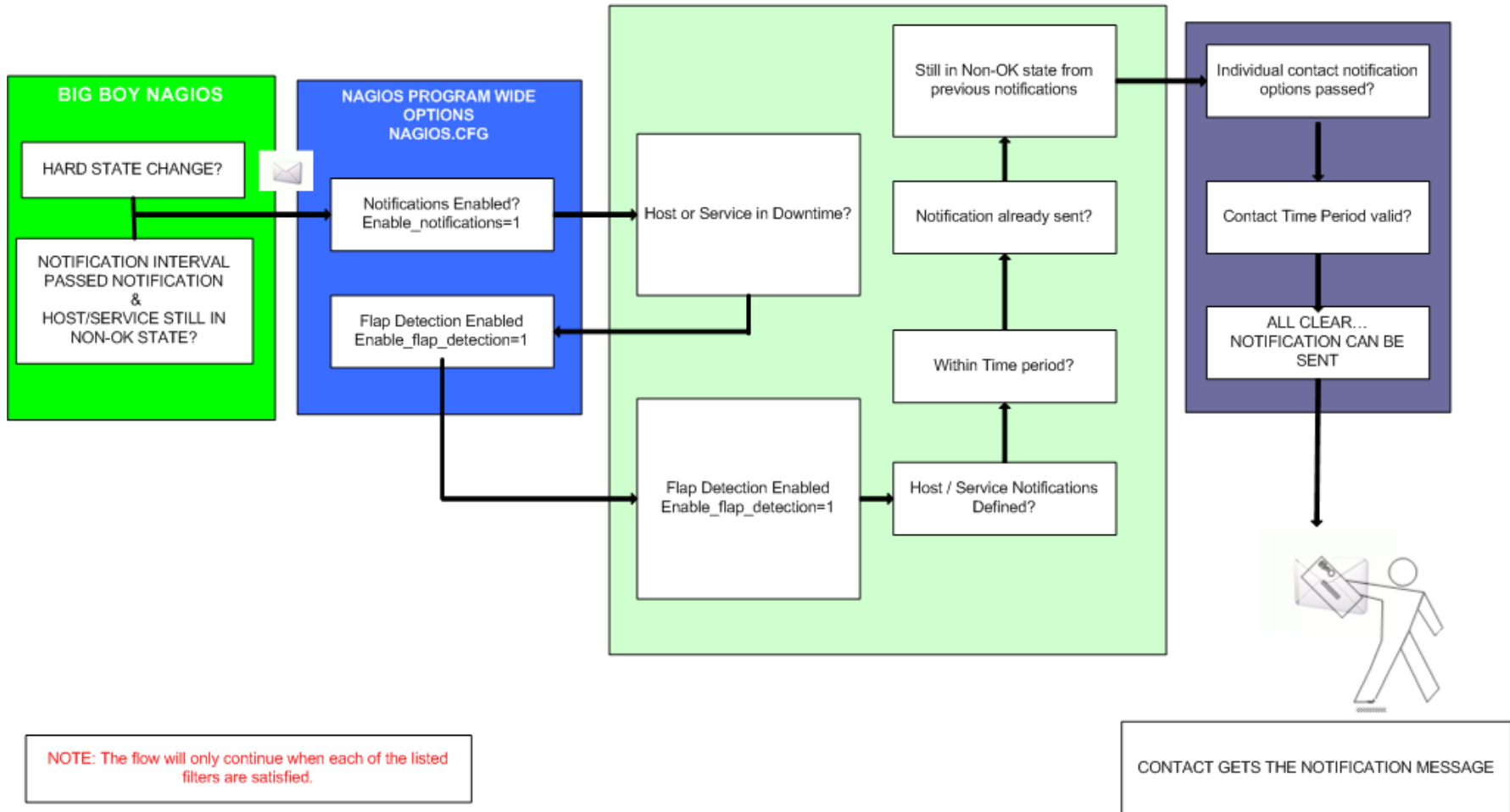
- Se base sur la topologie pour identifier les dépendances :
 - Nagios discerne ce qui est arrêté de ce qui n'est pas disponible, évitant ainsi des vérifications superflues.
- Nagios permet de définir le mode d'envoi des notifications en fonction de différents paramètres :
 - contacts et listes de contacts
 - périphériques et groupes de périphériques
 - services et groupes de services
 - horaires de personnes ou de groupes
 - état d'un service.

Et ce n'est pas tout...

Etats du service :

- Vous disposez des options de notification suivantes lorsque vous configurez un service :
 - **d**: DOWN : service interrompu (indisponible)
 - **u**: UNREACHABLE : l'hôte n'est pas visible
 - **r**: RECOVERY : (OK) l'hôte est en train de récupérer
 - **f**: FLAPPING : oscillation, l'hôte démarre ou s'interrompt ou son état est indéterminé
 - **n**: NONE : ne pas envoyer de notifications.

NAGIOS - NOTIFICATION FLOW DIAGRAM



Des fonctions et encore des fonctions...

- Permet de prendre acte d'un événement
 - l'utilisateur peut ajouter des commentaires avec l'interface graphique
- Permet de définir des périodes de maintenance
 - par périphérique ou groupe de périphériques
- Gère des statistiques de disponibilité.
- ✓ *Permet de détecter les oscillations et d'éviter des notifications supplémentaires.*
- Offre plusieurs méthodes de notification :
 - courrier électronique, SMS, incrustations d'écran, audio, etc...

Comment se déroulent les vérifications

- Un noeud/hôte/périphérique se compose d'un ou de plusieurs services (PING, HTTP, MYSQL, SSH, etc.)
- Nagios vérifie périodiquement chaque service de chaque noeud et détermine si son état a changé.
Les changements d'état sont :
 - CRITICAL (critique)
 - WARNING (alerte)
 - UNKNOWN (inconnu)
- A chacun de ces changements d'état vous pouvez associer :
 - des options de notification (comme précédemment)
 - des gestionnaires d'événements.

Comment se déroulent les notifications (suite)

Paramètres

- intervalle de vérification normal
- intervalle avant revérification
- nombre maximal de vérifications
- période de chaque vérification
- Les noeuds ne sont vérifiés que si les services répondent (et si cela a été configuré).
 - Un noeud peut être :
 - DOWN (arrêté)
 - UNREACHABLE (inaccessible).

Comment se déroulent les notifications (suite)

Cela peut prendre un moment avant que l'état d'un hôte passe à "DOWN" car Nagios effectue d'abord une vérification des services avant de vérifier les noeuds.

Nagios vérifie par défaut les noeuds 3 fois avant de les mettre à l'état "DOWN".

Vous pouvez naturellement modifier ces règles.

La notion de “parents”

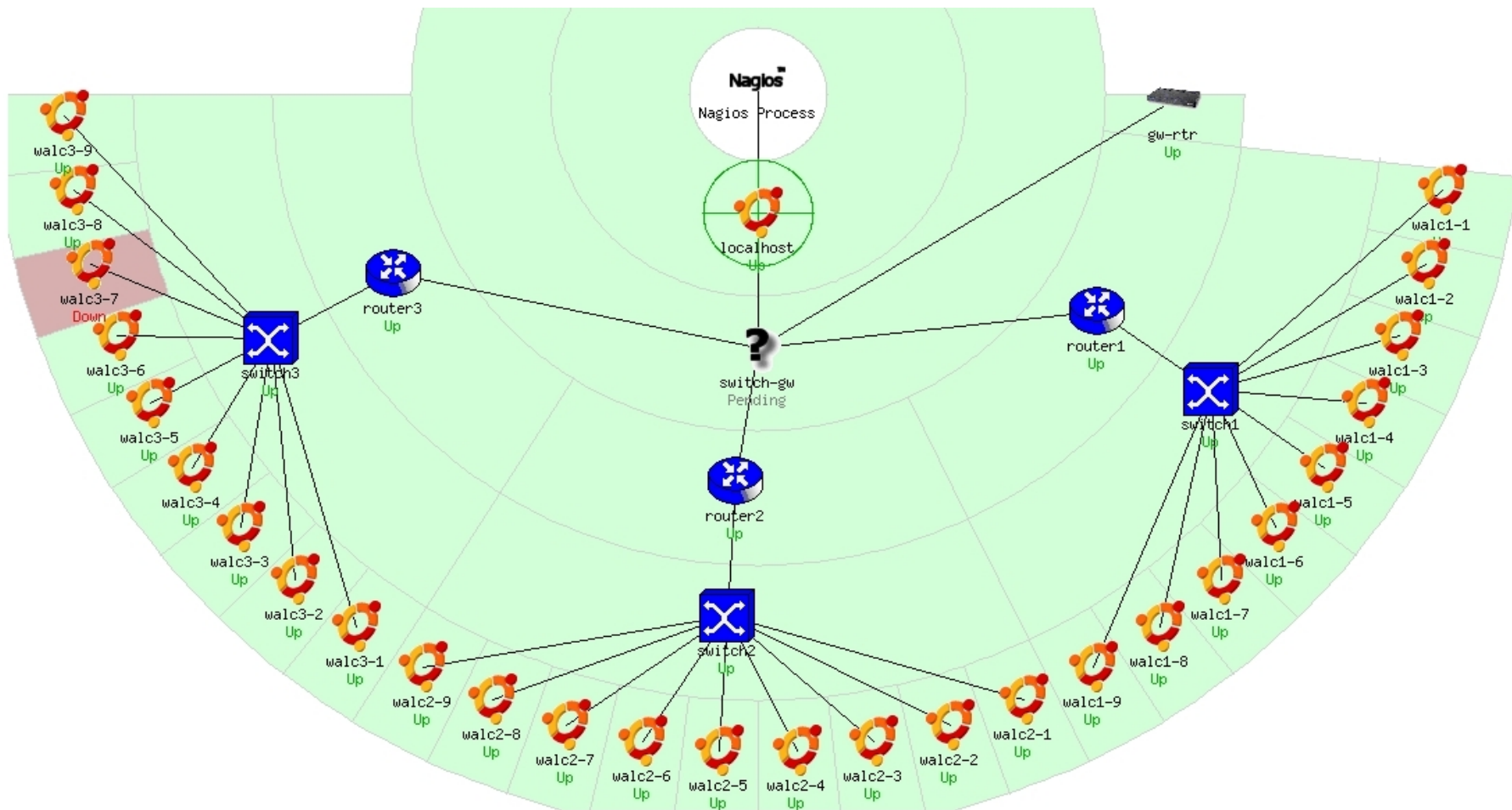
Les noeuds peuvent avoir des parents :

- ainsi, le parent d'un PC connecté à un commutateur serait le commutateur
- ceci nous permet de spécifier les dépendances existant entre machines, commutateurs, routeurs, etc. du réseau
- on évite ainsi que Nagios n'envoie des alarmes chaque fois qu'un parent ne répond pas
- un même noeud peut avoir plusieurs parents.

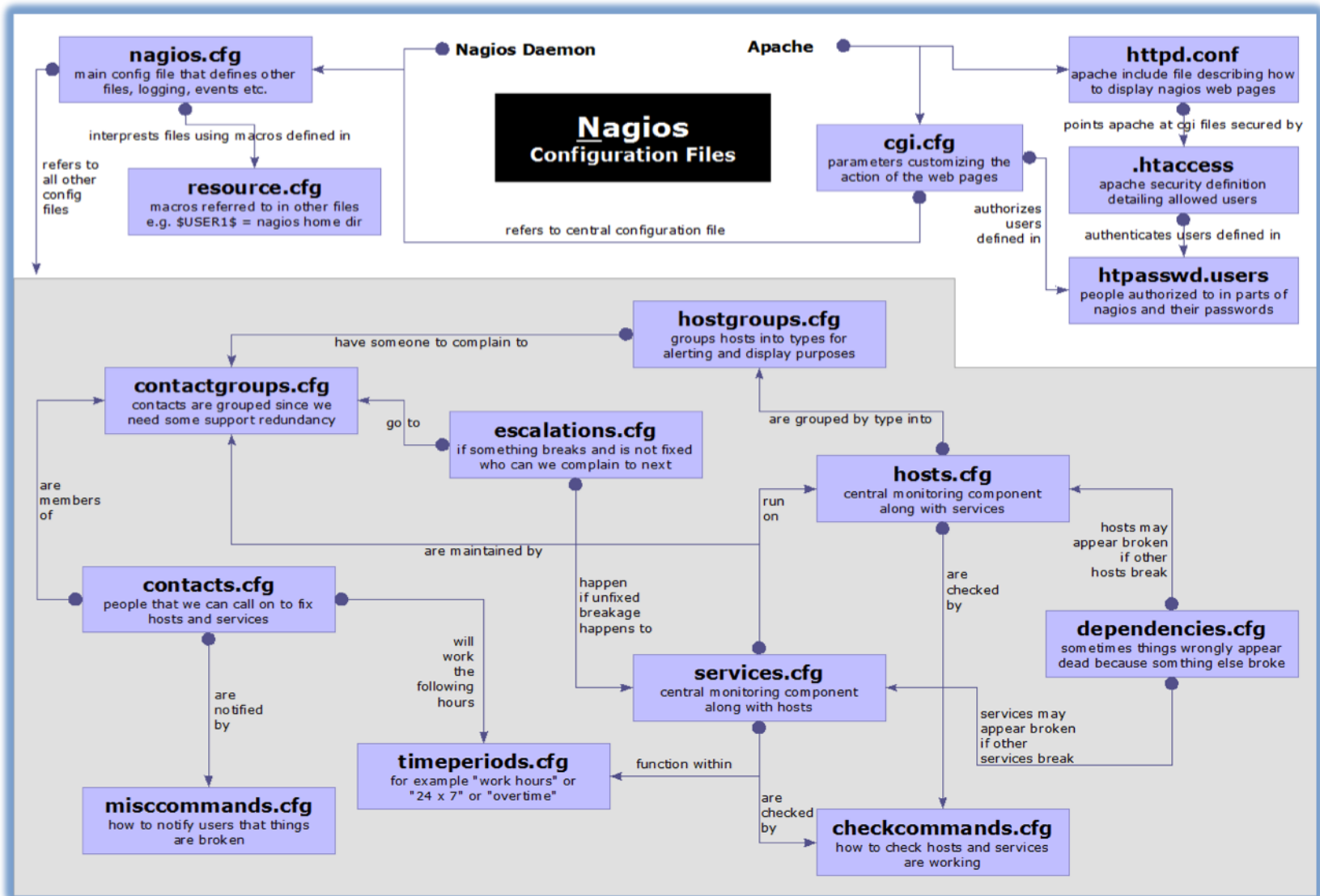
Point de vue du réseau

- De l'emplacement de votre serveur Nagios dépendra votre point de vue du réseau.
- Nagios autorise des machines Nagios parallèles en d'autres points du réseau.
- Il est souvent préférable de placer le serveur Nagios en bordure et non au coeur du réseau.

Point de vue de réseau



Fichiers de configuration Nagios



Fichiers de configuration

Situés dans `/etc/nagios3/`

Les fichiers importants incluent :

- `cgi.cfg` Contrôle de l'interface web et des options de sécurité.
- `commands.cfg` Commandes utilisées par Nagios pour les notifications.
- `nagios.cfg` Fichier de configuration principal.
- `conf.d/*` Toutes les autres configurations !

Fichiers de configuration (suite)

Dans conf.d/* (*exemple uniquement*)

- `contacts_nagios3.cfg` Utilisateurs et groupes
- `generic-host_nagios2.cfg` Modèle d'hôte par défaut
- `generic-service_nagios2.cfg` Modèle de service par défaut
- `hostgroups_nagios2.cfg` Groupes de noeuds
- `services_nagios2.cfg` Services à vérifier
- `timeperiods_nagios2.cfg` Quand contrôler et à qui adresser les notifications

Fichiers de configuration (suite)

Autres fichiers de configuration dans conf.d :

- `host-gateway.cfg` Définition de route par défaut
- `extinfo.cfg` Informations supplémentaires sur les noeuds
- `servicegroups.cfg` Groupes de noeuds et de services
- `localhost.cfg` Définit le serveur Nagios
- `pcs.cfg` Exemple de définitions de PC (hôtes)
- `switches.cfg` Définitions de commutateurs (hôtes)
- `routers.cfg` Définitions de routeurs (hôtes)

Plugins préinstallés dans Ubuntu

check_bgpstate	check_hpjd	check_mailq	check_overcr
check_ssmtp	check_breeze	check_http	check_mrtg
check_pgsql	check_swap	check_by_ssh	check_icmp
check_mrtgtraf	check_ping	check_tcp	check_clamd
check_ide_smart	check_mysql	check_pop	check_time
check_cluster	check_ifoperstatus	check_mysql_query	
check_procs	check_udp	check_dhcp	check_ifstatus
check_nagios	check_radius	check_ups	check_dig
check_imap	check_nntp	check_real	check_users
check_disk	check_ircd	check_nntps	check_rpc

Détail de la configuration principale

Paramètres généraux

Fichier : `/etc/nagios3/nagios.cfg`

- Indique où se trouvent les autres fichiers de configuration
- Comportement général de Nagios :
 - dans le cadre d'une grosse installation, ce fichier permet d'affiner l'installation.
 - Voir : *Tunning Nagios for Maximum Performance*
http://nagios.sourceforge.net/docs/2_0/tuning.html

Configuration CGI

`/etc/nagios3/cgi.cfg`

- vous pouvez changer de répertoire CGI si vous le souhaitez
- authentication et autorisation d'utilisation de Nagios :
 - Activation de l'authentification par le mécanisme `htpasswd` d'Apache ou par `RADIUS` ou `LDAP`.
 - Les variables suivantes permettent d'affecter des droits aux utilisateurs :
 - `authorized_for_system_information`
 - `authorized_for_configuration_information`
 - `authorized_for_system_commands`
 - `authorized_for_all_services`
 - `authorized_for_all_hosts`
 - `authorized_for_all_service_commands`
 - `authorized_for_all_host_commands`

Périodes de temps

Définition de périodes de base pour les vérification, les notifications, etc.

- Par défaut : 24 x 7
- Paramétrable selon les besoins – vérifications en semaine uniquement, par exemple.
- Possibilité de prévoir de nouvelles périodes, par exemple “hors horaires d’ouverture” par exemple, etc.

```
# '24x7'
define timeperiod{
    timeperiod_name 24x7
    alias            24 Hours A Day, 7 Days A Week
    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
}
```

Configuration des vérifications de service/d'hôtes :

Définition de la commande “host-alive”

```
# 'check-host-alive' command definition
define command{
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 2000.0,60% -c
5000.0,100% -p 1 -t 5
}
```

- située dans /etc/nagios-plugins/config, et ajustée dans /etc/nagios3/conf.d/services_nagios2.cfg
- bien qu'il s'agisse d'une vérification de “service” ou “d'hôte”, Nagios y fait référence en tant que “commande”.

Commandes de notification

Vous pouvez utiliser toutes les commandes souhaitées. Nous utiliserons ceci pour produire des tickets dans RT.

```
# 'notify-by-email' command definition
define command{
    command_name      notify-by-email
    command_line      /usr/bin/printf "%b" "Service: $SERVICEDESC$\nHost:
$HOSTNAME$\nIn: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\nInfo: $SERVICEOUTPUT$\nDate: $SHORTDATETIME$" | /bin/mail
-s '$NOTIFICATIONTYPE$: $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$'
$CONTACTEMAIL$
```

```
From: nagios@nms.localdomain
To: grupo-redes@localdomain
Subject: Host DOWN alert for switch1!
Date: Thu, 29 Jun 2006 15:13:30 -0700
```

```
Host: switch1
In: Core_Switches
State: DOWN
Address: 111.222.333.444
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds
```

Configuration de noeuds et de services

Basée sur des modèles :

- évite de perdre du temps en répétitions
- similaire à la programmation orientée objets

Création de modèles par défaut avec des paramètres par défaut pour :

- un noeud générique
- un service générique
- un contact générique

Modèle de noeud générique

```
define host{
    name                generic-host
    notifications_enabled 1
    event_handler_enabled 1
    flap_detection_enabled 1
    process_perf_data 1
    retain_status_information 1
    retain_nonstatus_information 1
    check_command        check-host-alive
    max_check_attempts   5
    notification_interval 60
    notification_period   24x7
    notification_options  d,r
    contact_groups        nobody
    register               0
}
```

Configuration de noeuds individuels

```
define host{  
    use                generic-host  
    host_name          switch1  
    alias              Core_switches  
    address            192.168.1.2  
    parents            router1  
    contact_groups     switch_group  
}
```

Configuration de services génériques

```
define service{
    name                                generic-service
    active_checks_enabled                1
    passive_checks_enabled               1
    parallelize_check                    1
    obsess_over_service                  1
    check_freshness                      0
    notifications_enabled                1
    event_handler_enabled                1
    flap_detection_enabled                1
    process_perf_data                    1
    retain_status_information             1
    retain_nonstatus_information          1
    is_volatile                          0
    check_period                         24x7
    max_check_attempts                   5
    normal_check_interval                 5
    retry_check_interval                  1
    notification_interval                 60
    notification_period                   24x7
    notification_options                  c,r
    register                             0
}
```

Configuration de services individuels

```
define service{  
    host_name          switch1  
    use                generic-service  
    service_description PING  
    check_command      check-host-alive  
    max_check_attempts 5  
    normal_check_interval 5  
    notification_options c,r,f  
    contact_groups      switch-group  
}
```

Configuration de groupes de services

```
# check that ssh services are running
define service {
    hostgroup_name      ssh-servers
    service_description SSH
    check_command        check_ssh
    use                  generic-service
    notification_interval 0 ; set > 0 if you want to be renotified
}
```

La description de service est importante si vous comptez créer des groupes de services. Voici un exemple de définition de groupe :

```
define servicegroup{
    servicegroup_name  Webmail
    alias               web-mta-storage-auth
    members             srvr1,HTTP,srvr1,SMTP,srvr1,POP,srvr1,IMAP,
                      srvr1,RAID,srvr1,LDAP, srvr2,HTTP,srvr2,SMTP,
                      srvr2,POP,srvr2,IMAP,srvr2,RAID,srvr2,LDAP
}
```

Messages d'alerte et sms

- Il est important d'intégrer à Nagios un dispositif d'avertissement opérationnel en dehors des heures de travail :
 - les problèmes se posent en dehors de la journée de travail... (injuste mais vrai)
- Impératif : un dispositif de SMS ou de messages indépendant du réseau :
 - tel qu'un modem et une ligne téléphonique
 - des progiciels tels que sendpage, qpage ou gnokii qui peuvent être utiles.

Références

- **Site web de Nagios**
<http://www.nagios.org/>
- **Site de plugins Nagios**
<http://sourceforge.net/projects/nagiosplug/>
- *Nagios System and Network Monitoring*, Wolfgang Barth, un bon ouvrage sur Nagios
- **Site de plugins Nagios non officiel**
<http://www.nagiosexchange.org/>
- **Tutoriel Debian sur Nagios**
<http://www.debianhelp.co.uk/nagios.htm>
- **Support commercial pour Nagios**
<http://www.nagios.com/>