Gestion et Supervision de Réseau

NAGIOS

Introduction

Outils de surveillance réseau

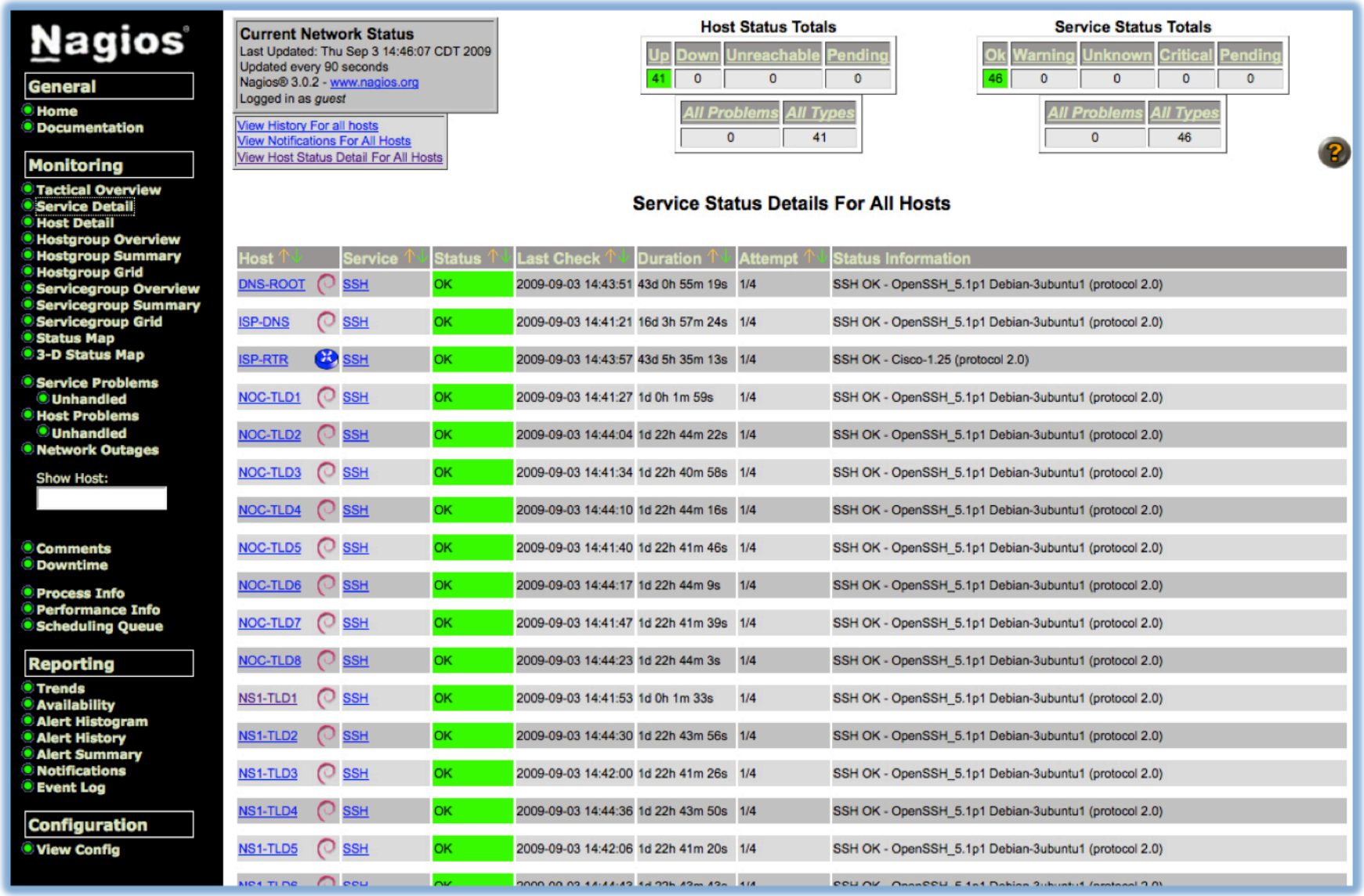
- Disponibilité
- Fiabilité
- Performances

Nagios surveille activement la disponibilité des machines et services

Introduction

- Probablement le logiciel libre de surveillance réseau le plus utilisé.
- Offre une interface web pour visualiser les états, naviguer l'historique, prévoir une fenêtre de maintenance, etc.
- Envoie des alertes via le mail. Peut être configuré pour utiliser d'autres mécanismes, tels que le SMS.

Détail des services



Caractéristiques

- Détermine les dépendances à partir de la topologie.
  - Fait la distinction entre ce qui est *"down"* (en panne) et ce qui est *"unreachable"* (inaccessible). Évite d'exécuter des contrôles inutiles et d'émettre des alarmes redondantes
- Vous permet de définir le mode d'envoi des notifications en fonction d'une combinaison des éléments suivants :
  - Contacts et listes de contacts
  - Équipements et groupes d’équipements
  - Services et groupes de services
  - Heures définies par personnes ou groupes
  - L'état d'un service.

Plugins (greffons)

Des plugins sont utilisés pour surveiller les services et périphériques :

- L'architecture Nagios est assez simple et permet d'écrire de nouveaux plugins de façon relativement facile dans le langage de votre choix.
- Il y a ***beaucoup, beaucoup*** de plugins disponibles (des milliers).
  - ✓ http://exchange.nagios.org/
  - ✓ http://nagiosplugins.org/

Plugins pré-installés dans Ubuntu

/usr/lib/nagios/plugins

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

/etc/nagios-plugins/config

```
apt.cfg      disk-smb.cfg  ftp.cfg       ldap.cfg   mysql.cfg    ntp.cfg     radius.cfg   ssh.cfg
breeze.cfg   dns.cfg       hppjd.cfg     load.cfg   netware.cfg  pgsql.cfg   real.cfg     tcp_udp.cfg
dhcp.cfg     dummy.cfg     http.cfg      mail.cfg   news.cfg     ping.cfg    rpc-nfs.cfg  telnet.cfg
disk.cfg     flexlm.cfg    ifstatus.cfg  mrtg.cfg   nt.cfg       procs.cfg   snmp.cfg     users.cfg
```

Déroulement des contrôles

- Nagios contrôle périodiquement chaque service de chaque machine/équipement. Les réponses possibles sont:
  - OK
  - WARNING (avertissement)
  - CRITICAL (critique)
  - UNKNOWN (inconnu)
- Si un service ne répond pas OK, il passe dans un état « soft » (non-confirmé). Au bout d'un certain nombres de rééssais (par défaut, 3), il passe dans un état « hard » (confirmé). À ce stade une alerte peut être envoyée
- On peut également déclencher un gestionnaire d'événement en synchronisation avec ces évènements.

Déroulement des contrôles (suite)

Paramètres

- Intervalle de contrôle normal
- Intervalle avant nouveau contrôle (si pas OK)
- Nombre maximal de contrôles
- Période de contrôle
- Période de notification

Ordonnancement

- Nagios répartit les contrôles dans l'intervalle de temps, afin de distribuer la charge
- L'interface Web indique le prochain contrôle

La notion de “parents”

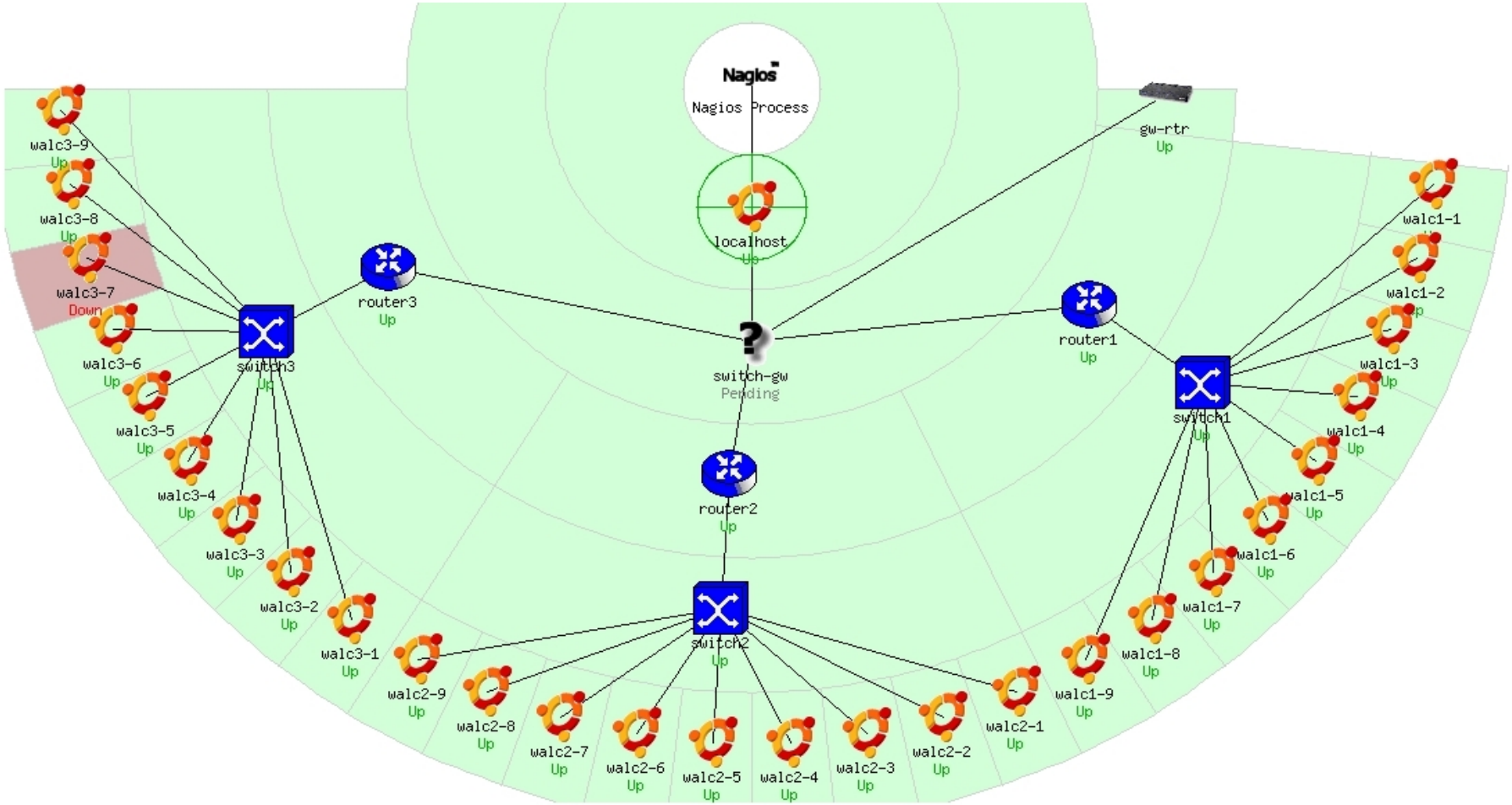
Les nœuds peuvent avoir des parents :

- Ainsi, le parent d’un PC connecté à un commutateur serait le commutateur.
- Ceci nous permet de spécifier les dépendances existant entre des périphériques.
- On évite ainsi que Nagios n’envoie des alarmes lorsqu’un parent ne répond pas.
- Un même nœud peut avoir plusieurs parents (double résidence).

Point de vue du réseau

- Votre point de vue du réseau dépendra de l'emplacement de votre serveur Nagios.
- Le serveur Nagios devient la "racine" de votre arbre de dépendances.

Point de vue du réseau



Démo Nagios

Installation

Sous Debian/Ubuntu

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

Répertoires clés

```
/etc/nagios3
/etc/nagios3/conf.d
/etc/nagios-plugins/conf
/usr/lib/nagios/plugins
/usr/share/nagios3/htdocs/images/logos
```

L'interface web de Nagios se trouve ici :

http://pcX.ws.nsrc.org/nagios3/

Caractéristiques

- Configuration effectuée dans des fichiers texte

  ```
  /etc/nagios3/conf.d/*.cfg
  ```

  - Details at http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html
- La configuration par défaut est divisée en plusieurs fichier avec différents objets dans différents fichier, mais c'est à vous de décider de l'organisation
- Toujours vérifier avant de redémarrer Nagios – sinon votre système de supervision risque de crasher!

  ```
  nagios3 –v /etc/nagios3/nagios.cfg
  ```

Configuration des hôtes et services

Basée sur des modèles (gabarits)

- Grand gain de temps en évitant les répétitions

Il y a des modèles par défaut avec des paramètres par défaut pour:

- *hôte typique/générique* (generic-host_nagios2.cfg)
- *service typique/générique* (generic-service_nagios2.cfg)

- Les réglages individuels peuvent êtres redéfinis (outrepassés)
- Les valeurs par défaut sont raisonnables

Supervision d'un seul hôte

pcs.cfg

```
define host {
    host_name pc1
    alias     pc1 in group 1
    address   pc1.ws.nsrc.org
    use       generic-host
}
```

Importer réglages de ce modèle

- Configuration fonctionnelle minimale
  - Nagios se limite à pinguer l'hôte; Nagios vous préviendra que vous ne surveillez aucun service
- Les fichiers peuvent avoir n'importe quel nom, finissant en **`.cfg`**
- Organisez vos équipements comme vous le voulez – par exemple, hôtes de même type dans un même fichier

Modèle de nœud générique

```
define host{
        name                            generic-host    ; Nom de ce modèle d'hôte
        notifications_enabled           1               ; Notifications de l'hôte  activées
        event_handler_enabled           1               ; Gestionnaire d'événements de l'hôte activé
        flap_detection_enabled          1               ; Détection de l'oscillation activée
        failure_prediction_enabled      1               ; Prévision de défaillance activée
        process_perf_data               1               ; Traite les données de performances
        retain_status_information       1               ; Conserve les informations sur le statut lors des redémarrages de programme
        retain_nonstatus_information    1               ; Conserve les informations non liées au statut lors des redémarrages de
programme
                check_command                   check-host-alive
                max_check_attempts              10
                notification_interval           0
                notification_period             24x7
                notification_options            d,u,r
                contact_groups                  admins
        register                        0       ; N'ENREGISTREZ PAS CETTE DÉFINITION - IL NE S'AGIT PAS D'UN HÔTE RÉEL,
MAIS D'UN MODÈLE !
        }
```

Redéfinition des valeurs par défaut

Tous les réglages peuvent être redéfinis pour chaque hôte

pcs.cfg

```
define host {
    host_name                   pc1
    alias                       pc1 in group 1
    address                     pc1.ws.nsrc.org
    use                         generic-host
    notification_interval       120
    contact_groups              admins,managers
}
```

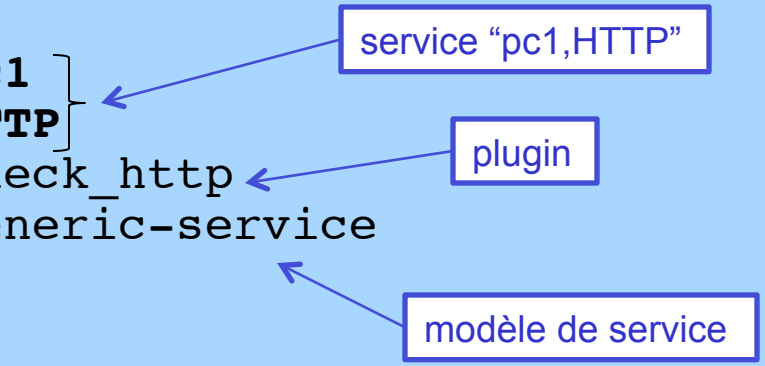
Définition de services (méthode directe)

pcs.cfg

```
define host {
    host_name       pc1
    alias           pc1 in group 1
    address         pc1.ws.nsrc.org
    use             generic-host
}

define service {
    host_name               pc1
    service_description     HTTP
    check_command           check_http
    use                     generic-service
}

define service {
    host_name               pc1
    service_description     SSH
    check_command           check_ssh
    use                     generic-service
}
```



Contrôle des services

- La combination de hôte + service est un identifiant unique pour les de service. Par exemple:
  - “pc1,HTTP”
  - “pc1,SSH”
  - “pc2,HTTP”
  - “pc2,SSH”
- *check_command* indique quel plugin utiliser
- *Le modèle de service* importe les réglages tels que l’intervalle de contrôle, et qui alerter (et quand)

Configuration de services génériques

generic-service_nagios2.cfg*

```
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
        failure_prediction_enabled      1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
          notification_interval           0
          is_volatile                     0
          check_period                    24x7
          normal_check_interval           5
          retry_check_interval            1
          max_check_attempts              4
          notification_period             24x7
          notification_options            w,u,c,r
          contact_groups                  admins
        register                        0    ; DONT REGISTER THIS DEFINITION
        }
```

Redéfinition des valeurs par défaut

Ici aussi, les réglages peuvent être redéfinis au niveau du service

services_nagios2.cfg

```
define service {
    host_name               pc1
    service_description     HTTP
    check_command           check_http
    use                     generic-service
    contact_groups          admins,managers
    max_check_attempts      3
}
```

Contrôle de services pour plusieurs hôtes

- Souvent nous allons effectuer un contrôle de service identique sur une multitude d'hôtes
- Pour éviter la répétition, une méthode plus efficace est de définir un contrôle de service pour tous les hôtes appartenant à un *groupe d'hôtes* ***(hostgroup)***

Création d'un groupe d'hôte

hostgroups_nagios2.cfg

```
define hostgroup {
   hostgroup_name   http-servers
   alias            HTTP servers
   members          pc1,pc2
}

define hostgroup {
   hostgroup_name   ssh-servers
   alias            SSH servers
   members          pc1,pc2
}
```

Contrôle de services dans des groupe d'hôtes (hostgroups)

services_nagios2.cfg

```
define service {
    hostgroup_name          http-servers
    service_description     HTTP
    check_command           check_http
    use                     generic-service
}

define service {
    hostgroup_name          ssh-servers
    service_description     SSH
    check_command           check_ssh
    use                     generic-service
}
```

Explication: si le groupe d'hôte "http-servers" comprend pc1 et pc2, alors Nagios effectuera un contrôle de service HTTP pour chacun d'entre eux. Les contrôles de service sont "pc1,HTTP" et "pc2,HTTP"

Vue alternative

- Au lieu de dire “ce groupe d’hôte comprend ces machines”, on peut exprimer “ce PC appartient aux groupes d’hôtes suivants”
- Pas besoin d’indiquer la ligne “members” dans le fichier de groupe d’hôtes.

Membre d'un groupe (vue alternative)

pcs.cfg

```
define host {
    host_name     pc1
    alias         pc1 in group 1
    address       pc1.ws.nsrc.org
    use           generic-host
    hostgroups    ssh-servers,http-servers
}

define host {
    host_name     pc2
    alias         pc2 in group 1
    address       pc2.ws.nsrc.org
    use           generic-host
    hostgroups    ssh-servers,http-servers
}
```

Les hôtes et les services sont définies au même endroit – pratique!

Autres utilisations des groupes d'hôtes

Choix de pictogrammes pour la cartographie d'états

pcs.cfg

```
define host {
   host_name    pc1
   alias        pc1 in group 1
   address      pc1.ws.nsrc.org
   use          generic-host
   hostgroups   ssh-servers,http-servers,debian-servers
}
```

extinfo_nagios2.cfg

```
define hostextinfo {
   hostgroup_name    debian-servers
   notes             Serveurs Debian GNU/Linux
   icon_image        base/debian.png
   statusmap_image   base/debian.gd2
}
```

Facultatif: servicegroups (groupes de services)

- On peut également regrouper ensemble des services en “groupes de service”
- Ceci sert à lier ensemble des services associés ou interdépendents, visibles ensemble dans l’interface web
- Les définitions de ces services doivent déjà avoir été définies.

servicegroups.cfg

```
define servicegroup {
   servicegroup_name   mail-services
   alias         Services de la plateforme de mail
   members       web1,HTTP,web2,HTTP,mail1,IMAP,db1,MYSQL
}
```

Définition de la topologie

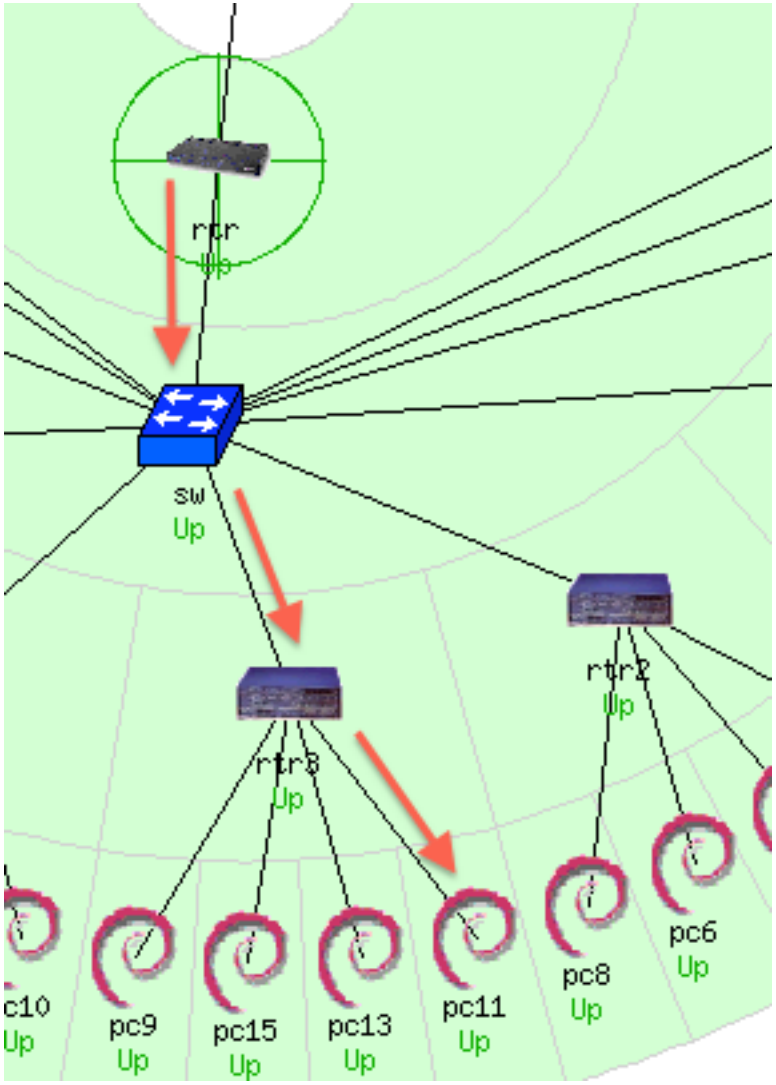
pcs.cfg

```
define host {
    host_name    pc1
    alias        pc1 in group 1
    address      pc1.ws.nsrc.org
    use          generic-host
    parents      rtr1
}
```

hôte parent

- Ceci veut dire “pc1 est de l’autre côté de rtr1”
- Si rtr1 est en panne, pc1 est marqué comme étant “unreachable” (injoignable) et non “down”
- Evite une avalanche d’alertes en cas de panne de rtr1
- Permet à Nagios d’afficher une superbe cartographie du réseau

Une autre vue de la configuration



RTR

```
define host {
    use             generic-host
    host_name       rtr
    alias           Routeur passerelle
    address         10.10.0.254     }
```

SW

```
define host {
    use             generic-host
    host_name       sw
    alias           Commutateur
    address         10.10.0.253
    parents         rtr     }
```

RTR3

```
define host {
    use             generic-host
    host_name       rtr3
    alias           router 3
    address         10.10.3.254
    parents         sw      }
```

PC11…

Notifications hors bande (OoB)

Un élément essentiel à retenir : un dispositif de SMS ou de messages indépendant du réseau.

- Utiliser un téléphone cellulaire, ou un modem USB avec carte SIM, raccordé au serveur Nagios
- On peut utiliser des outils tels que:

gammu: http://wammu.eu/
gnokii: http://www.gnokii.org/
sms-tools: http://smstools3.kekekasvi.com/

Références

- **Site Web de Nagios**
  http://www.nagios.org/
- **Site de plugins Nagios**
  http://www.nagios.org/
- *Nagios System and Network Monitoring*, de Wolfgang Barth. Un bon ouvrage sur Nagios.
- **Site de plugins Nagios non officiel**
  http://nagios.exchange.org/
- **Tutoriel Debian sur Nagios**
  http://www.debianhelp.co.uk/nagios.htm
- **Support commercial pour Nagios**
  http://www.nagios.com/

Questions?

?

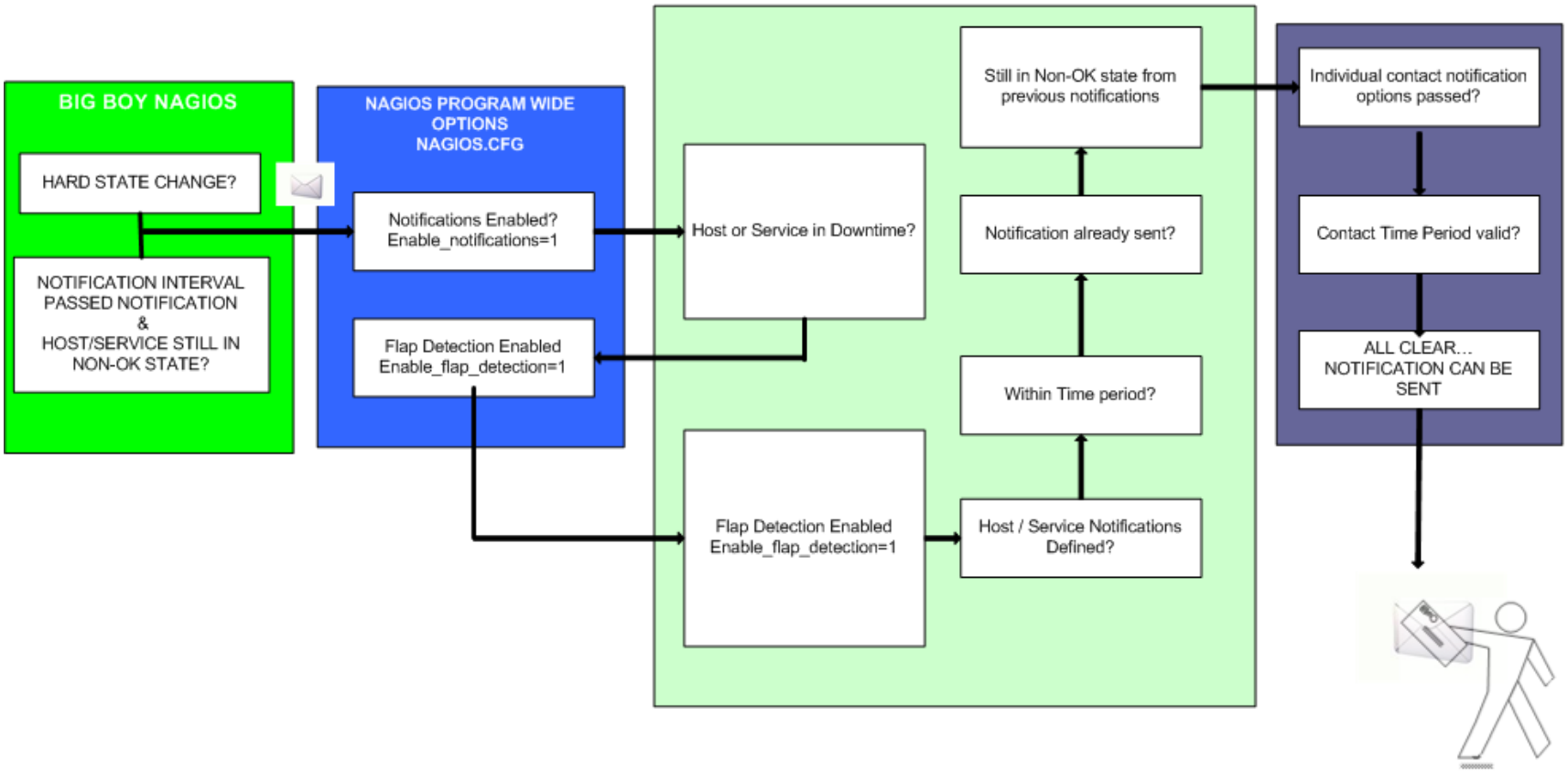
Informations complémentaires

Quelques diapositives supplémentaires que vous pourriez trouver utiles ou intéressantes...

Des fonctions, encore des fonctions…

- Permet de prendre acte d'un événement
  - L'utilisateur peut ajouter des commentaires via 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.
- Permet de définir des niveaux de notification pour l'escalade.

ORDINOGRAMME DES NOTIFICATIONS NAGIOS



NOTE: The flow will only continue when each of the listed filters are satisfied.

CONTACT GETS THE NOTIFICATION MESSAGE

Options de notification (hôte)

État de l'hôte :

Lorsque vous configurez un hôte, vous disposez des options de notification suivantes :

- **d:** DOWN (l'hôte est arrêté)
- **u:** UNREACHABLE (l'hôte est inaccessible)
- **r:** RECOVERY (l'hôte se rétablit)
- **f:** FLAPPING (l'hôte oscille)
- **n:** NONE (aucune notification)

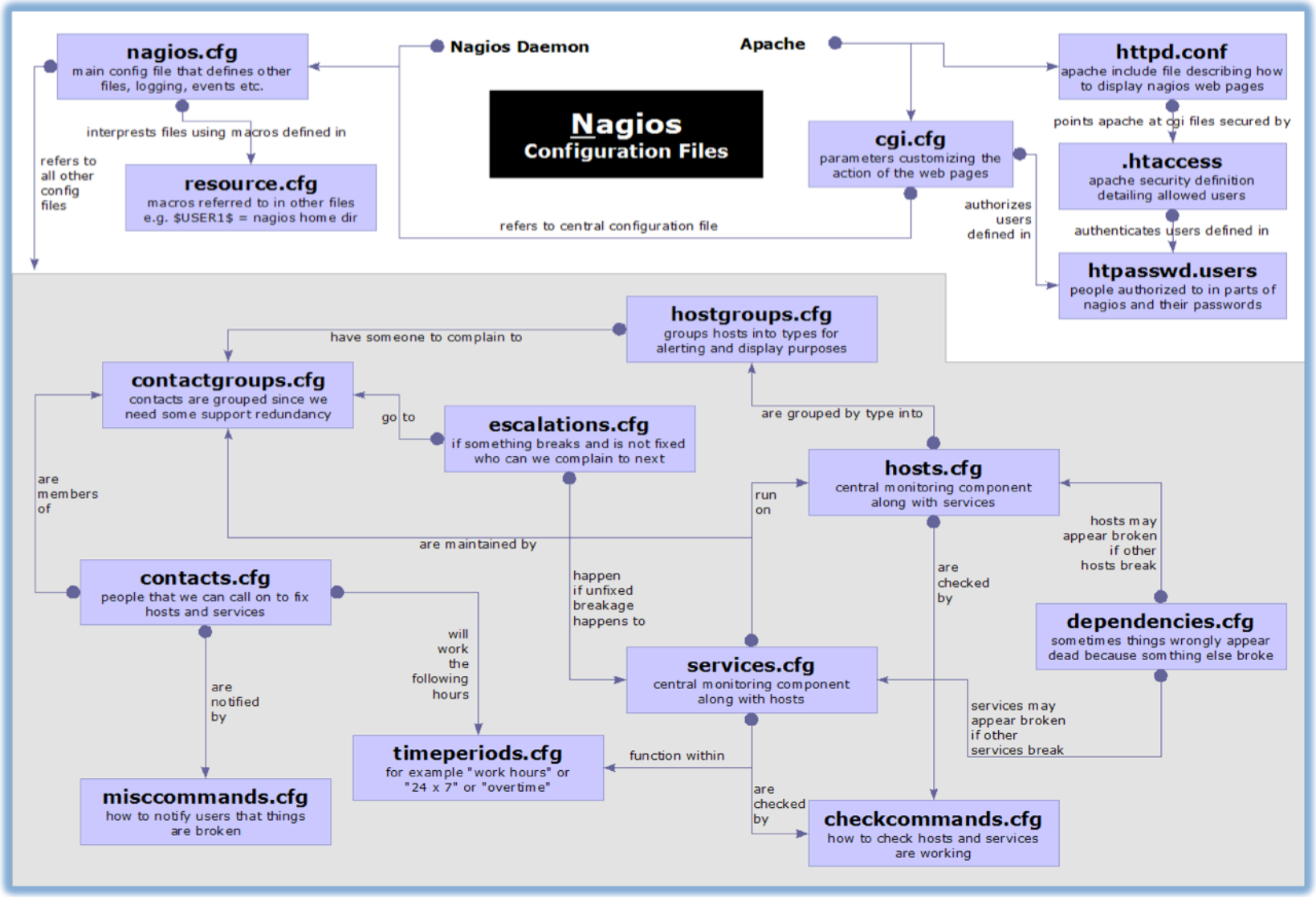
Options de notification (Service)

État de service:

Quand on définit un contrôle de services, on peut être prévenu des conditions suivantes:

- **w:** WARNING (ATTENTION)
- **c:** CRITICAL (CRITIQUE)
- **u:** UNKNOWN (état inconnu)
- **r:** RECOVERY (REPRISE)
- **f:** FLAPPING (start/end) – (oscillation)
- **s:** SCHEDULED DOWNTIME (start/end) MAINTENANCE PLANIFIÉE
- **n:** NONE aucun évènement

Fichiers de configuration (Officiels)



Disposition des fichiers de configuration (Debian/Ubuntu)

Situés dans /etc/nagios3/

Les fichiers importants incluent :

- cgi.cfg — Contrôle l'interface web et les 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/*

contacts_nagios2.cfg	utilisateurs et groupes
extinfo_nagios2.cfg	embellit votre interface utilisateur
generic-host_nagios2.cfg	modèle d'hôte par défaut
generic-service_nagios2.cfg	modèle de service par défaut
host-gateway_nagios3.cfg	définition par déf. hôte-passerelle
hostgroups_nagios2.cfg	groupes de nœuds
localhost_nagios2.cfg	définition de l'hôte nagios
services_nagios2.cfg	Services à contrôler
timeperiods_nagios2.cfg	Quand contrôler et à qui adresser les notifications

Fichiers de configuration (suite)

Autres fichiers de configuration dans conf.d :

- servicegroups.cfg — Groupes de nœuds et de services
- pcs.cfg — Exemple de définitions de PC (hôtes)
- switches.cfg — Définitions de commutateurs (hôtes)
- routers.cfg — Définitions de routeurs (hôtes)

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
- Authentification 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 contrôles, les notifications, etc.

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

/etc/nagios-plugins/config/ssh.cfg

```
define command {
  command_name  check_ssh
  command_line  /usr/lib/nagios/plugins/check_ssh '$HOSTADDRESS$'
}

define command {
  command_name  check_ssh_port
  command_line  /usr/lib/nagios/plugins/check_ssh -p '$ARG1$' '$HOSTADDRESS$'
}
```

- Notez que le même plugin peut être invoqué de plusieurs façons (“command”)
- Les commandes et les paramètres sont séparées par des points d’exclamation (!)
- Par exemple, pour contrôler SSH sur un port non standard:

```
define service {
   hostgroup_name          ssh-servers-2222
   service_description     SSH-2222
   check_command           check_ssh_port!2222
   use                     generic-service
}
```

Ici $ARG1$

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: router_group@localdomain
Subject: Host DOWN alert for TLD1-RTR!
Date: Thu, 29 Jun 2006 15:13:30 -0700

Host: gw-rtr
In: Core_Routers
State: DOWN
Address: 192.0.2.100
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds

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 ; spécifiez une valeur > 0 si vous voulez être renotifié
}
```

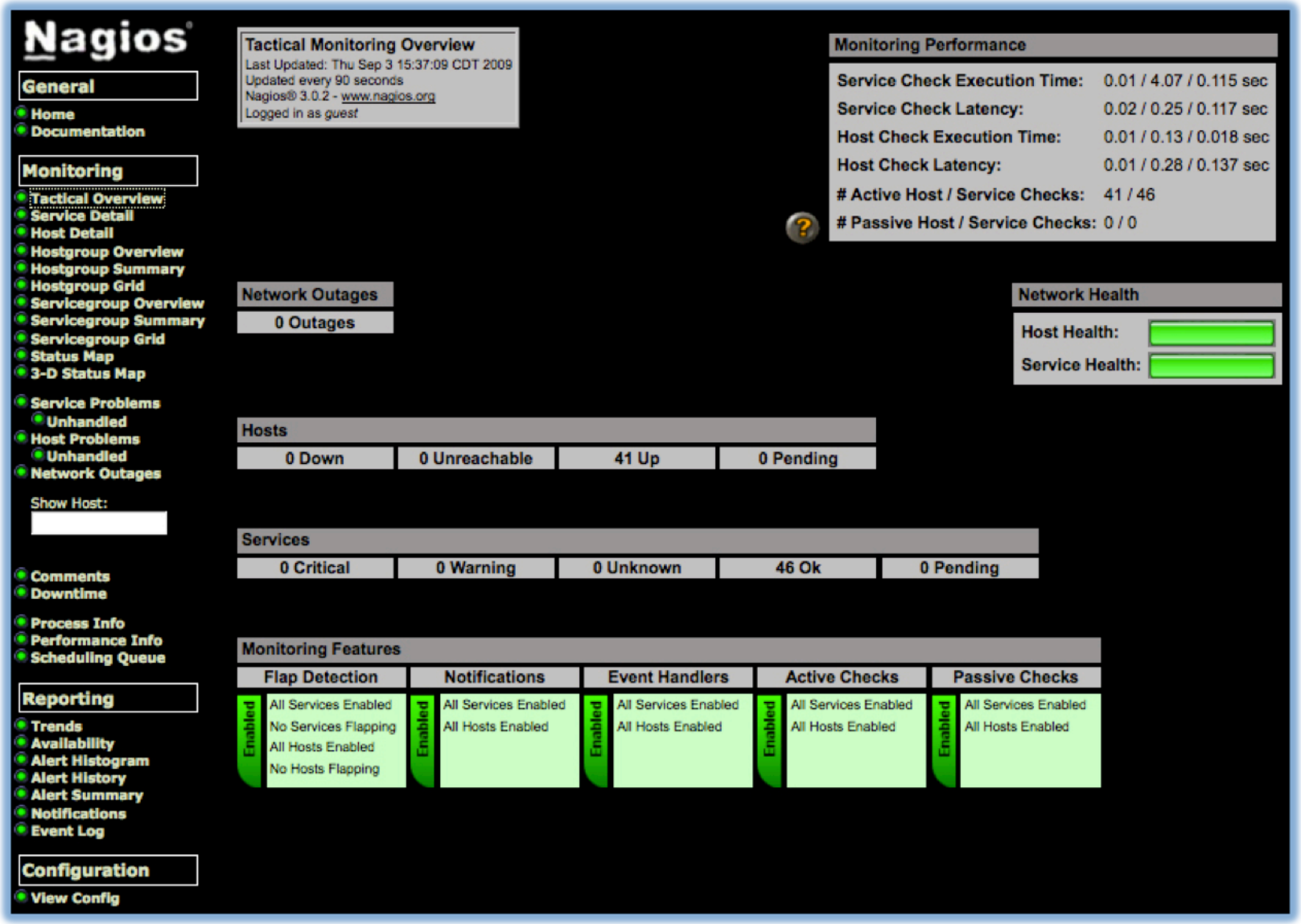
La description de service (« service_description ») est importante si vous comptez créer des groupes de services. Voici un exemple de définition de groupe de services :

```
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
}
```

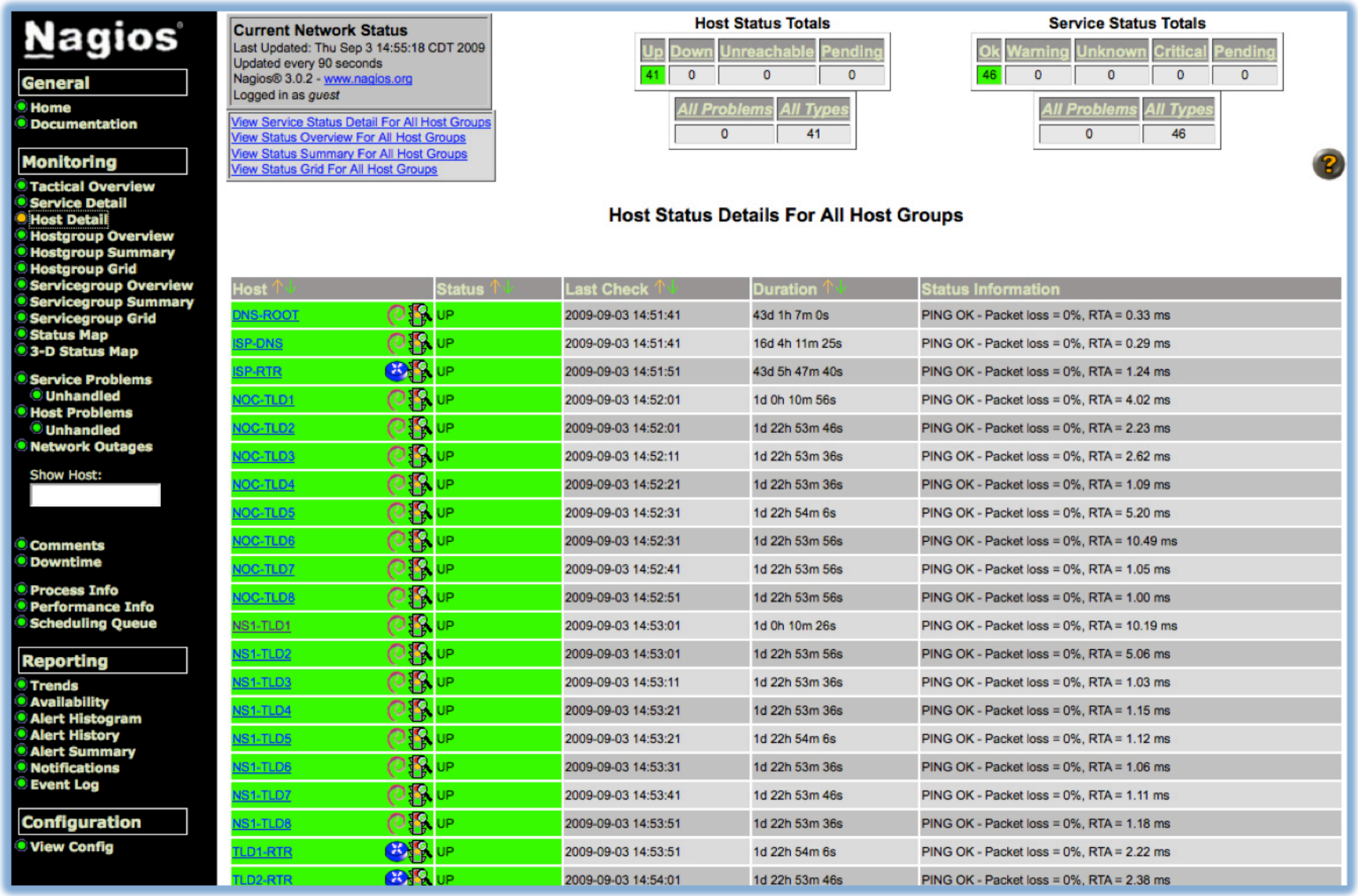
Captures d’écran

Quelques exemples de captures d'écran provenant d'une installation Nagios.

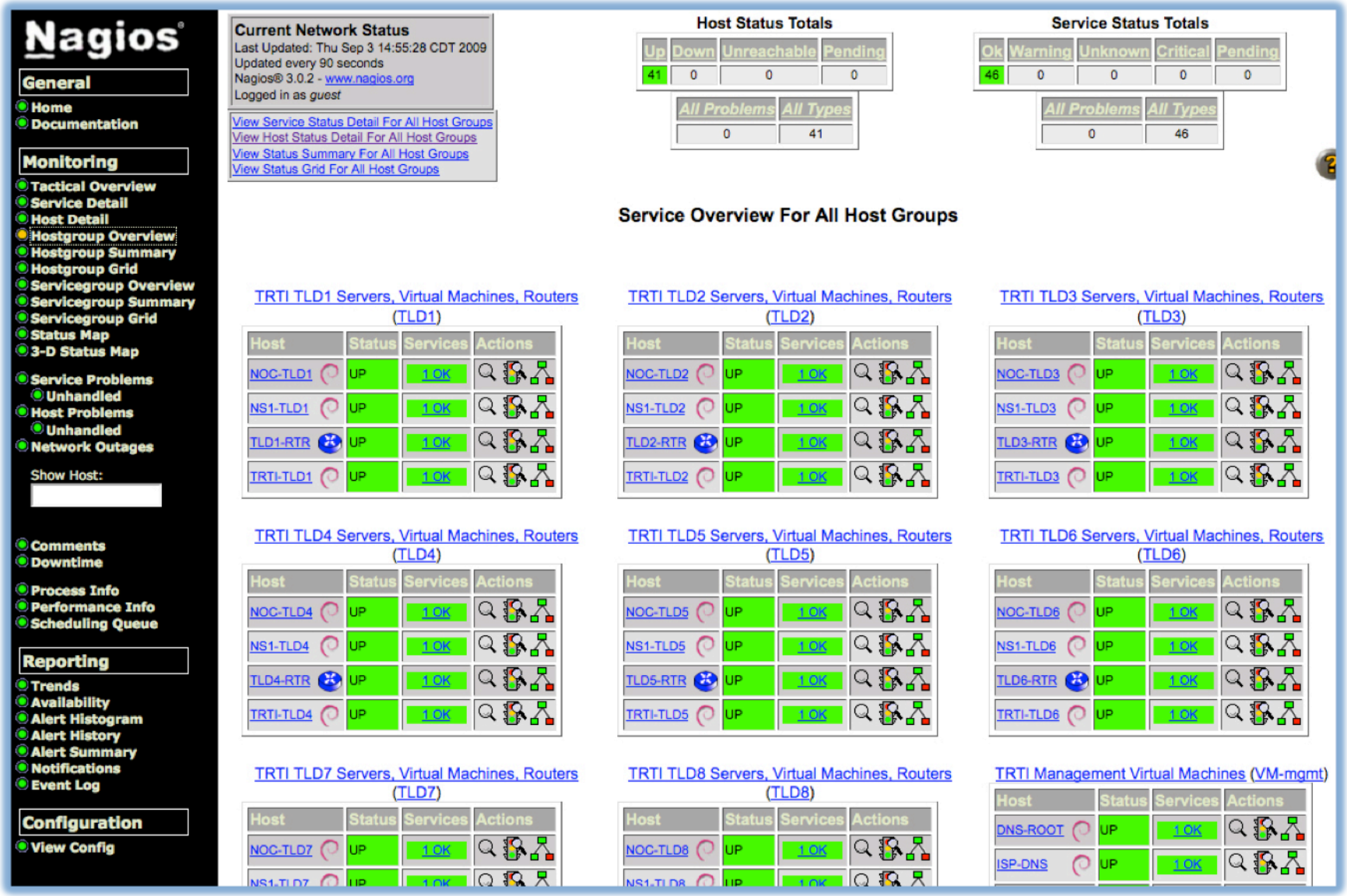
Présentation générale



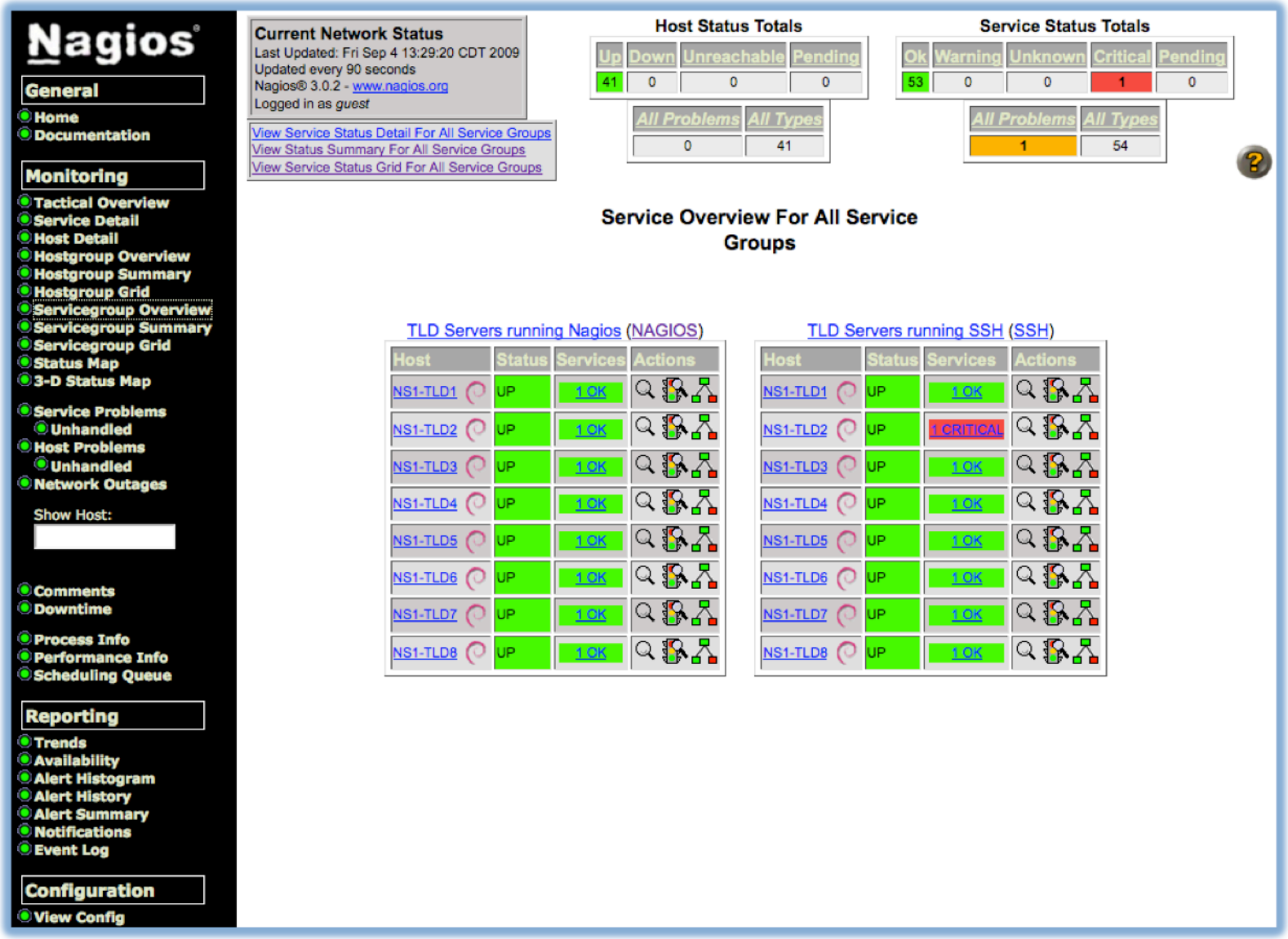
Détail des hôtes



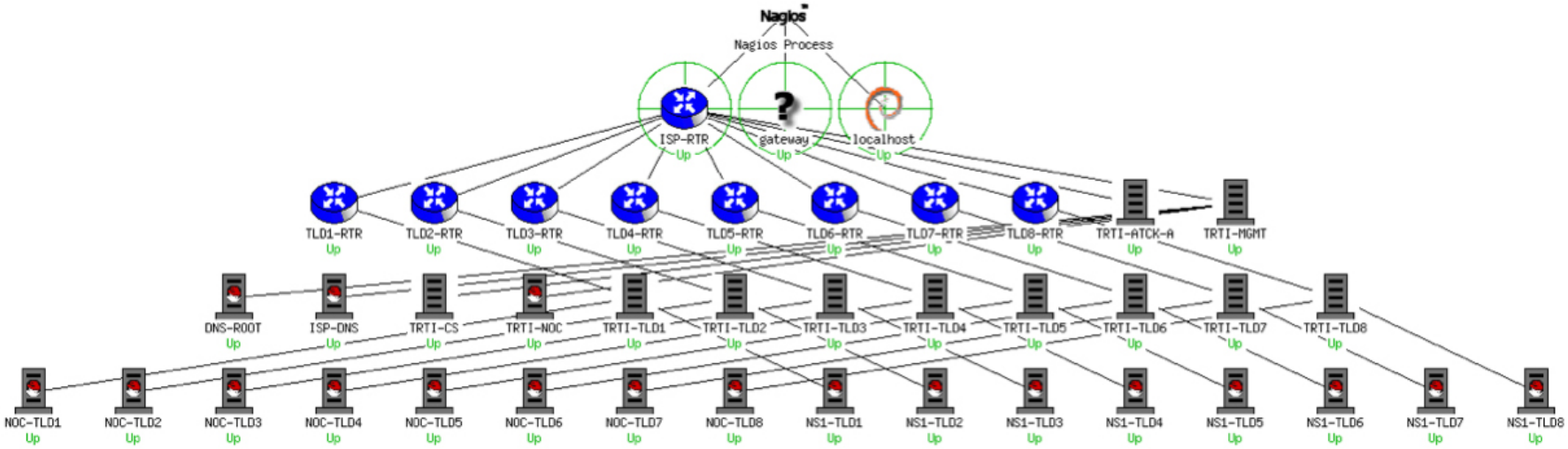
Vue d’ensemble des groupes d’hôtes



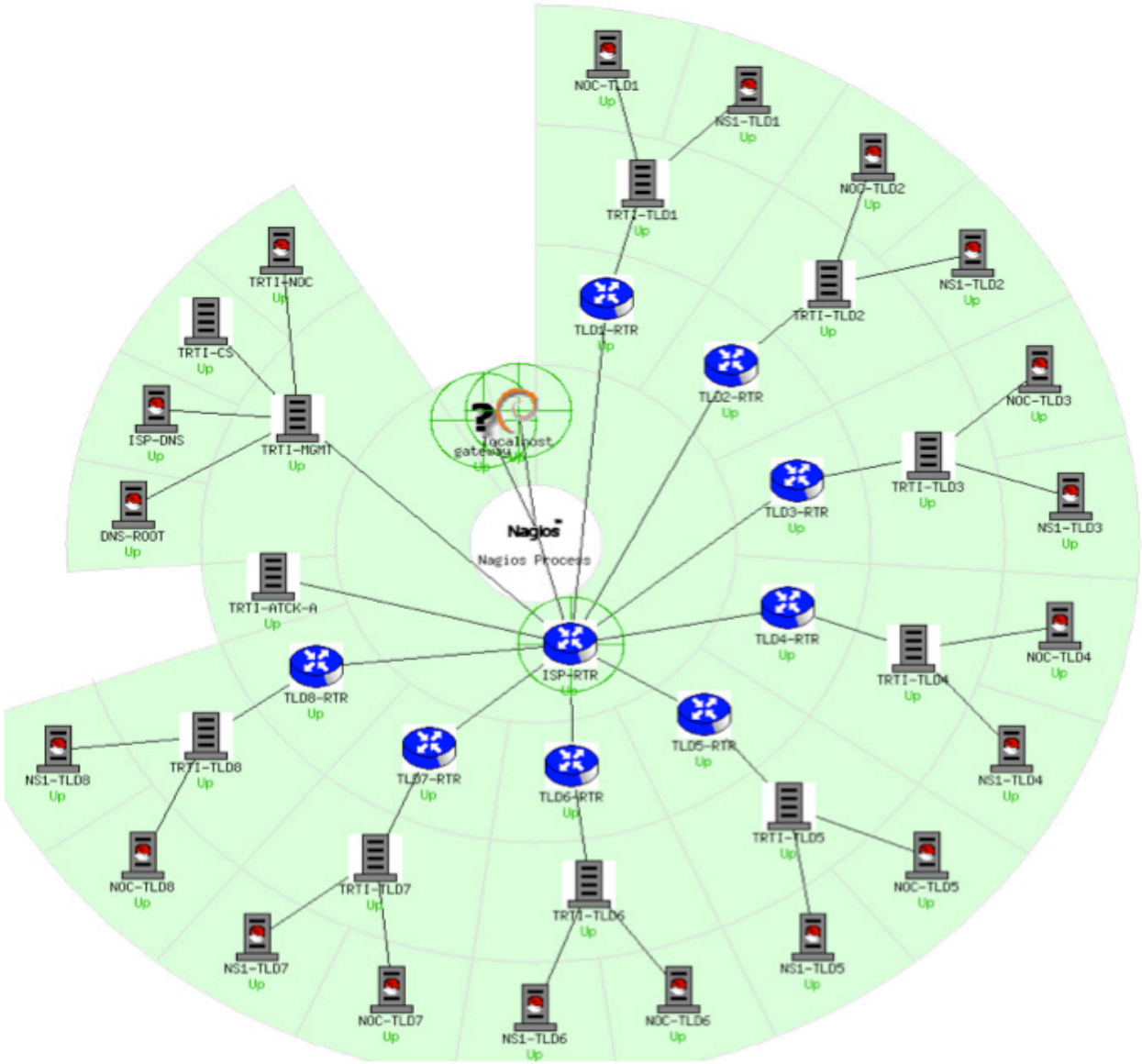
Vue d’ensemble des groupes de services



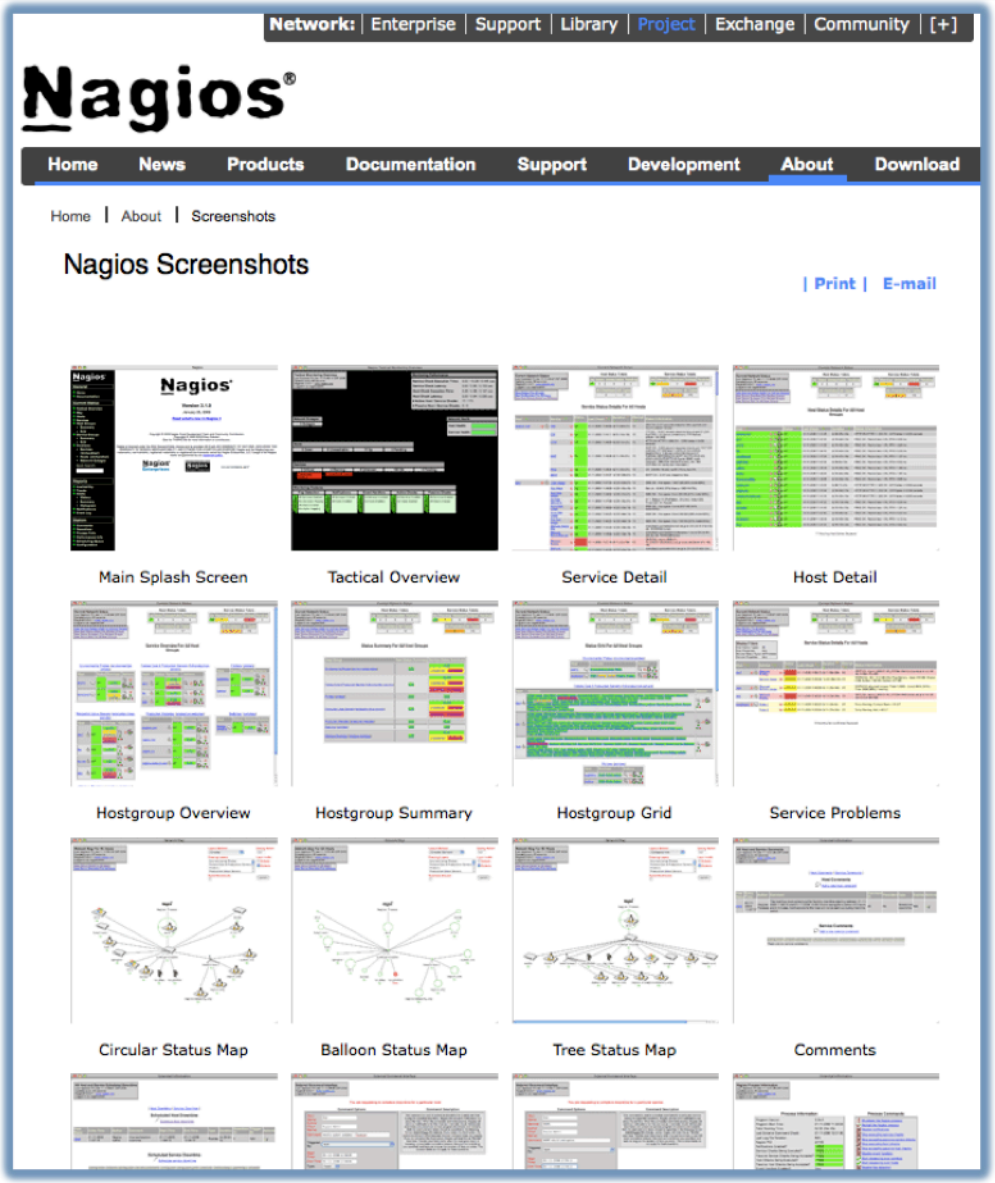
Représentation arborescente du statut des hôtes



Représentation circulaire du statut des hôtes



Autres captures d'écran



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

http://www.nagios.org/about/screenshots