

SUPERVISION DE RÉSEAU AVEC NAGIOS

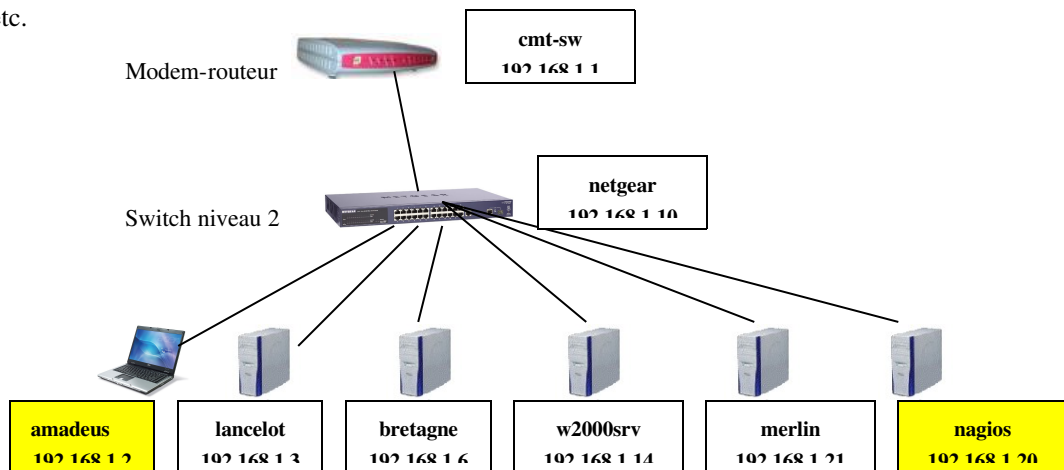
Auteur : Henri TSOUNGUI, © H.T. Lille, dec. 2006

Utilitaires : nagios 1.4 pour le premier superviseur,
nagios 1.1 et nagat 1.02 pour le 2^{ème} superviseur

1. Contexte et objectifs

Nous travaillons dans un réseau comportant 6 hôtes dont un portable, un switch adressable et un modem-routeur ADSL.

L'objectif est de surveiller la continuité de l'activité des ordinateurs et certains services comme http, mysql, postgresql, etc.



2. Fichiers de configuration pour l'accès par interface web

-Fichier **.htaccess** à placer dans /usr/local/nagios/

```
AuthName " Controle Acces Nagios "  
AuthType Basic  
AuthUserFile /usr/local/nagios/etc/htpasswd.users  
require valid-user
```

-Fichier /usr/local/nagios/etc/**htpasswd.users** à créer avec la commande Apache

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagios
```

-Fichier **nagios.conf** à inclure dans /etc/httpd/conf/httpd.conf ou ajouter à la fin :

```
#Section pour securisation Nagios  
  
ScriptAlias /nagios/cgi-bin/ "/usr/local/nagios/sbin/"  
  
<Directory "/usr/local/nagios/sbin/">  
AllowOverride All  
order allow,deny  
allow from all  
Options ExecCGI  
</Directory>
```

```
Alias /nagios/ /usr/local/nagios/share/
<Directory "/usr/local/nagios/share/">
AllowOverride All
order allow,deny
allow from all
</Directory>
```

*Faire attention de placer ScriptAlias avant Alias.

3. Configuration du premier serveur de supervision

Paramètres TCP-IP :

```
Nom : amadeus.linux.tme
IP : 192.168.1.2/255.255.255.0
```

Config dans le fichier **/usr/local/nagios/etc/hosts.cfg** :

```
# 'amadeus' host definition
define host{
    use                generic-host          ; nom de l'hôte générique
    host_name          amadeus
    alias              Linux Server #1
    address            192.168.1.2
    check_command      check-host-alive
    max_check_attempts 10
    notification_interval 480
    notification_period 24x7
    notification_options d,u,r
    parents            netgear-sw
}
```

Dans le fichier des groupes d'hôtes **/usr/local/nagios/etc/hostgroups.cfg** , amadeus fait partie du groupe des serveurs linux :

```
# 'linux-boxes' host group definition
define hostgroup{
    hostgroup_name linux-boxes
    alias          Linux Servers
    contact_groups linux-admins
    members        lancelet,amadeus
}
```

En cas de problème un message est envoyé au contact linux-admins défini dans les fichiers des contacts **/usr/local/nagios/etc/contacts.cfg** :

```
# 'nagios' contact definition
define contact{
    contact_name          nagios
    alias                Nagios Admin
    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,notify-by-epager
host_notification_commands       host-notify-by-email,host-notify-by-epager
email                            nagios-admin@localhost.localdomain
pager                            pagenagios-admin@localhost.localdomain
}

```

Signification des options de notification w =>warning u=>unknown c=>critical r=>recovering d =>down

Définition de groupe de contacts **/usr/local/nagios/etc/contacts.cfg** :

```

# 'linux-admins' contact group definition
define contactgroup{
    contactgroup_name    linux-admins
    alias                Linux Administrators
    members              nagios,root
}

```

Il faut ensuite configurer au moins un service à surveiller dans **/usr/local/nagios/etc/services.cfg** . Le service à configurer, comme les autres, peut hériter de la définition du service générique qui ne constitue qu'un modèle, un « template ».

```

# Generic service definition template
define service{
    name                generic-service ; The 'name' of this service template,
referenced in other service definitions
    active_checks_enabled    1 ; Active service checks are enabled
    passive_checks_enabled    1 ; Passive service checks are enabled/accepted
    parallelize_check         1 ; Active service checks should be parallelized
    obsess_over_service        1 ; We should obsess over this service (if necessary)
    check_freshness            0 ; Default is to NOT check service 'freshness'
    notifications_enabled      1 ; Service notifications are enabled
    event_handler_enabled      1 ; Service 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
    register                 0 ; on n'enregistre pas le service générique
}

```

Voici comment tester la machine amadeus avec un **ping** régulier :

```

# Service definition
define service{
    use                generic-service ; récup définition du service générique
    host_name          amadeus
    service_description    PING
    is_volatile         0
    check_period        24x7
    max_check_attempts    3
    normal_check_interval    5
    retry_check_interval    1
    contact_groups       linux-admins
    notification_interval    240
}

```

```
notification_period      24x7
notification_options     c,r
check_command            check_ping!100.0,20%!500.0,60%
}
```

Autre test : fonctionnement du service mysql de la machine bretagne sur le port TCP par défaut 3306 :

```
# Service definition
define service{
    use                generic-service ; Name of service template to use
    host_name          bretagne
    service_description TCP
    is_volatile        0
    check_period       24x7
    max_check_attempts 3
    normal_check_interval 2
    retry_check_interval 1
    contact_groups     nt-admins
    notification_interval 240
    notification_period 24x7
    notification_options w,u,c,r
    check_command      check_tcp!3306
}
```

4. Test de la configuration de nagios (concerne le fichier principal nagios.cfg).

On se place dans `.. /nagios/bin` puis on tape la commande : `./nagios -v /usr/local/nagios/etc/nagios.cfg`

```
[root@amadeus bin]# ./nagios -v /usr/local/nagios/etc/nagios.cfg
```

```
Nagios 1.4.1
Copyright (c) 1999-2006 Ethan Galstad (nagios@nagios.org)
Last Modified: 05-15-2006
License: GPL
```

```
Reading configuration data...
```

```
Running pre-flight check on configuration data...
```

```
Checking services...
  Checked 17 services.
Checking hosts...
  Checked 7 hosts.
Checking host groups...
  Checked 4 host groups.
Checking contacts...
  Checked 2 contacts.
Checking contact groups...
  Checked 4 contact groups.
Checking service escalations...
  Checked 0 service escalations.
Checking host group escalations...
  Checked 0 host group escalations.
Checking service dependencies...
  Checked 0 service dependencies.
Checking host escalations...
```

```
Checked 0 host escalations.
Checking host dependencies...
Checked 0 host dependencies.
Checking commands...
Checked 22 commands.
Checking time periods...
Checked 4 time periods.
Checking for circular paths between hosts...
Checking for circular service execution dependencies...
Checking global event handlers...
Checking obsessive compulsive service processor command...
Checking misc settings...
```

```
Total Warnings: 0
Total Errors: 0
```

```
Things look okay - No serious problems were detected during the pre-flight check
[root@amadeus bin]# service nagios restart
Running configuration check...done
Stopping network monitor: nagios
Starting network monitor: nagios
  PID TTY          TIME CMD
20319 ?        00:00:00 nagios
```

La configuration est réputée correcte, on n'a plus qu'à redémarrer le service nagios.

```
#service nagios restart
```

**** NE JAMAIS REDEMARRER nagios SI DES ERREURS PERSISTENT.**

Ensuite, avec un navigateur, on se connecte au serveur de supervision amadeus :

```
http://192.168.1.2/nagios/
```

-En cliquant sur le panneau sur fond noir à gauche sur le lien **Service Detail**, on obtient l'écran suivant. On peut noter que le serveur w2000srv (192.168.1.14), comme par hasard, un serveur windows ne répond pas ; il est down !

Current Network Status
 Last Updated: Mon Dec 18 23:14:32 CET 2006
 Updated every 90 seconds
 Nagios® - www.nagios.org
 Logged in as nagios

Host Status Totals

Up	Down	Unreachable	Pending
6	1	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
12	0	0	5	0

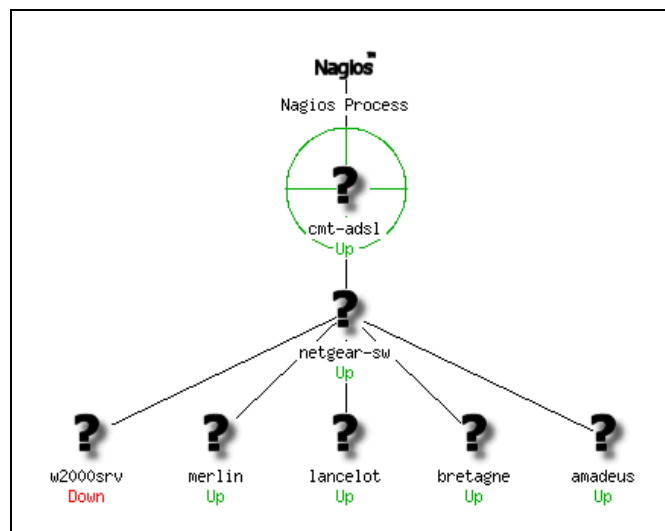
Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
amadeus	PING	OK	18-12-2006 23:12:02	0d 8h 30m 41s	1/3	PING OK - Paquets perdus = 0%, RTA = 0.05 ms
bretagne	HTTP	OK	18-12-2006 23:13:34	0d 8h 35m 49s	1/3	HTTP OK HTTP/1.1 200 OK - 5117 bytes in 0.032 seconds
	PING	OK	18-12-2006 23:07:42	0d 8h 27m 55s	1/3	PING OK - Paquets perdus = 0%, RTA = 0.24 ms
	TCP-MYSQL	OK	18-12-2006 23:14:17	0d 0h 2m 15s	1/3	TCP OK - 0,000 second response time on port 3306
cmt-ads1	PING	OK	18-12-2006 23:13:49	0d 9h 3m 7s	1/3	PING OK - Paquets perdus = 0%, RTA = 0.84 ms
lancetot	/devhda1 Free Space	OK	18-12-2006 23:07:58	0d 9h 1m 17s	1/3	DISK OK - free space: / 6012 MB (44% inode=93%):
	/devhdb2 Free Space	CRITICAL	18-12-2006 23:12:33	0d 11h 34m 48s	3/3	DISK CRITIQUE - /devhdb2 n'existe pas
	Current Users	OK	18-12-2006 23:14:05	0d 9h 2m 47s	1/3	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	OK	18-12-2006 23:11:14	0d 8h 28m 41s	1/3	HTTP OK HTTP/1.1 200 OK - 478 bytes in 0.003 seconds
	PING	OK	18-12-2006 23:12:48	0d 8h 27m 11s	1/3	PING OK - Paquets perdus = 0%, RTA = 0.21 ms
merlin	PING	OK	18-12-2006 23:08:28	0d 3h 41m 4e	1/3	PING OK - Paquets perdus = 0%, RTA = 0.50 ms
netgear-sw	PING	OK	18-12-2006 23:13:03	0d 0h 7m 39s	1/3	PING OK - Paquets perdus = 0%, RTA = 11.97 ms
w2000srv	FTP	CRITICAL	18-12-2006 23:07:11	0d 4h 57m 25s	3/3	Aucun chemin d'accès pour atteindre l'hôte cible
	HTTP	CRITICAL	18-12-2006 23:08:44	0d 4h 55m 46s	3/3	No route to host
	PING	CRITICAL	18-12-2006 23:13:19	0d 4h 59m 15s	1/3	CRITIQUE - Hôte injoignable (192.168.1.14)
	SMTP	CRITICAL	18-12-2006 23:11:27	0d 11h 33m 38s	3/3	Aucun chemin d'accès pour atteindre l'hôte cible

17 Matching Service Entries Displayed

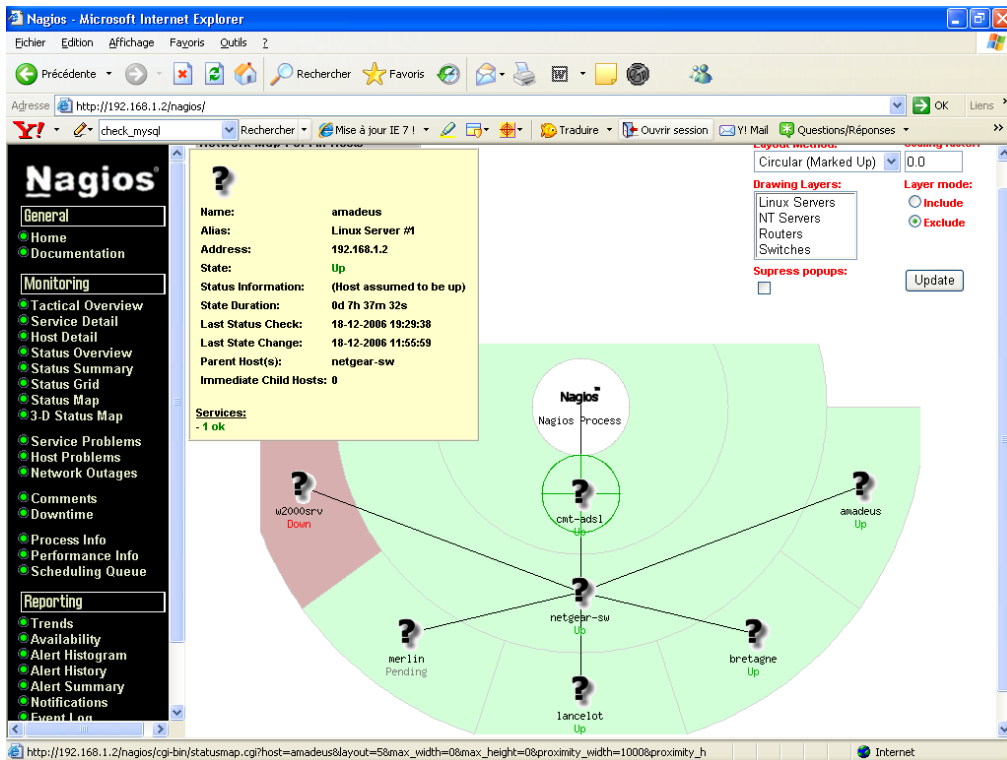
5.Arborescence

Les machines à superviser dépendent toutes du switch netgear qui lui-même dépend du routeur adsl comtrend et du processus nagios selon l'arborescence ci-après :

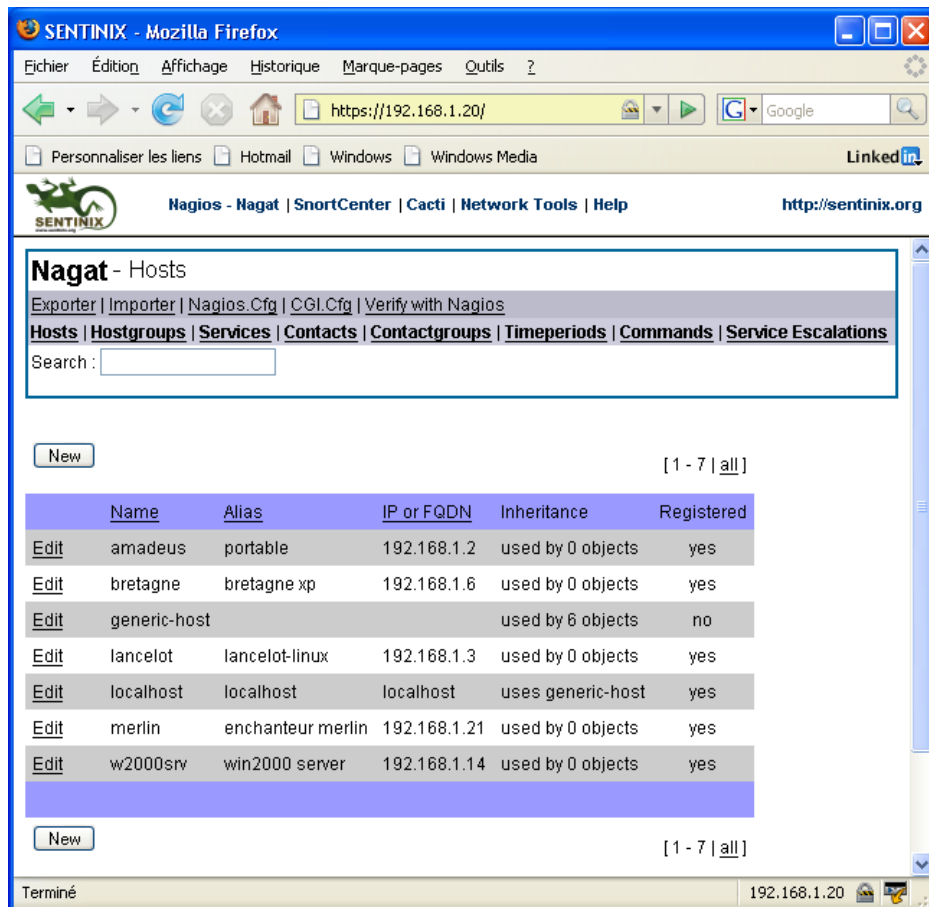


Ecran de l'ordinateur **amadeus.linux.tme(192.168.1.2)** où NAGIOS a été configuré « à la main » par modification de ses fichiers

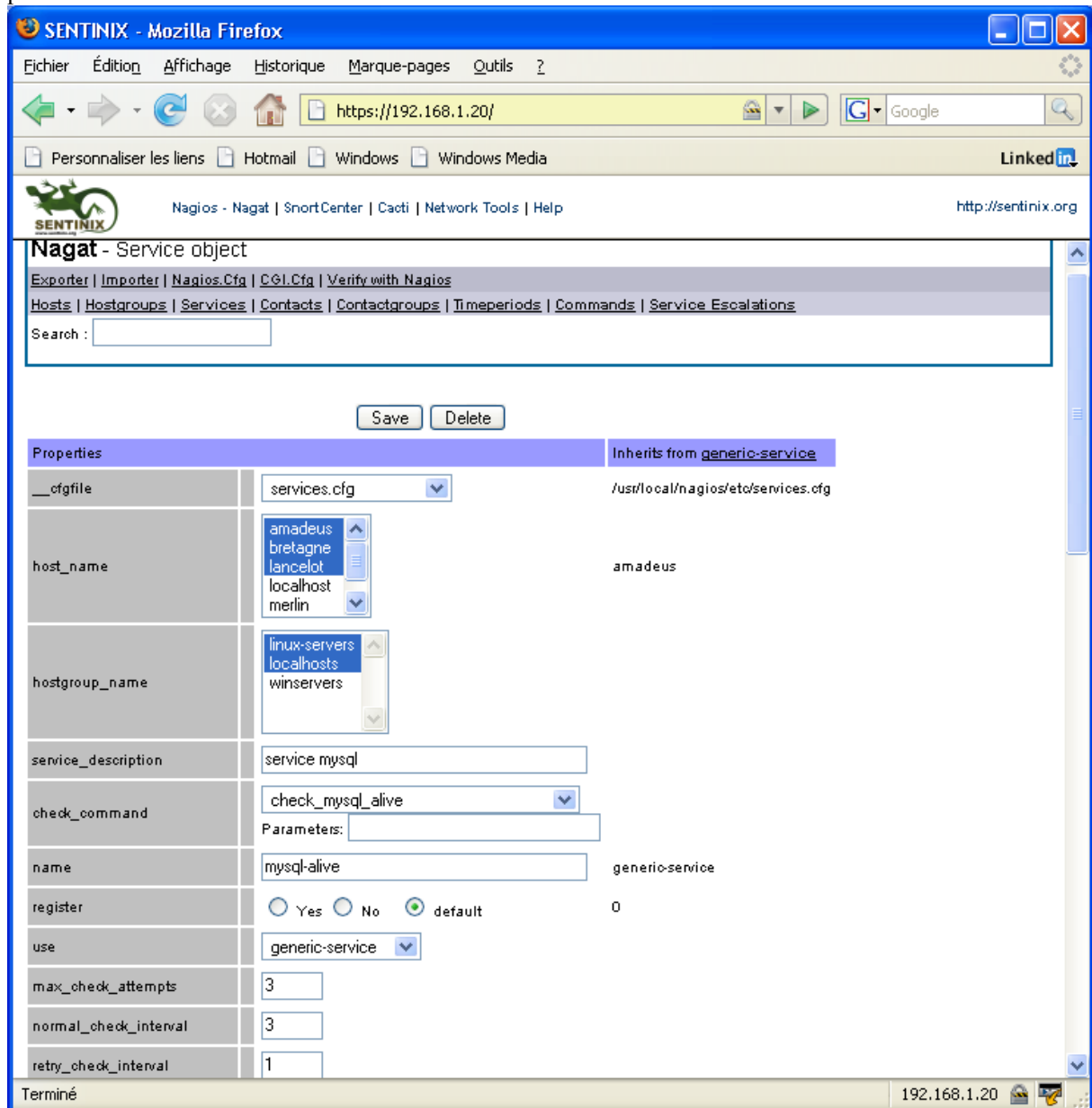
Résultat graphique :



Sur nagios.linux.tme (192.168.1.20) la supervision est configurée par NAGAT. Elle est nettement plus aisée, les résultats identiques et nous ne la détaillerons pas dans ce document.



Il suffit de configurer tour à tour les hôtes, les services, les contacts, etc, comme je l'ai fait à la main en manipulant les fichiers. Toutefois, il est vivement déconseillé de retoucher les fichiers modifiés par nagat sous peine de rencontrer de nombreuses difficultés.



The screenshot shows the Nagat web interface for configuring a service object. The browser window is titled "SENTINIX - Mozilla Firefox" and the address bar shows "https://192.168.1.20/". The page content includes a search bar, "Save" and "Delete" buttons, and a "Properties" section with the following fields:

Property	Value	Inherits from
__cfgfile	services.cfg	generic-service
host_name	amadeus	amadeus
hostgroup_name	linux-servers	
service_description	service mysql	
check_command	check_mysql_alive	
name	mysql-alive	generic-service
register	default	0
use	generic-service	
max_check_attempts	3	
normal_check_interval	3	
retry_check_interval	1	

Configuration de la surveillance du service mysql avec le plugin **check_mysql_alive** avec nagat.

Configuration des groupes d'hôtes en mode graphique

SENTINIX - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

https://192.168.1.20/

Personnaliser les liens Hotmail Windows Windows Media [LinkedIn](#)

SENTINIX Nagios - Nagat | SnortCenter | Cacti | Network Tools | Help <http://sentinix.org>

Nagat - Hostgroup object

[Exporter](#) | [Importer](#) | [Nagios.Cfg](#) | [CGI.Cfg](#) | [Verify with Nagios](#)

[Hosts](#) | [Hostgroups](#) | [Services](#) | [Contacts](#) | [Contactgroups](#) | [Timeperiods](#) | [Commands](#) | [Service Escalations](#)

Search :

Properties

__cfgfile	hostgroups.cfg
hostgroup_name	linux-servers
alias	linux servers
name	linux-servers
register	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> default
use	
contact_groups	admins
members	amadeus bretagne lancelot localhost merlin

The following 2 object(s) are using this object:

- 'service'-object: [template mysql-alive](#)
- 'service'-object: [template postgresql](#)

Terminé 192.168.1.20

Le résultat est tout aussi bien.

Current Network Status
 Last Updated: Mon Dec 18 23:36:37 CET 2006
 Updated every 90 seconds
 Nagios® - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
4	2	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
10	0	2	3	0

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
amadeus	opu	OK	2006-12-18 23:35:36	0d 1h 57m 56s	1/3	OK - load average: 0.05, 0.12, 0.17
	service_mysql	OK	2006-12-18 23:35:24	1d 6h 24m 36s	1/3	TCP OK - 0.001 second response time on port 3306
	service_postgresql	UNKNOWN	2006-12-18 23:33:25	1d 10h 22m 37s	3/3	Server port must be a positive integer
bretagne	check_alive	OK	2006-12-18 23:34:39	0d 7h 1m 1s	1/3	PING OK - Packet loss = 0%, RTA = 0.20 ms
	host_alive	OK	2006-12-18 23:35:36	0d 5h 25m 2s	1/4	PING OK - Packet loss = 0%, RTA = 5.40 ms
	service_mysql	OK	2006-12-18 23:34:38	0d 4h 10m 55s	1/3	TCP OK - 0.001 second response time on port 3306
lhost0j	service_mysql	OK	2006-12-18 23:34:48	0d 7h 33m 59s	1/3	TCP OK - 0.001 second response time on port 3306
	service_postgresql	UNKNOWN	2006-12-18 23:35:47	1d 10h 26m 17s	1/3	Server port must be a positive integer
localhost	opu	OK	2006-12-18 23:35:36	0d 1h 57m 56s	1/3	OK - load average: 0.05, 0.12, 0.17
	service_mysql	OK	2006-12-18 23:34:59	0d 6h 58m 33s	1/3	TCP OK - 0.002 second response time on port 3306
	service_pop3	CRITICAL	2006-12-18 23:36:02	1d 8h 14m 31s	3/3	Connection refused by host
merlin	check_alive	OK	2006-12-18 23:34:39	0d 5h 23m 38s	1/3	PING OK - Packet loss = 0%, RTA = 1.60 ms
	host_alive	OK	2006-12-18 23:35:12	0d 5h 25m 26s	1/4	PING OK - Packet loss = 0%, RTA = 0.60 ms
w20000rv	check_alive	CRITICAL	2006-12-18 23:33:17	0d 5h 20m 4s	1/3	CRITICAL - Plugin timed out after 10 seconds
	host_alive	CRITICAL	2006-12-18 23:34:39	0d 5h 19m 46s	1/4	CRITICAL - Plugin timed out after 10 seconds