



www.cnrs.fr

Mise en place d'un outil de supervision :



Grégory Hakon,
Ernest Chiarello,
Délégation Régionale Rhône Auvergne CNRS



I Plan

- | Un outils de supervision pour faire quoi ?
- | Historique
- | Les autres
- | Installation
- | Comment ça marche ?
- | Paramétrage
- | L'interface web
- | Personnalisations de la DR
- | Les plus
- | Les moins
- | Les sources



| Un outils de supervision pour faire quoi ?

- Vérifier les services du système d'information (HTTP, LDAP...)
- Surveiller les ressources des hôtes (charge CPU, espace disque...)
- Contrôler des équipement réseau (temps de réponse...)



I Historique

Nagios est entièrement basé sur le moteur de NetSaint , ancien outil de supervision réseau. Le développeur principal est Ethan Galstad

- Mars 1999 : première version de NetSaint
- Mars 2002 : dernière version de NetSaint
- Novembre 2002 : première version stable de Nagios 1.0
- Courant 2005 : sortie de la version 2.0 de Nagios
- Mars 2008 : sortie de la version 3.0 de Nagios
- Mars 2010 : dernière version stable 3.2.3



| Les autres outils

- Zabbix
- Icinga : fork de Nagios
- Shinken : fork de Nagios re-écrit en Python
- OpenNMS
- Centreon et Cacti en surcouche de Nagios



I Installation

Suivant votre distribution préférée :

- Fedora : *yum install nagios*
- Ubuntu : *apt-get install nagios3*
- Red Hat : RPM disponible sur <http://pkgs.repoforge.org/nagios/>
- Gentoo : *emerge nagios*
- OpenSUSE : à partir des sources

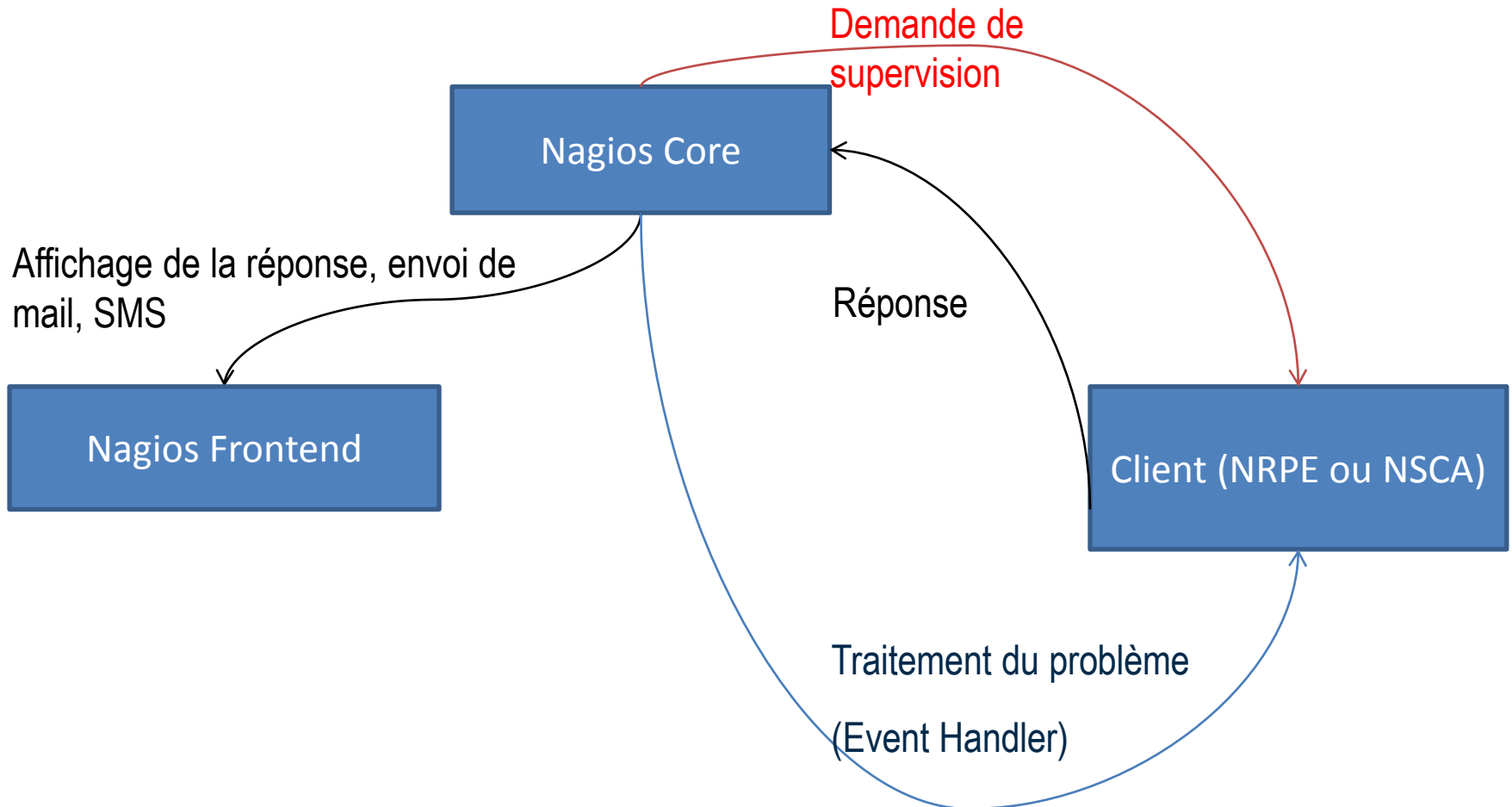
Nombreux tutoriels sur le sujet



I Comment ça marche ?

Trois parties :

- Le moteur de l'application qui vient ordonnancer les tâches de supervision (Nagios Core)
- L'interface web qui permet d'avoir la vue d'ensemble des points surveillés et ceux qui sont en faute (Nagios Frontends)
- Les plugins qui permettent de superviser les services ou ressources que l'on souhaite (Nagios Plugins)





I Paramétrage

Dans les fichiers de configuration du serveur :

- `/etc/nagios/cgi.cfg` pour gérer le script cgi
- `/etc/nagios/nagios.cfg` pour la partie serveur
- `/etc/nagios/objects/templates.cfg` pour les modèles
- `/etc/nagios/objects/commands.cfg` pour ajouter des commandes de supervision
- `/etc/nagios/objects/linux.cfg` pour décrire vos clients linux par exemple

Sur le client :

- `/etc/nagios/nrpe.cfg`



/etc/nagios/cgi.cfg

- main_config_file=/etc/nagios/nagios.cfg
- use_authentication=1
- use_ssl_authentication=1
- authorized_for_all_services=*
-



/etc/nagios/nagios.cfg

```
log_file=/var/log/nagios.log
```

```
cfg_file=/etc/nagios/objects/commands.cfg
```

```
cfg_file=/etc/nagios/objects/linux.cfg
```

```
....
```

```
process_performance_data=1
```

```
service_perfdata_command=process-service-perfdata
```

```
host_perfdata_command=process-host-perfdata
```



/etc/nagios/objects/templates.cfg

```
define host {
name                ALL
max_check_attempts  3
normal_check_interval 2
check_period        24x7
notification_interval 30
notification_period workhours
notification_options d,u,r
notifications_enabled 1
check_command       check-host-alive
contact_groups      admins
action_url           /pnp4nagios/graph?host=$HOSTNAME$
register             0
icon_image           gentoo.gif
statusmap_image      gentoo40.jpg
icon_image_alt       Serveur Gentoo
}
```



/etc/nagios/objects/templates.cfg

```
define service {
name                generic-service
service_description Reglage par défaut
max_check_attempts 4
normal_check_interval 4
retry_check_interval 1
check_period        24x7
notification_interval 30
notification_period workhours
notification_options w,c,r
notifications_enabled 1
contact_groups      admins
process_perf_data   0
Register            0
}
```



/etc/nagios/objects/commands.cfg

```
define command {  
    command_name    check-host-alive  
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p 1  
}
```

```
define command {  
    command_name    check-ldap-dr  
    command_line    /usr/lib/nagios/plugins/check_ldaps -H pravda.dr7.cnrs.fr -b dc=pravda,dc=dr7,dc=cnrs,dc=fr  
}
```



/etc/nagios/objects/linux.cfg

```
define host {
use                ALL,DMZ
host_name          oblatif
alias              Serveur de calendrier partagés
address            194.167.215.115
}

define hostgroup {
hostgroup_name     SERVEURS_nonRAID5
alias              Serveurs
Members            oblatif,parangon,picaresque,pravda,recamia
}
```



```
define service {
hostgroup_name      SERVEURS_nonRAID5
use                 generic-service
service_description Espace disque
check_command       check_nrpe!check_disk_all
name                Espace disque
action_url          /pnp4nagios/graph?host=$HOSTNAME&&srv=$SERVICEDESC$
process_perf_data   1
}
```




/etc/nagios/nrpe.cfg

PORT NUMBER

server_port=5666

ALLOWED HOST ADDRESSES

allowed_hosts=194.167.215.73

DESCRIPTION DES COMMANDES

command[check_disk_all]=/usr/lib/nagios/plugins/check_disk -w 10% -c 5% -u MB



I L'interface web

- Permet d'avoir une vue rapide des services ou des hôtes
- Permet d'ordonnancer manuellement
- Permet d'établir une cartographie du réseau
- Affiche un historique des alertes
- Est personnalisable grâce à de nombreux thème fournis par la communauté



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: Wed Jun 15 10:52:48 CEST 2011
 Updated every 90 seconds
 Nagios® Core™ 3.2.1 - www.nagios.org
 Logged in as Gregory Hakon

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

Host Status Totals

Up	Down	Unreachable	Pending
61	2	0	0
All Problems		All Types	
2		63	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
216	2	0	1	0
All Problems		All Types		
3		219		

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
affide	Espace disque	OK	15-06-2011 10:52:31	13d 22h 24m 25s	1/4	DISK OK - free space: / 1 GB (23% inode=51%); /dev 0 GB (98% inode=99%); /var/log 4 GB (95% inode=99%); /var/lib/mysql 4 GB (95% inode=99%); /var/www 1 GB (97% inode=98%); /home/sauvegarde 3 GB (76% inode=99%); /dev/shm 0 GB (100% inode=99%);
	Etat des disques	OK	15-06-2011 10:50:51	13d 22h 24m 24s	1/4	OK : tous les disques sont ok!
	OpenVpn	OK	15-06-2011 10:51:11	13d 22h 24m 21s	1/4	PROCS OK: 1 processus avec nom de la commande 'openvpn'
	Sauvegarde locale	OK	15-06-2011 10:29:31	79d 2h 33m 41s	1/4	OK: sauvegarde locale sans erreur
	Sauvegarde sur choukran	OK	15-06-2011 10:52:34	5d 4h 38m 42s	1/4	OK: envoi de la sauvegarde sur choukran
	Syslog-ng	OK	15-06-2011 10:50:54	13d 22h 24m 25s	1/4	PROCS OK: 2 processus avec nom de la commande 'syslog-ng'
	Temperature des disques	OK	15-06-2011 10:51:14	13d 22h 24m 24s	1/4	OK : la temperature des disques est hda = 30, hdb = 31,
ampliation	Espace disque	OK	15-06-2011 10:51:35	49d 20h 38m 9s	1/4	DISK OK - free space: / 2 GB (42% inode=44%); /dev 0 GB (98% inode=99%); /var/log 4 GB (96% inode=99%); /home/sauvegarde 4 GB (96% inode=99%); /dev/shm 0 GB (100% inode=99%);
	Etat des disques	OK	15-06-2011 10:52:37	49d 20h 37m 8s	1/4	OK : tous les disques sont ok!
	OpenVpn	OK	15-06-2011 10:50:56	49d 20h 37m 22s	1/4	PROCS OK: 1 processus avec nom de la commande 'openvpn'
	Sauvegarde locale	OK	15-06-2011 10:27:16	49d 20h 20m 19s	1/4	OK: sauvegarde locale sans erreur
	Sauvegarde sur choukran	OK	15-06-2011 10:29:36	5d 5h 0m 23s	1/4	OK: envoi de la sauvegarde sur choukran
	Syslog-ng	OK	15-06-2011 10:52:39	49d 20h 37m 17s	1/4	PROCS OK: 2 processus avec nom de la commande 'syslog-ng'
	Temperature des disques	OK	15-06-2011 10:50:59	25d 9h 3m 14s	1/4	OK : la temperature des disques est hda = 32, hdb = 29,
aporie	Espace disque	OK	15-06-2011 10:51:19	13d 22h 24m 24s	1/4	DISK OK - free space: / 0 GB (15% inode=70%); /dev 0 GB (98% inode=99%); /var/log 4 GB (94% inode=99%); /usr 3 GB (34% inode=38%); /usr/portage 9 GB (68% inode=85%); /home/sauvegarde 4 GB (96% inode=99%); /dev/shm 0 GB (100% inode=99%);
	Etat des disques	OK	15-06-2011 10:51:39	13d 22h 24m 24s	1/4	OK : tous les disques sont ok!
	OpenVpn	OK	15-06-2011 10:50:43	13d 22h 24m 24s	1/4	PROCS OK: 1 processus avec nom de la commande 'openvpn'
	Sauvegarde locale	OK	15-06-2011 10:25:02	76d 19h 23m 53s	1/4	OK: sauvegarde locale sans erreur
	Sauvegarde sur choukran	OK	15-06-2011 10:27:23	5d 5h 3m 2s	1/4	OK: envoi de la sauvegarde sur choukran
	Syslog-ng	OK	15-06-2011 10:51:41	13d 22h 24m 24s	1/4	PROCS OK: 2 processus avec nom de la commande 'syslog-ng'
	Temperature des disques	OK	15-06-2011 10:50:45	13d 22h 24m 24s	1/4	OK : la temperature des disques est hda = 34, hdb = 31,
aroutie	Espace disque	OK	15-06-2011 10:51:04	9d 0h 4m 44s	1/4	DISK OK - free space: / 1 GB (30% inode=50%); /dev 0 GB (98% inode=99%); /var/log 4 GB (95% inode=99%); /home/sauvegarde 3 GB (91% inode=99%); /dev/shm 0 GB (100% inode=99%);
	Etat des disques	OK	15-06-2011 10:51:25	79d 2h 33m 41s	1/4	OK : tous les disques sont ok!

Les services à problèmes

Current Network Status
 Last Updated: Wed Jun 15 12:26:19 CEST 2011
 Updated every 90 seconds
 Nagios® Core™ 3.2.1 - www.nagios.org
 Logged in as Gregory Hakon

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

Display Filters:
 Host Status Types: All
 Host Properties: Any
 Service Status Types: All Problems
 Service Properties: Any

Host Status Totals

Up	Down	Unreachable	Pending
60	3	0	0
All Problems		All Types	
3		63	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
211	2	0	6	0
All Problems		All Types		
8		219		

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
choukran	Backuppc sur choukran	CRITICAL	15-06-2011 12:24:50	0d 0h 53m 29s	1/4	Connection refused or timed out
	DirLogs sur choukran	CRITICAL	15-06-2011 12:24:09	0d 0h 54m 10s	1/4	Connection refused or timed out
	Espace disque	CRITICAL	15-06-2011 12:25:15	0d 0h 53m 6s	1/4	Connection refused or timed out
	FileLogs sur choukran	CRITICAL	15-06-2011 12:24:35	0d 0h 53m 44s	1/4	Connection refused or timed out
	Syslog-ng	CRITICAL	15-06-2011 12:25:54	0d 0h 54m 26s	1/4	Connection refused or timed out
firewall	Ntop	CRITICAL	15-06-2011 12:24:37	9d 3h 10m 20s	4/4	PROCS CRITIQUE: 0 processus avec nom de la commande 'ntop'
paranqon	Sauvegarde locale	WARNING	15-06-2011 12:01:16	1d 11h 31m 43s	4/4	Warning: probleme dans la sauvegarde. /home/sauvegarde/paranqon/erreur is 41344 seconds old and 69 bytes
pravda	Espace disque	WARNING	15-06-2011 12:24:46	8d 19h 7m 1s	4/4	DISK WARNING - free space: / 2 GB (32% inode=41%); /dev 0 GB (98% inode=99%); /var/log 4 GB (93% inode=99%); /home/sauvegarde 19 GB (99% inode=99%); /home/partimage 6 GB (9% inode=99%); /export/home 4 GB (14% inode=98%); /dev/shm 0 GB (100% inode=99%);

8 Matching Service Entries Displayed



Détail d'un serveur

Current Network Status
 Last Updated: Wed Jun 15 11:24:10 CEST 2011
 Updated every 90 seconds
 Nagios® Core™ 3.2.1 - www.nagios.org
 Logged in as Gregory Hakon

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

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0
All Problems		All Types	
0		1	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
7	0	0	0	0
All Problems		All Types		
0		7		

Service Status Details For Host 'oblatif'

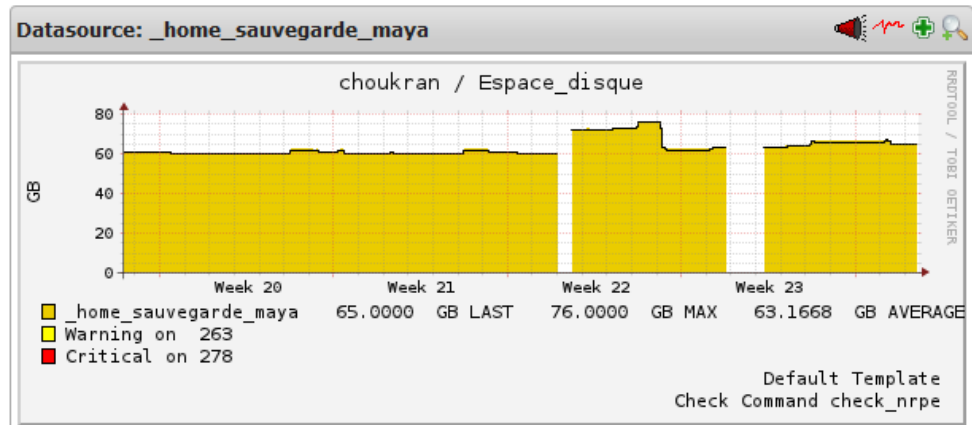
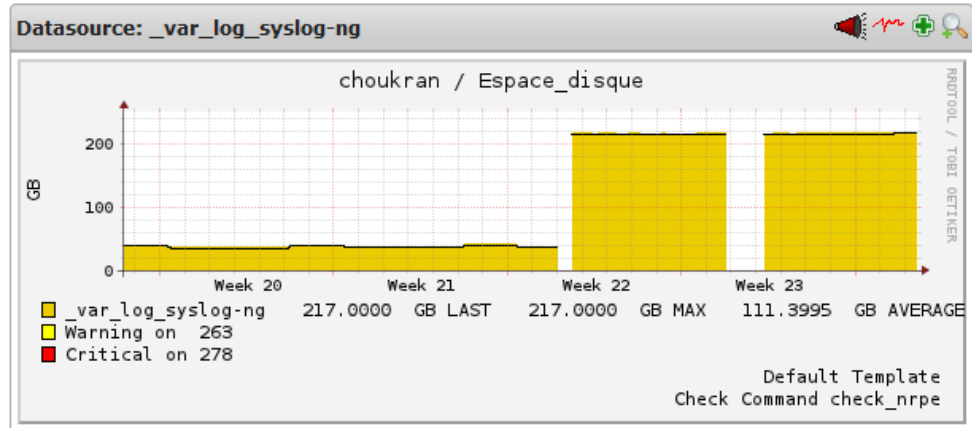
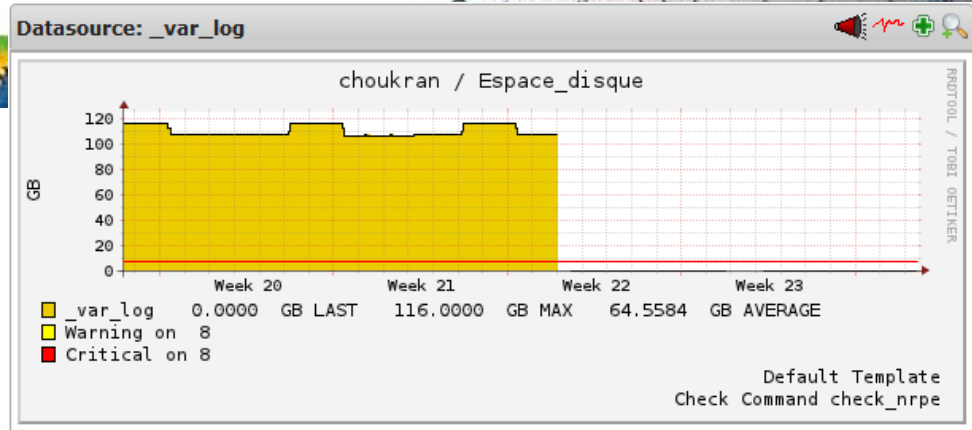
Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
oblatif	Espace disque	OK	15-06-2011 11:22:31	10d 10h 13m 45s	1/4	DISK OK - free space: / 0 GB (20% inode=52%); /dev 0 GB (98% inode=99%); /var/log 3 GB (69% inode=99%); /var/lib/postgresql 1 GB (81% inode=98%); /var/www 0 GB (89% inode=94%); /var/lib/egroupware 1 GB (97% inode=99%); /home/sauvegarde 13 GB (79% inode=96%); /dev/shm 0 GB (100% inode=99%);
	Etat des disques	OK	15-06-2011 11:22:51	13d 22h 55m 46s	1/4	OK : tous les disques sont ok !
	OpenVpn	OK	15-06-2011 11:23:11	13d 22h 55m 46s	1/4	PROCS OK: 1 processus avec nom de la commande 'openvpn'
	Sauvegarde locale	OK	15-06-2011 10:54:13	76d 20h 22m 31s	1/4	OK: sauvegarde locale sans erreur
	Sauvegarde sur choukran	OK	15-06-2011 10:56:33	5d 5h 8m 8s	1/4	OK: envoi de la sauvegarde sur choukran
	Syslog-ng	OK	15-06-2011 11:22:53	13d 22h 55m 47s	1/4	PROCS OK: 2 processus avec nom de la commande 'syslog-ng'
	Temperature des disques	OK	15-06-2011 11:23:13	13d 22h 55m 46s	1/4	OK : la temperature des disques est hda = 32, hdb = 31,

7 Matching Service Entries Displayed



Visualisation en graphique avec PNP4Nagios

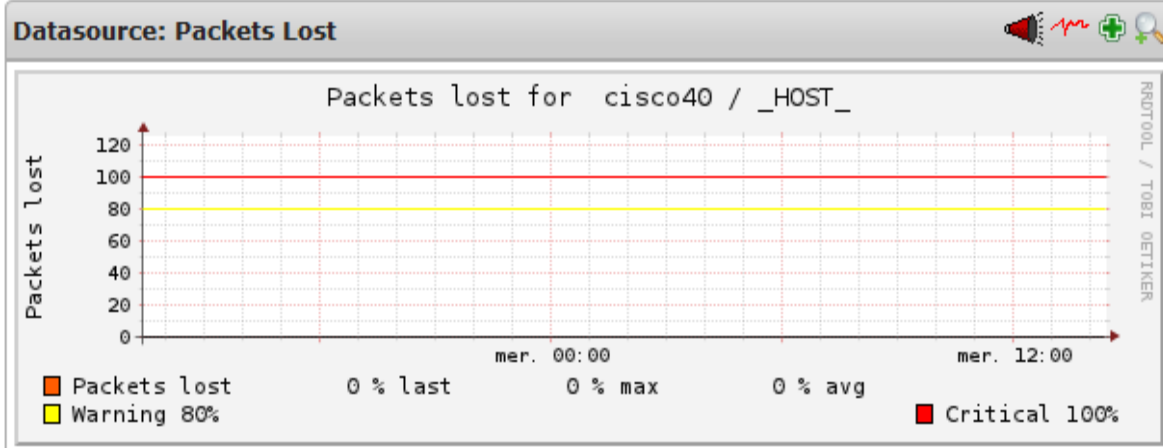
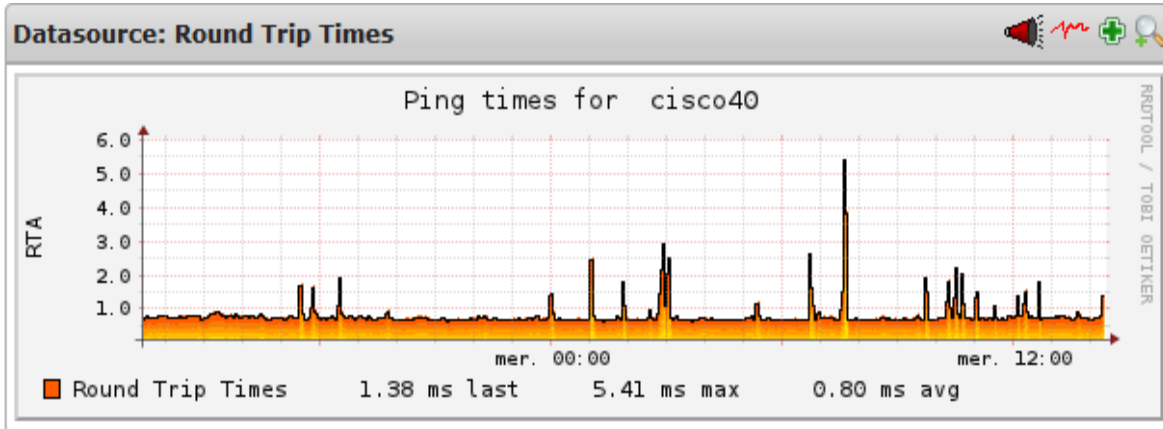
Espace disque





Visualisation en graphique avec PNP4Nagios

Réponse au ping





I Personnalisations de la DR

- Authentification par certificats CNRS
- Création de commandes pour superviser :
 - les sauvegardes
 - les températures des disques
 - la centralisation des logs
- Un seul fichier nrpe.cfg



Authentication x509

- Dans le cgi.cfg
 - use_authentication=1
 - use_ssl_authentication=1
 - authorized_for_all_services=*

- Dans la configuration d'apache

```

<Location />
Satisfy any
AuthType Basic
Require valid-user
#####
####Authentication par certificats
#####
SSLVerifyClient optional
SSLVerifyDepth 3
SSLRequireSSL
SSLUserName SSL_CLIENT_S_DN_CN
SSLRequire %{SSL_CLIENT_S_DN_OU} eq "MOY700"
SSLRequire %{SSL_CLIENT_I_DN_CN} in {"CNRS2-Plus"}
#####
####En local
AuthUserFile /etc/nagios/htpasswd.users
AuthName "Authentication Local"
#####
</Location>
    
```



Les commandes personnalisées

- Température des disques
 - Script en perl
 - Utilisation de SmartMonTools
 - Sorties Nagios : « Warning, Critical, Unknown »
 - Génération des données de performance RTA pour affichage en graphique
 - Deux scripts :
 - exécuté par nagios : remonte les t° min et max
 - exécuté par root : analyse le résultat et arrête la machine

Les commandes personnalisées

- Script exécuté par nagios

...

```
$temp_disque = `/usr/sbin/smartctl -A /dev/$device | grep Temperature_Celsius |
sed 's/ */;/g' | cut -d ';' -f 10`;
```

....

```
# on ecrit la temperature minimum si et seulement si la machine
```

```
# tourne depuis au moins 2h (7200s)
```

```
if ($uptime > 7200) {
```

```
    if ( $temp_disque < $temp_min ) {
```

```
        `echo "$temp_disque" > /usr/local/nagios/temp_min_$device`;
```

```
    }
```

```
}
```



Les commandes personnalisées

- Script exécuté dans un cron par root

...

```
$temp_arret = ( $temp_min + 15 );  
    if ( $temp_disque > $temp_arret ) {  
        print "Trop chaud, on arrete la machine\n";  
        `echo -e "Le disque $device est trop chaud, on arrete la machine" | mail -s  
"$hostname disque trop chaud" admin\@dr7.cnrs.fr`;  
        `/sbin/shutdown -h -t 120 now`;  
    }
```



Les commandes personnalisées

- Centralisation des logs
 - Utilisation du script `check_file_age`
 - Vérification de la mise à jour des fichiers en fonction des serveurs :

```
# le fichier a-t-il plus de $hosts{$hostname} minutes ?
  $nagios_said = ` $nagios_pluginslib/check_file_age -c $hosts{$hostname} /var/log/syslog-
ng/$jour/$hostname/everything.log `;
....
if ($log) {
  print "Etat critique: log KO. Il faut relancer syslog-ng ou SNARE sur $log\n";
  exit 2;
}
```



Plugin nrpe

- Un seul fichier nrpe.cfg est géré sur un serveur modèle
- Echange de clé ssh pour la copie entre le serveur modèle et les clients
- Gestion des services à surveiller sur le serveur Nagios Core



| Les plus

- Un projet stable qui repose sur des fondations de plus de 10ans
- La base NagiosExchange (1957 plugins)
- De nombreux tutoriels
- Des graphiques avec PNP4Nagios ou Centreon
- Une configuration assez simple mais qui peut être hyper personnalisable



| Les moins

- Un projet qui semble stagner depuis la mise en place d'une solution sous Licence.
- Une interface graphique de base pas très ergonomique.



| Les sources

<http://www.nagios.org>

http://nagios.sourceforge.net/docs/3_0/configmain.html

<http://exchange.nagios.org>

<http://blog.nicolargo.com>

<http://www.monitoring-fr.org>

<http://fr.wikipedia.org/wiki/Nagios>



www.cnrs.fr

Merci

Questions ?