

Titre

Auteurs :
NOMS

Référence		Version	1.0
Avancement		<input type="checkbox"/> Validé <input type="checkbox"/> Validé après modif. <input type="checkbox"/> Revalidé	
Dernière mise à jour			

Visa			
Date		Responsable	

Table des matières

1	Historique du document	4
2	Annexe 4 : Organisation de Nagios	5
2.1	NAGIOS	5
2.1.1	NSC.INI	5
2.1.2	NAGIOS.CFG	6
2.1.3	WINDOWS.CFG	7
2.2	Résultats NAGIOS	9
2.3	MRTG	15
2.3.1	134.214.105.222.cfg	15
2.4	Résultats MRTG	16
2.5	NRPE	18
2.5.1	NRPE.CFG	18
2.5.2	h4312_linux.cfg	20
2.5.3	NAGIOS.CFG	21
2.6	Résultats NRPE	22
2.7	Analyse critique de l'Installation/Utilisation de Nagios	23

1 Historique du document

Date	Auteur	Version	Sujet de la modification

2 Annexe 4 : Organisation de Nagios

Parmi les logiciels libre de supervision, Nagios est le plus répandu et également le plus suivi par la communauté de développeur. Nagios (anciennement appelé Netsaint) est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes vont mal et quand ils vont mieux.

2.1 NAGIOS

Nous allons ajouter la machine windows if213-06 , IP 134.214.105.165. On va modifier les fichiers de configuration : en premier le fichier NSC.ini de NSClient++ et après Nagios.cfg et Windows.cfg sur le serveur Nagios (à travers une connexion SSH). En fait on va créer un fichier de configuration (Exemple.cfg) pour chaque host qu'on ajoute et va ajouter ce fichier dans Nagios.cfg (cfg_file=/usr/local/nagios/etc/objects/Exe

2.1.1 NSC.INI

[modules]

FileLogger.dll

CheckSystem.dll

CheckDisk.dll

NSClientListener.dll

NRPEListener.dll

SysTray.dll

CheckEventLog.dll

CheckHelpers.dll

;CheckWMI.dll

[Settings]

;# OBFUSCATED PASSWORD

; This is the same as the password option but here you can store the password in an obfuscated manner.

; *NOTICE* obfuscation is *NOT* the same as encryption, someone with access to this file can still figure out the

; password. Its just a bit harder to do it at first glance.

;obfuscated_password=Jw0KAUUdXIAAUwASDAAB

;

;# PASSWORD

; This is the password (-s) that is required to access NSClient remotely. If you leave this blank everyone will be able to access the daemon remotly.

```

password=passe
;
;# ALLOWED HOST ADDRESSES
; This is a comma-delimited list of IP address of hosts that are allowed to talk to the all daemons.
; If leave this blank anyone can access the daemon remotly (NSClient still requires a valid password).
allowed_hosts=134.214.105.165,134.214.105.156
[log]
;# LOG DEBUG
; Set to 1 if you want debug message printed in the log file (debug messages are always printed to
stdout when run with -test)
;debug=1
;
;# LOG FILE
; The file to print log statements to
file=NSC_H4312.log
;
;# LOG DATE MASK
; The format to for the date/time part of the log entry written to file.
;date_mask=%Y-%m-%d %H :%M :%S
[NSClient]
;# NSCLIENT PORT NUMBER
; This is the port the NSClientListener.dll will listen to.
port=12489

```

2.1.2 NAGIOS.CFG

```

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg

```

2.1.3 WINDOWS.CFG

```
#####  
#####  
#  
# HOST DEFINITIONS  
#  
#####  
#####  
# Define a host for the Windows machine we'll be monitoring  
# Change the host_name, alias, and address to fit your situation  
define host{  
    use windows-server ; Inherit default values from a template  
    host_name if213-06 ; The name we're giving to this host  
    alias Machine-test ; longer name associated with the host  
    address 134.214.105.165 ; IP address of the host  
}  
#####  
#####  
#  
# HOST GROUP DEFINITIONS  
#  
#####  
#####  
# Define a hostgroup for Windows machines  
# All hosts that use the windows-server template will automatically be a member of this group  
define hostgroup{  
    hostgroup_name windows-servers ; The name of the hostgroup  
    alias Windows Servers ; Long name of the group  
}  
#####  
#####  
#  
# SERVICE DEFINITIONS
```

```
#
```

```
#####
```

```
#####
```

```
# Create a service for monitoring the version of NSClient++ that is installed
```

```
# Change the host_name to match the name of the host you defined above
```

```
define service{
```

```
use generic-service
```

```
host_name if213-06
```

```
service_description NSClient++ Version
```

```
check_command check_nt !CLIENTVERSION
```

```
}
```

```
# Create a service for monitoring the uptime of the server
```

```
# Change the host_name to match the name of the host you defined above
```

```
define service{
```

```
use generic-service
```

```
host_name if213-06
```

```
service_description Uptime
```

```
check_command check_nt !UPTIME
```

```
}
```

```
# Create a service for monitoring CPU load
```

```
# Change the host_name to match the name of the host you defined above
```

```
define service{
```

```
use generic-service
```

```
host_name if213-06
```

```
service_description CPU Load
```

```
check_command check_nt !CPULOAD !-I 5,80,90
```

```
}
```

```
# Create a service for monitoring memory usage
```

```
# Change the host_name to match the name of the host you defined above
```

```
define service{
```

```
use generic-service
```

```
host_name if213-06
```

```
service_description Memory Usage
```



```

check_command check_nt !MEMUSE !-w 80 -c 90
}
# Create a service for monitoring C :\ disk usage
# Change the host_name to match the name of the host you defined above
define service{
use generic-service
host_name if213-06
service_description C :\ Drive Space
check_command check_nt !USEDISKSPACE !-l c -w 80 -c 90
}
# Create a service for monitoring the W3SVC service
# Change the host_name to match the name of the host you defined above
define service{
use generic-service
host_name if213-06
service_description W3SVC
check_command check_nt !SERVICESTATE !-d SHOWALL -l W3SVC
}
# Create a service for monitoring the Explorer.exe process
# Change the host_name to match the name of the host you defined above
define service{
use generic-service
host_name if213-06
service_description Explorer
check_command check_nt !PROCSTATE !-d SHOWALL -l Explorer.exe
}

```

2.2 Résultats NAGIOS

On va commencer par monter la machine que nous avons ajouté : if213-06.


Current Network Status
 Last Updated: Thu Apr 7 12:22:01 CEST 2011
 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
3	0	0	1
All Problems		All Types	
0		4	

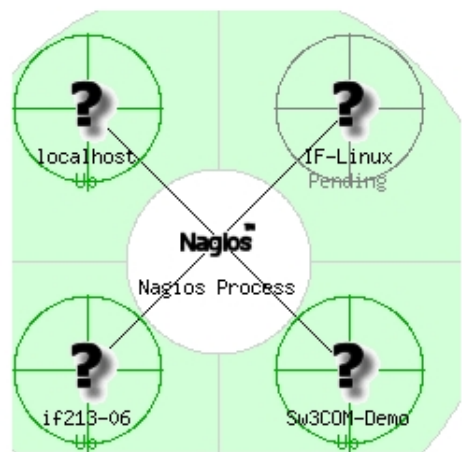
Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
17	1	1	5	0
All Problems		All Types		
7		24		

Host Status Details For All Host Groups

Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
IF-Linux 	PENDING	N/A	13d 5h 10m 28s	Host check scheduled for Thu Apr 7 12:24:30 CEST 2011
Sw3COM-Demo 	UP	04-07-2011 12:20:24	5d 23h 44m 41s	PING OK - Paquets perdus = 0%, RTA = 1.69 ms
if213-06 	UP	04-07-2011 12:19:54	0d 5h 48m 7s	PING OK - Paquets perdus = 0%, RTA = 0.39 ms
localhost 	UP	04-07-2011 12:16:54	402d 8h 3m 53s	PING OK - Paquets perdus = 0%, RTA = 0.03 ms

4 Matching Host Entries Displayed

Localhost est la machine propre à Nagios.
 La carte gerée pas Nagios :



On peut aussi voir les details d'etat de chaque host et faire des check manuellement :

11

On va essayer eteindre la machine if213-06, faire un check manuellement et regarder a partir d'une autre machine son status :

Nagios - Mozilla Firefox

Page précédente Page suivante

Historique

Actuel

Planète INSA

Emploi du temps

Webmail

Support

Nagios

Current Network Status

Last Updated: Wed Apr 6 17:52:35 CEST 2011

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
3	0	0	1

All Problems **All Types**

0 4

Service Status Totals

OK	Warning	Unknown	Critical	Pending
12	0	1	11	0

All Problems **All Types**

12 24

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
if213-06	Port 1241 Link Status	OK	04-06-2011 17:45:51	11d 14h 9m 9s	3/3	CHECK_NRPE Error - Could not complete SSL handshake.
if213-06	Port 24 Bandwidth Usage	OK	04-06-2011 17:47:12	11d 14h 11m 2s	3/3	CHECK_NRPE Error - Could not complete SSL handshake.
if213-06	TRAP	OK	04-06-2011 17:48:33	11d 14h 7m 50s	3/3	CHECK_NRPE Error - Could not complete SSL handshake.
if213-06	Uptime	OK	04-06-2011 17:49:55	11d 14h 16m 31s	3/3	CHECK_NRPE Error - Could not complete SSL handshake.
if213-06	SNMP OK - Packets per second	OK	04-06-2011 17:51:16	5d 5h 11m 19s	1/3	PING OK - Packets per second = 0%, RTA = 1.97 ms
if213-06	SNMP OK - up(1)	OK	04-06-2011 17:42:37	5d 5h 9m 58s	1/3	SNMP OK - up(1)
if213-06	Port 24 Bandwidth Usage	OK	04-06-2011 17:44:11	0d 7h 28m 24s	1/3	Traffic OK - Moyenne Entrée = 3.5 Kbits, Moyenne Sortie = 127.0 Kbits
if213-06	TRAP	OK	04-06-2011 17:51:30	12d 5h 1m 22s	3/3	No OIDs specified
if213-06	Uptime	OK	04-06-2011 17:46:54	5d 5h 13m 41s	1/3	SNMP OK - Timeticks: (45072792) 5 days, 5:12:07.92
if213-06	CPU Drive Space	CRITICAL	04-06-2011 17:51:15	0d 0h 1m 20s	1/3	Connexion refusée
if213-06	CPU Load	CRITICAL	04-06-2011 17:51:43	0d 0h 0m 52s	1/3	Connexion refusée
if213-06	Explorer	CRITICAL	04-06-2011 17:44:29	0d 0h 20m 18s	3/3	Explorer.exe: Stopped
if213-06	Memory Usage	CRITICAL	04-06-2011 17:52:02	0d 0h 0m 33s	1/3	Connexion refusée
if213-06	NSClient++ Version	CRITICAL	04-06-2011 17:51:43	0d 0h 0m 52s	1/3	Connexion refusée
if213-06	Uptime	CRITICAL	04-06-2011 17:52:18	0d 0h 0m 17s	1/3	Connexion refusée
if213-06	WGSVC	CRITICAL	04-06-2011 17:52:28	0d 0h 0m 7s	3/3	Connexion refusée
if213-06	Current Load	OK	04-06-2011 17:50:15	412d 17h 5m 39s	1/4	OK - Charge moyenne: 0.00, 0.00, 0.00
if213-06	Current Users	OK	04-06-2011 17:51:36	412d 17h 11m 35s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
if213-06	HTTP	OK	04-06-2011 17:47:57	10d 17h 14m 39s	1/4	HTTP OK HTTP/1.1 200 OK - 374 bytes en 0.001 secondes
if213-06	PING	OK	04-06-2011 17:51:31	401d 13h 32m 45s	1/4	PING OK - Packets per second = 0%, RTA = 0.03 ms
if213-06	Root Partition	OK	04-06-2011 17:47:53	412d 17h 12m 9s	1/4	DISK OK - free space: 79413 MB (73% inode=96%)
if213-06	SSH	OK	04-06-2011 17:49:14	401d 13h 31m 30s	1/4	SSH OK - OpenSSH_4.3 (protocol 2.0)
if213-06	Swap Usage	OK	04-06-2011 17:50:35	412d 17h 10m 54s	1/4	SWAP OK - 100% libre (1357 MB sur un total de 1357 MB)
if213-06	Total Processes	OK	04-06-2011 17:51:56	412d 17h 10m 18s	1/4	PROCS OK - 19 processus avec ETAT = RSZDT

Reports

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

System

- Comments
- Downtime
- Process Info
- Performance Info

[démarrer](#)

FR

17:52

On peut voir que tous les services sont passés à critical d'où on a bien détecté que la machine à était éteinte.

En suite on va regarder les problemes, les raports et les alerts.

Pour voir les problemes au moment actuel on peut cliquer sur Problems.

Current Network Status
Last Updated: Thu Apr 7 12:24:01 CEST 2011
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
3	0	0	1

All Problems	All Types
0	4

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
17	1	1	5	0

All Problems	All Types
7	24

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

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
IF-Linux	All Procs	CRITICAL	04-07-2011 12:15:51	12d 8h 40m 35s	3/3	CHECK_NRPE: Error - Could not complete SSL handshake.
	CPU Load	CRITICAL	04-07-2011 12:17:12	12d 8h 42m 28s	3/3	CHECK_NRPE: Error - Could not complete SSL handshake.
	Users	CRITICAL	04-07-2011 12:18:33	12d 8h 39m 16s	3/3	CHECK_NRPE: Error - Could not complete SSL handshake.
	Zombie	CRITICAL	04-07-2011 12:19:55	12d 8h 47m 57s	3/3	CHECK_NRPE: Error - Could not complete SSL handshake.
Sw3COM-Demo	TRAP	UNKNOWN	04-07-2011 12:21:30	13d 3h 32m 48s	3/3	No OIDs specified
if213-06	Explorer	CRITICAL	04-07-2011 12:20:50	0d 18h 51m 44s	3/3	Explorer.exe: Stopped
	W3SVC	WARNING	04-07-2011 12:16:28	0d 5h 51m 33s	3/3	W3SVC: Unknown

7 Matching Service Entries Displayed

Pat contre, si on veut avoir de statistiques au consulter l'historique, on peut le faire dans la partie Reports. On va créer un rapport pour la derniere semaine et regarder l'activité de tous les hosts :

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

Hostgroup Availability Report

Last Updated: Thu Apr 7 12:25:34 CEST 2011
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as *nagiosadmin*

All Hostgroups

03-31-2011 12:25:34 to 04-07-2011 12:25:34

Duration: 7d 0h 0m 0s

First assumed host state: Unspecified

First assumed service state: Unspecified

Report period: Last 7 Days

Backtracked archives: 4

Update

[Availability report completed in 0 min 0 sec]

Hostgroup 'linux-servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
localhost	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Hostgroup 'switches' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
Sw3COM-Demo	85.598% (85.598%)	14.402% (14.402%)	0.000% (0.000%)	0.000%
Average	85.598% (85.598%)	14.402% (14.402%)	0.000% (0.000%)	0.000%

Hostgroup 'windows-servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
if213-06	3.489% (33.192%)	7.022% (66.808%)	0.000% (0.000%)	89.489%
Average	3.489% (33.192%)	7.022% (66.808%)	0.000% (0.000%)	89.489%

On peut aussi regrader l'activité plus en détail d'un seul host. Pour exemple notre host, if213-06 pendant les dernières 24h :

Host Availability Report

Last Updated: Thu Apr 7 12:27:53 CEST 2011
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as *nagiosadmin*

Host 'if213-06'

04-06-2011 12:27:40 to 04-07-2011 12:27:40

Duration: 1d 0h 0m 0s

First assumed host state: Unspecified

First assumed service state: Unspecified

Report period: [Current time range]

Backtracked archives: 4

Update

[Availability report completed in 0 min 0 sec]

Host State Breakdowns:

UP

DOWN

UNREACHABLE

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	0d 5h 53m 46s	24.567%	33.324%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 5h 53m 46s	24.567%	33.324%
DOWN	Unscheduled	0d 11h 47m 50s	49.155%	66.676%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 11h 47m 50s	49.155%	66.676%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Nagios Not Running		0d 0h 0m 0s	0.000%	

2.3 MRTG

On va monitorer le switch 134.214.105.222.

Dans un premier temps on va créer le dossier /var/www/mrtg/134.214.105.222

```
sudo mkdir /var/www/mrtg/A.B.C.D
```

On ajoute la machine a superviser et donc on crée son fichier de configuration (un fichier de configuration/machine a superviser)

```
cfgmaker -global 'WorkDir : /var/www/mrtg/134.214.105.222' \ -ifdesc=descr \ -global 'Language : french' \ -global 'Options[_] : bits,growright' \ public@134.214.105.222 > /var/www/mrtg/134.214.105.222/134.222.cfg
```

Gérer automatiquement les graphes : nous allons donc créer un script SHELL que nous lancerons en utilisant la crontab. Ce script SHELL va lancer MRTG avec le fichier de configuration créé auparavant.

```
#!/bin/sh # /var/www/mrtg/134.214.105.222 env LANG=C /usr/bin/mrtg /var/www/mrtg/134.214.105.222/134.222.cfg
```

Puis on lui donne les droits en exécution :

```
chmod a+x /usr/local/bin/mrtgcron.sh
```

Et enfin, on programme la crontab (crontab -l) en ajoutant la ligne suivante :

```
*/5 * * * * /usr/local/bin/mrtgcron.sh
```

2.3.1 134.214.105.222.cfg

Pour pouvoir voir et afficher les graphes il faut ajouter une entrée pour chaque graphe dans le fichier de configuration 134.214.105.222.cfg (on va mettre ici que le code pour le premier graphe, les 3 autres étant similaires).

```
# /usr/bin/cfgmaker -global 'WorkDir : /var/www/mrtg/134.214.105.222' -ifdesc=descr -global 'Language : french' -global 'Options[_] : bits,growright' public@134.214.105.222
```

```
### Global Defaults
```

```
EnableIPv6 : no
```

```
WorkDir : /var/www/mrtg/134.214.105.222
```

```
Language : french
```

```
Options[_] : bits,growright
```

```
### Interface 101 >> Descr : 'RMON-Port-01-on-unit-1' | Name : " | Ip : " | Eth : " ###
```

```
Target[134.214.105.222_101] : 101 :public@134.214.105.222 :
```

```
SetEnv[134.214.105.222_101] : MRTG_INT_IP="" MRTG_INT_DESCR="RMON-Port-01-on-unit-1"
```

```
MaxBytes[134.214.105.222_101] : 12500000
```

```
Title[134.214.105.222_101] : RMON Port 01 on unit 1 – switchTP222
```

```
PageTop[134.214.105.222_101] : <h1>RMON Port 01 on unit 1 – switchTP222</h1>
```

```

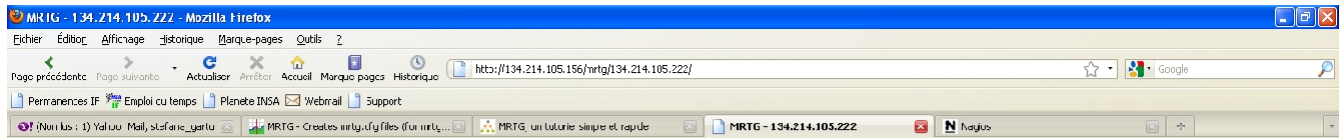
<div id="sysdetails">
<table>
<tr>
<td>System :</td>
<td>switchTP222 in chez nous</td>
</tr>
<tr>
<td>Maintainer :</td>
<td>admin</td>
</tr>
<tr>
<td>Description :</td>
<td>RMON-Port-01-on-unit-1 RMON Port 01 on unit 1 </td>
</tr>
<tr>
<td>ifType :</td>
<td>ethernetCsmacd (6)</td>
</tr>
<tr>
<td>ifName :</td>
<td></td>
</tr>
<tr>
<td>Max Speed :</td>
<td>100.0 Mbits/s</td>
</tr>
</table>
</div>

```

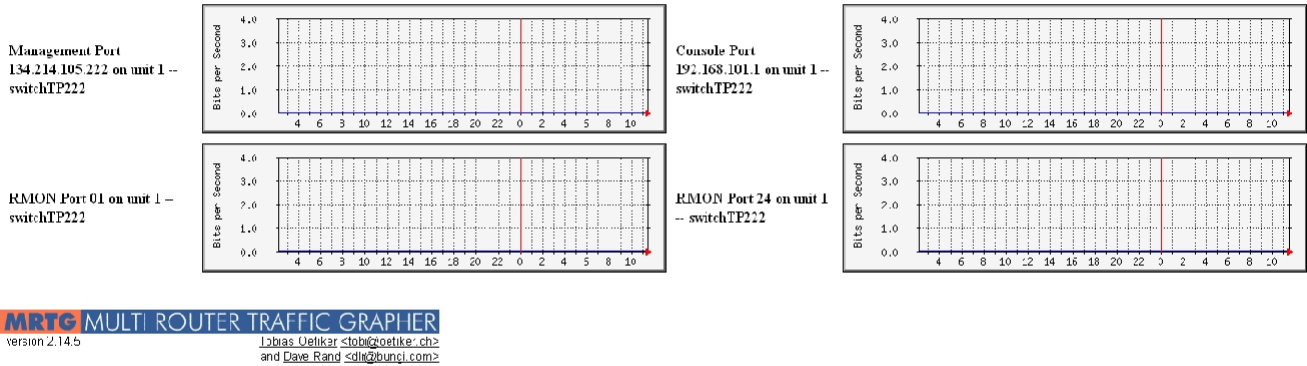
2.4 Résultats MRTG

On a monitorer pendant 3 jours. Dans le repertoire www/mrtg/134.214.105.222 on a 16 images generées automatiquement. On a des information par jour, semaine, mois, an pour les 4 ports choisis.

Au jour de demarrage :



MRTG - 134.214.105.222



Après 3 jours pour le Managemet Port, 134.214.105.222 on unit 1, swtchTP222 :

Image par jour :

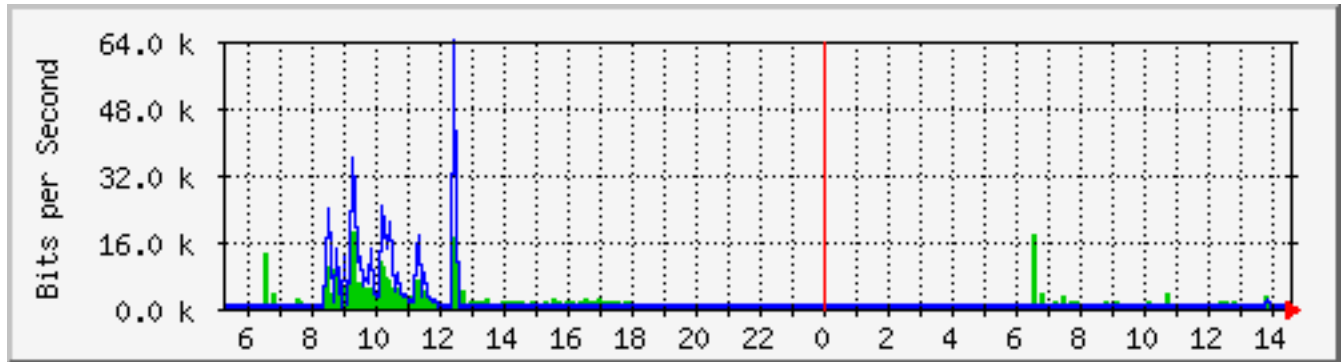


Image par semaine :

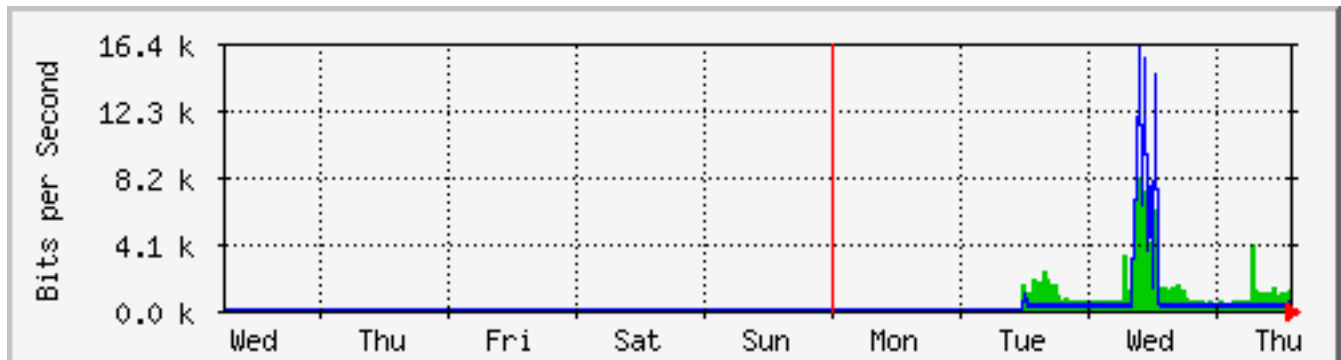


Image par mois :

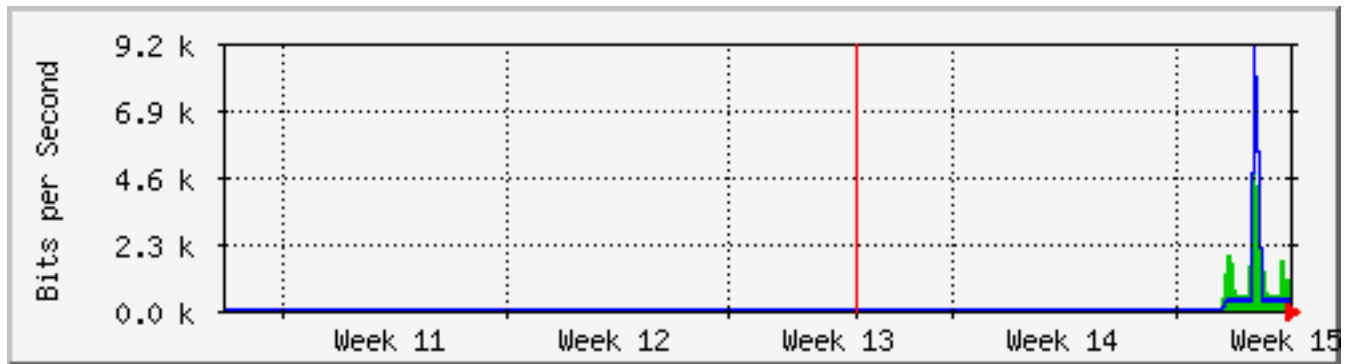
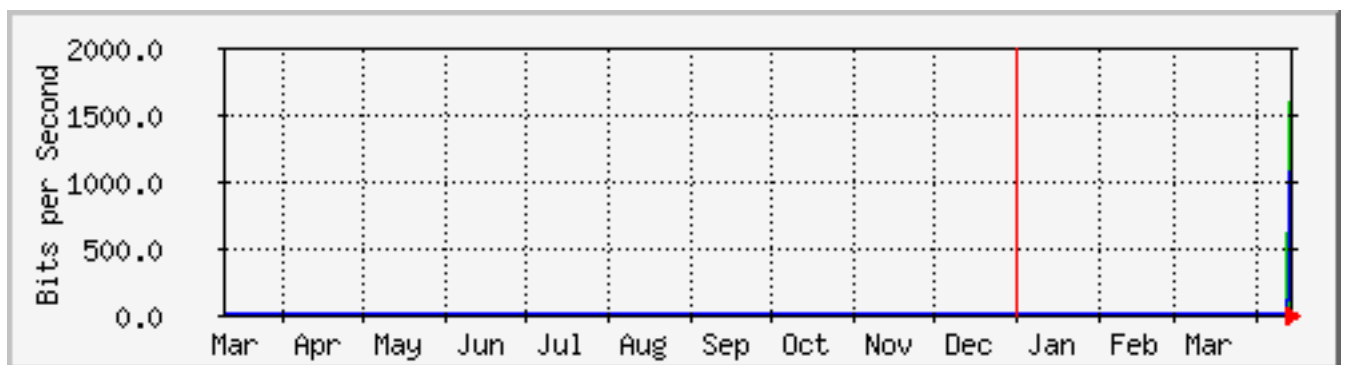


Image par an :



2.5 NRPE

A l'aide de NRPE on va superviser de machines Linux. On a ajouter la machine 134.214.105.189 (nom : h4312_linux) et on a changé la configuration du serveur Nagios pour qu'il utilise NRPE (nouveau nom : h4312_localhost).

On a repris la base NRPE qui était fournie et on l'a modifié pour pouvoir ajouter les deux machines.

2.5.1 NRPE.CFG

```
# LOG FACILITY
```

```
# The syslog facility that should be used for logging purposes.
```

```
log_facility=daemon
```

```
# PID FILE
```

```
# The name of the file in which the NRPE daemon should write it's process ID
```

```
# number. The file is only written if the NRPE daemon is started by the root
```

```
# user and is running in standalone mode.
```

```
pid_file=/var/run/nrpe.pid
```

```
# COMMAND ARGUMENT PROCESSING
```

```

# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK ! ***
# Read the SECURITY file for information on some of the security implications
# of enabling this variable.
#
# Values : 0=do not allow arguments, 1=allow command arguments
dont_blame_nrpe=0
# DEBUGGING OPTION
# This option determines whether or not debugging messages are logged to the
# syslog facility.
# Values : 0=debugging off, 1=debugging on
debug=0
# COMMAND TIMEOUT
# This specifies the maximum number of seconds that the NRPE daemon will
# allow plugins to finish executing before killing them off.
command_timeout=60
# CONNECTION TIMEOUT
# This specifies the maximum number of seconds that the NRPE daemon will
# wait for a connection to be established before exiting. This is sometimes
# seen where a network problem stops the SSL being established even though
# all network sessions are connected. This causes the nrpe daemons to
# accumulate, eating system resources. Do not set this too low.
connection_timeout=300
# COMMAND DEFINITIONS
# Command definitions that this daemon will run. Definitions
# are in the following format :
#
# command[<command_name>]=<command_line>
#

```

```
# When the daemon receives a request to return the results of <command_name>
# it will execute the command specified by the <command_line> argument.
#
# Unlike Nagios, the command line cannot contain macros - it must be
# typed exactly as it should be executed.
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10
command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20
command[check_hda1]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/sda1
command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200
command[check_hdd]=/usr/local/nagios/libexec/check_disk -w 20 -c 10 -p /
command[check_swaphdd]=/usr/local/nagios/libexec/check_swap -w 20 -c 10
```

2.5.2 h4312_linux.cfg

On a ajouter les services demandés (gestion des users, zombies, processus et charge CPU) pour monitorer la machine. Le code pour le serveur Nagios est similaire a celui-ci et donc on va pas le mettre dans le compte-rendu.

```
#####
# Monitoring teacher's linux avec NRPE
#####
#####
## HOST
#####
define host {
use linux-server
host_name h4312_linux
alias remote Linux
address 134.214.105.189
}
#####
## SERVICES
#####
# Charge CPU
```

```

define service{
use generic-service
host_name h4312_linux
service_description CPU Load
check_command check_nrpe!check_load
}

# Users
define service{
use generic-service
host_name h4312_linux
service_description Users
check_command check_nrpe!check_users
}

# Zombies
define service{
use generic-service
host_name h4312_linux
service_description Zombies
check_command check_nrpe!check_zombie_procs
}

# Processus
define service{
use generic-service
host_name h4312_linux
service_description Processus
check_command check_nrpe!check_total_procs
}

```

2.5.3 NAGIOS.CFG

```

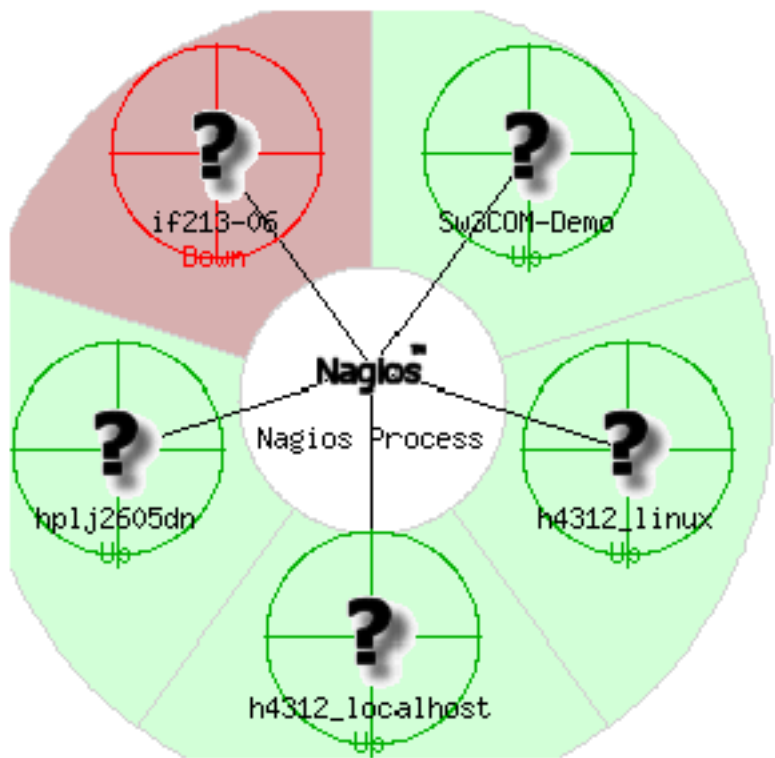
# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/h4312_localhost.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg

```

2.6 Résultats NRPE

On a ajouté la machine linux monitorée a l'aide de NRPE :



Le client sur la machine if213-06 est éteint. On peut visualiser pour la machine Linux le status des parametres qu'on a ajouté :

Current Network Status
Last Updated: Fri Apr 15 10:44:56 CEST 2011
Updated every 90 seconds
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as: *nagiosadmin*

[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 Details For Host 'h4312_linux'

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑
h4312_linux	CPU Load	OK	04-15-2011 10:44:37	0d 19h 10m 19s	1/3
	Processus	OK	04-15-2011 10:38:40	0d 18h 56m 16s	1/3
	Users	OK	04-15-2011 10:36:30	0d 18h 58m 26s	1/3
	Zombies	OK	04-15-2011 10:36:39	0d 18h 58m 17s	1/3

4 Matching Service Entries Displayed

2.7 Analyse critique de l'Installation/Utilisation de Nagios

Le gros avantage de Nagios est le fait que c'est un outil qui dispose d'une documentation très fournie. Il est très modulable et flexible grâce à son fonctionnement par fichier de configuration. Mais ce qui fait sa force fait aussi sa faiblesse car ces fichiers de configurations multiples peuvent poser des problèmes s'il y en a beaucoup, particulièrement lorsqu'on n'est pas habitué à cette méthode de fonctionnement. Cela nécessite une bonne organisation pour s'y retrouver mais lorsqu'on est bien organisé, on peut facilement automatiser le traitement des informations grâce à des scripts.

Son installation n'est pas très compliquée. C'est un simple système client-serveur. On installe le serveur puis les clients puis il faut configurer. Il faut configurer les clients pour qu'ils acceptent les connexions et les échanges d'information. Il faut configurer le serveur pour chaque client que l'on ajoute. Il faut savoir que l'on peut utiliser un seul fichier de configuration pour tout le programme mais ce n'est pas conseillé pour une raison de lisibilité. Il faut donc bien réfléchir à l'arborescence des fichiers dès le départ, ce qui peut être difficile lorsque l'on n'a pas l'habitude.

Son utilisation par l'interface web est assez intuitive et permet une navigation rapide entre les différents services associés aux machines monitorées. La maintenance (ajout de nouvelles machines, nouveaux services, ...) dépend beaucoup de la façon dont ont été créés les fichiers de configuration au départ. Cela peut donc varier entre très simple, voire automatisé et très compliqué. Pour nous, une fois que nous avons compris comment tout s'agencait, cela a été plutôt facile.

C'est un outil qui permet de regrouper les informations sur toutes les machines surveillées, ce qui est très pratique mais il ne fait que du monitoring système et ne permet pas le monitoring réseau. Il ne reconnaît pas non plus la topologie réseau, ce qui peut poser quelques problèmes, notamment lorsque les machines sont équipées d'adresses IP dynamiques (les fichiers de configurations ne peuvent pas prendre en compte ce type de cas). Ce pourrait être un outil très puissant couplé avec une application de monitoring réseau.