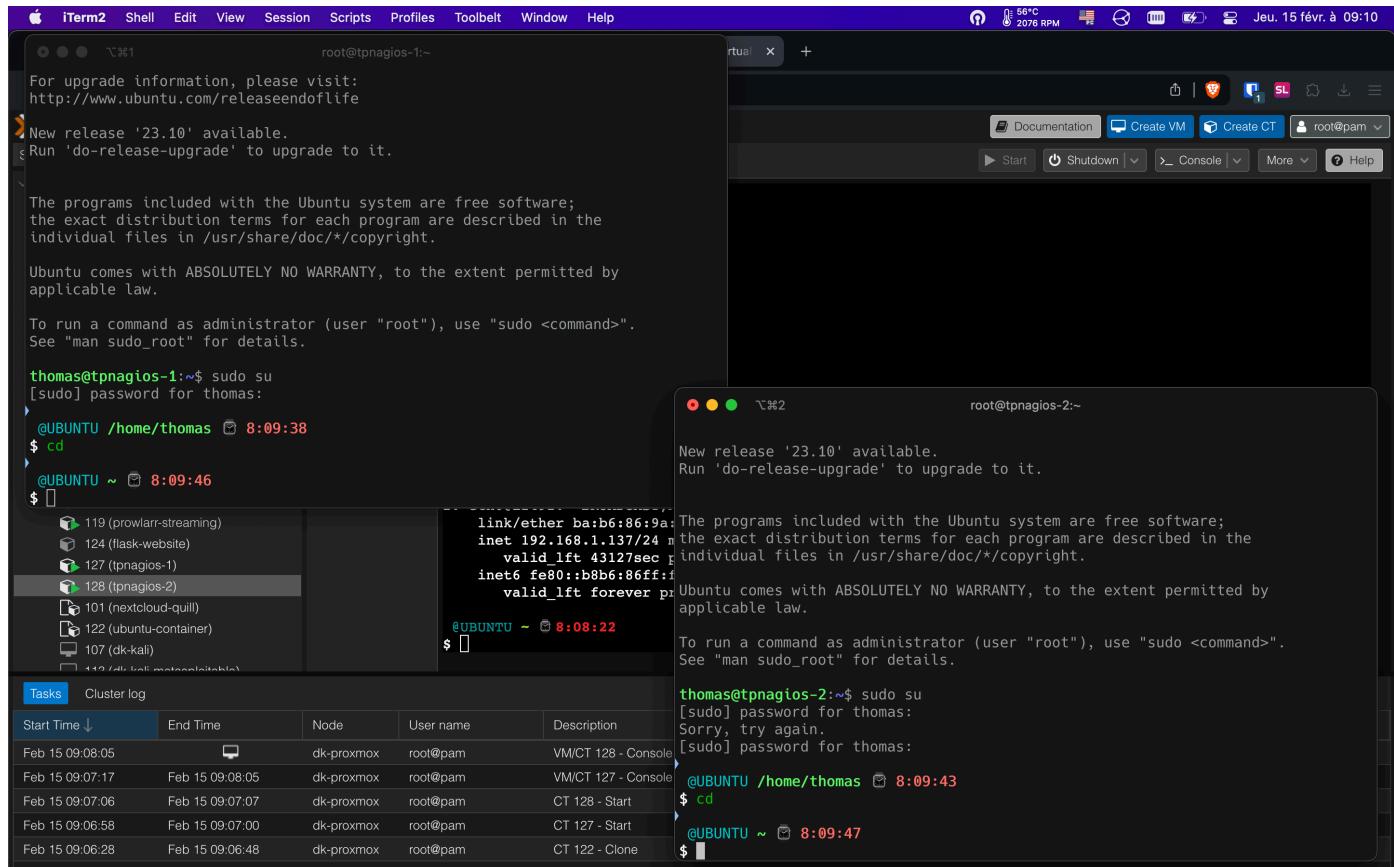


# Supervision - Rendu TP01

TP effectué par Thomas PEUGNET et David TEJEDA .

## Introduction

Préparation des VMs.



## Script d'installation

Voici le script d'installation commenté.

```
#!/bin/bash

# Check if script is run as root, exit if not
if [ ! $UID -eq 0 ]
then
echo "Script must be run as root"
exit 1
fi

# Add nagios user and nagcmd group
useradd nagios
groupadd nagcmd

# Add nagios and www-data users to nagcmd group
usermod -a -G nagcmd nagios
usermod -a -G nagcmd www-data
```

```

# Create temporary directory and navigate to it
$TMP_DIR=$(mktemp -d)
cd $TMP_DIR

# Download Nagios core software
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.1.1.tar.gz

# Extract Nagios package
tar xvzf nagios-4.1.1.tar.gz
cd nagios-4.1.1

# Configure and compile Nagios core
./configure --with-command-group=nagcmd
make all

# Install Nagios, init script, config files, and command mode
make install
make install-init
make install-config
make install-commandmode

# Install Nagios web configuration for Apache
make install-webconf

# Create admin user for Nagios web interface
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

# Reload Apache to apply changes
/etc/init.d/apache2 reload

cd $TMP_DIR

# Download Nagios plugins
wget http://www.nagiosplugins.org/download/nagios-plugins-2.1.1.tar.gz

# Extract plugins package
tar xvzf nagios-plugins-2.1.1.tar.gz
cd nagios-plugins-2.1.1

# Configure and compile Nagios
./configure --with-nagios-user=nagios --with-nagios-group=nagios
make
make install

```

## Installation de Nagios

Ayant rencontré de nombreux problèmes lors de l'installation du script, nous avons utilisé `docker` pour faire tourner notre instance.

Nous avons donc créé les différents dossiers nécessaires au fonctionnement de Nagios.

```
$ tree nagios
nagios
|-- custom-plugins
|-- etc
|-- var

3 directories, 0 files
```

Puis nous avons lancé notre image `docker` avec un ensemble de paramètres.

```
$ docker run --name nagios \
-v /root/nagios/etc:/opt/nagios/etc/ \
-v /root/nagios/var:/opt/nagios/var/ \
-v /root/nagios/custom-plugins:/opt/Custom-Nagios-Plugins \
-p 0.0.0.0:8080 \
manios/nagios:latest
```

Une fois que l'instance est lancée, nous nous rendons sur notre navigateur à `http://192.168.1.28:8080`, étant l'adresse de notre conteneur `proxmox`.

Visiblement, ça fonctionne correctement.

# Machine supervisée par défaut

La machine supervisée par défaut est `localhost`, à savoir le serveur sur lequel tourne l'instance de Nagios.

The screenshot shows the Nagios web interface at `http://192.168.1.28:8080`. The main page displays the following information:

- Host Information:** Host `localhost` (localhost), Last Updated: Thu Feb 15 09:14:46 UTC 2024, Updated every 90 seconds, Nagios Core 4.5.0 - [www.nagios.org](http://www.nagios.org).
- Host State Information:** Host Status: **UP** (for 0d 0h 0m 46s+). Status Information: PING OK - Packet loss = 0%, RTA = 0.02 ms. Performance Data: rta=0.024000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0. Current Attempt: 1/10 (HARD state). Last Check Time: 2024-02-15 09:14:01. Check Type: ACTIVE. Check Latency / Duration: 0.501 / 4.017 seconds. Next Scheduled Active Check: 2024-02-15 09:19:01. Last State Change: N/A. Last Notification: N/A (notification 0). Is This Host Flapping?: NO (0.00% state change). In Scheduled Downtime?: NO. Last Update: 2024-02-15 09:14:40 (0d 0h 0m 6s ago).
- Host Commands:** A list of actions available for the host, including Locate host on map, Disable active checks of this host, Re-schedule the next check of this host, Submit passive check result for this host, Stop accepting passive checks for this host, Stop obsessing over this host, Disable notifications for this host, Send custom host notification, Schedule downtime for this host, Schedule downtime for all services on this host, Disable notifications for all services on this host, Enable notifications for all services on this host, Schedule a check of all services on this host, Disable checks of all services on this host, Enable checks of all services on this host, Disable event handler for this host, Disable flap detection for this host, and Clear flapping state for this host.
- Host Comments:** A section where users can add comments. It includes a link to add a new comment and a link to delete all comments. The message "This host has no comments associated with it" is displayed.

The left sidebar contains navigation links for General, Home, Documentation, Current Status, Host Groups, Service Groups, Problems, Reports, and System.

Page Tour

## Ajout de la supervision d'un serveur ftp

Nous ajoutons le fichier de configuration pour monitorer notre serveur `ftp`, avec `192.168.1.137` l'adresse de notre second conteneur Proxmox.

```
root@tpnagios-1:~/nagios/etc

@UBUNTU ~/nagios/etc 9:22:56
$ ls
cgi.cfg  check_ftp.cfg  htpasswd.users  nagios.cfg  objects  resource.cfg
@UBUNTU ~/nagios/etc 9:22:57
$ cat check_ftp.cfg
define host {
    use linux-server
    host_name serveur-ftp
    address 192.168.1.137
}
@UBUNTU ~/nagios/etc 9:23:01
$
```

Après avoir déplacé le fichier dans le dossier `objects`, puis renommé en `ftp.cfg`, nous modifions le fichier de configuration `nagios.cfg` en ajoutant notre fichier de configuration.

```

19
20
21
22 # OBJECT CONFIGURATION FILE(S)
23 # These are the object configuration files in which you define hosts,
24 # host groups, contacts, contact groups, services, etc.
25 # You can split your object definitions across several config files
26 # if you wish (as shown below), or keep them all in a single config file.
27
28 # You can specify individual object config files as shown below:
29 cfg_file=/opt/nagios/etc/objects/commands.cfg
30 cfg_file=/opt/nagios/etc/objects/contacts.cfg
31 cfg_file=/opt/nagios/etc/objects/timeperiods.cfg
32 cfg_file=/opt/nagios/etc/objects/templates.cfg
33 cfg_file=/opt/nagios/etc/objects/ftp.cfg
34
35 # Definitions for monitoring the local (Linux) host
36 cfg_file=/opt/nagios/etc/objects/localhost.cfg
37
38 # Definitions for monitoring a Windows machine
39 #cfg_file=/opt/nagios/etc/objects/windows.cfg
40
nagios.cfg

```

33,30

1%

-- VISUAL LINE --

1

Après avoir relancé le service, nous obtenons le résultat suivant.

The screenshot shows the Nagios web interface at <http://192.168.1.28:8080>. The left sidebar includes links for General, Current Status, Host Groups, Service Groups, Problems, Reports, and System. The main content area displays the "Current Network Status" with last updated time and version information. It also shows "Host Status Totals" and "Service Status Totals" with counts for Ok, Warning, Unknown, Critical, and Pending states. Below this is a table titled "Host Status Details For All Host Groups" showing two hosts: "localhost" and "serveur-ftp", both marked as UP.

Nous pouvons constater que notre hôte `serveur-ftp` est bien détecté et en status `UP`.

## Attribution du service `check_ftp`

Nous modifions maintenant notre fichier `ftp.cfg` pour ajouter l'attribution du service `check_ftp`.

```
root@tpnagios-1:~/nagios/etc          @UBUNTU ~/nagios/etc  9:51:18
$ cat objects/ftp.cfg
define host {
    use linux-server
    host_name serveur-ftp
    address 192.168.1.137
}

define service {
    use local-service
    host_name serveur-ftp
    service_description FTP
    check_command check_ftp
    check_interval 1
}
>
@UBUNTU ~/nagios/etc  9:51:19
$
```

Après avoir relancé notre instance Nagios, nous constatons que le service est passé du status `pending` au status `up`.

The screenshot shows the Nagios web interface with the following details:

- Current Network Status:** Last Updated: Thu Feb 15 09:47:42 UTC 2024. Updated every 90 seconds. Nagios Core: 4.5.0 - www.nagios.org. Logged in as nageosadmin.
- Host Status Totals:** Up: 2, Down: 0, Unreachable: 0, Pending: 0. All Problems: 0, All Types: 2.
- Service Status Totals:** Ok: 6, Warning: 1, Unknown: 0, Critical: 2, Pending: 0. All Problems: 3, All Types: 9.
- Service Status Details For All Hosts:** A table listing services across various hosts. Key entries include:
 

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	2024-02-15 09:45:32	0d 0h 33m 5s	1/4	OK - load average: 0.22, 0.25, 0.27
localhost	Current Users	OK	2024-02-15 09:46:47	0d 0h 32m 27s	1/4	USERS OK - 0 users currently logged in
HTTP		WARNING	2024-02-15 09:43:02	0d 0h 28m 50s	4/4	HTTP WARNING: HTTP/1.1 401 Unauthorized - 691 bytes in 0.000 second response time
	PING	OK	2024-02-15 09:44:17	0d 0h 31m 12s	1/4	PING OK - Packet loss = 0%, RTA = 0.03 ms
	SSH	CRITICAL	2024-02-15 09:47:24	0d 0h 22m 47s	4/4	DISK OK - free space / 6958 MB (84.94% inode=100%). connect to address 127.0.0.1 and port 22: Connection refused
	Swap Usage	CRITICAL	2024-02-15 09:43:39	0d 0h 22m 8s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	OK	2024-02-15 09:46:57	0d 0h 28m 42s	1/4	PROCS OK - 15 processes with STATE = R/S/Z/D/T
serveur-ftp	FTP	OK	2024-02-15 09:47:31	0d 0h 1m 11s+	1/4	FTP OK - 0.002 second response time on 192.168.1.137 port 21 [220 ProFTPD Server (Debian) [:ffff:192.168.1.137]]

A noter que nous pouvons observer certains services en `CRITICAL`. Ceci est lié à l'utilisation d'une image docker n'ayant pas toutes les permissions ou les ports ouverts requis.

## Notifications

Création des utilisateurs et des groupes pour obtenir des notifications.

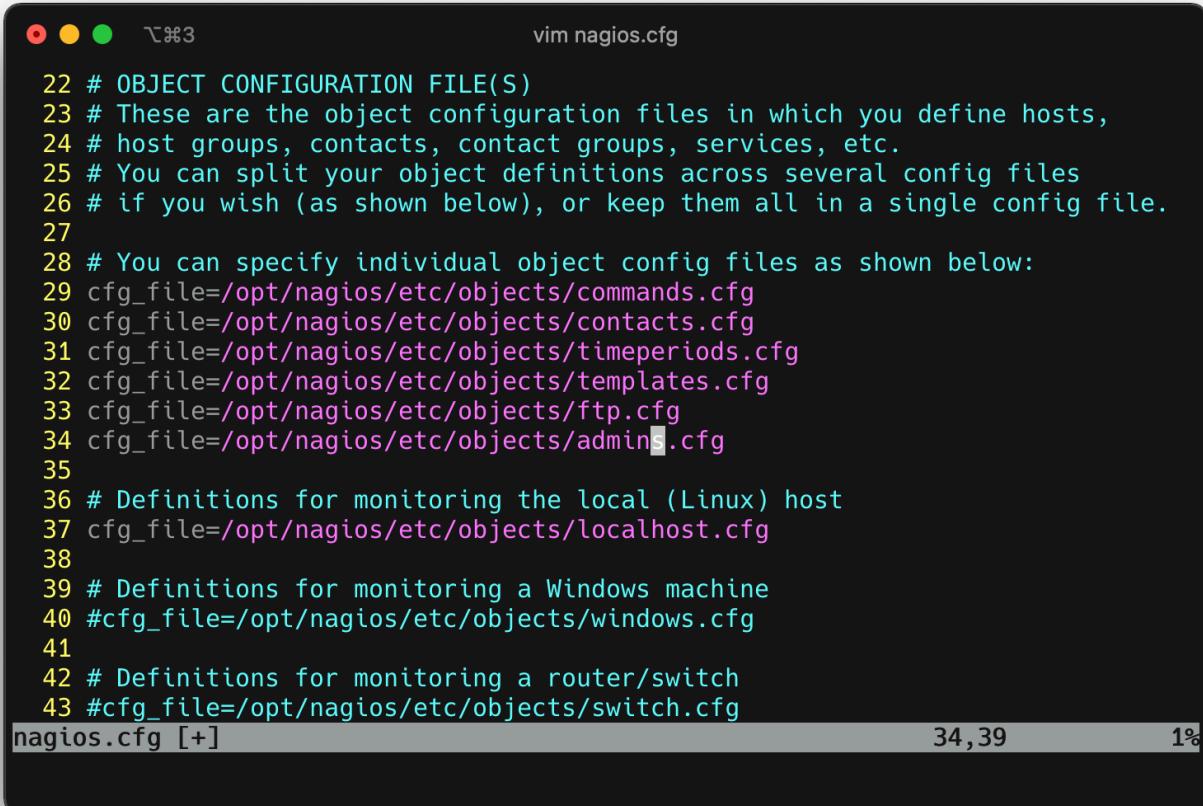
```
vim objects/admins.cfg

1 define contact {
2     contact_name thomas_peugnet
3     use generic-contact
4     email thomas.peugnet@efrei.net
5 }
6
7 define contact {
8     contact_name david_tejeda
9     use generic-contact
10    email david.tejeda@efrei.net
11 }
12
13 define contactgroup {
14     contactgroup_name admins
15     members thomas_peugnet,david_tejeda
16 }

~
~
~
~
~

objects/admins.cfg [+]          6,1           All
"objects/admins.cfg" [New]
-- INSERT --
```

On modifie maintenant notre fichier de configuration `nagios.cfg` pour intégrer le nouveau fichier `admins.cfg`



```
vim nagios.cfg

22 # OBJECT CONFIGURATION FILE(S)
23 # These are the object configuration files in which you define hosts,
24 # host groups, contacts, contact groups, services, etc.
25 # You can split your object definitions across several config files
26 # if you wish (as shown below), or keep them all in a single config file.
27
28 # You can specify individual object config files as shown below:
29 cfg_file=/opt/nagios/etc/objects/commands.cfg
30 cfg_file=/opt/nagios/etc/objects/contacts.cfg
31 cfg_file=/opt/nagios/etc/objects/timeperiods.cfg
32 cfg_file=/opt/nagios/etc/objects/templates.cfg
33 cfg_file=/opt/nagios/etc/objects/ftp.cfg
34 cfg_file=/opt/nagios/etc/objects/admins.cfg
35
36 # Definitions for monitoring the local (Linux) host
37 cfg_file=/opt/nagios/etc/objects/localhost.cfg
38
39 # Definitions for monitoring a Windows machine
40 #cfg_file=/opt/nagios/etc/objects/windows.cfg
41
42 # Definitions for monitoring a router/switch
43 #cfg_file=/opt/nagios/etc/objects/switch.cfg
nagios.cfg [+]
```

34,39      1%

## Arrêt du service proftpd

Après avoir arrêté le service `proftpd` sur le conteneur distant, nous constatons au bout de 90 secondes, que le service est passé en `CRITICAL`. Peu de temps après, nous voyons une nouvelle entrée dans la page Notifications.

**Notifications**  
Last Updated: Thu Feb 15 10:05:26 UTC 2024  
Nagios® Core™ 4.5.0 - www.nagios.org  
Logged in as nagiosadmin

**All Hosts and Services**

Latest Archive    Log File Navigation  
Thu Feb 15 00:00:00 UTC 2024 to Present..  
File: /opt/nagios/var/nagios.log

Host	Service	Type	Time	Contact	Notification Command	Information
serveur-ftp	FTP	CRITICAL	2024-02-15 10:04:21	nagiosadmin	notify-service-by-email	connect to address 192.168.1.137 and port 21: Connection refused
localhost	Swap Usage	CRITICAL	2024-02-15 09:25:34	nagiosadmin	notify-service-by-email	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.

**Reports**  
Availability Trends (Legacy)  
Alerts History Summary Histogram (Legacy)  
Notifications Event Log

**System**  
Comments Downtime Process Info Performance Info Scheduling Queue Configuration

En cliquant sur le contact, nous trouvons la page suivante, indiquant que notre fichier de configuration avec les nouveaux contacts a bien été pris en compte.

**Configuration**  
Last Updated: Thu Feb 15 10:08:58 UTC 2024  
Nagios® Core™ 4.5.0 - www.nagios.org  
Logged in as nagiosadmin

**Contacts**

Contact Name	Alias	Email Address	Pager Address/Number	Minimum Importance	Service Notification Options	Host Notification Options	Service Notification Period	Host Notification Period	Service Notification Commands	Host Notification Commands	Retention Options
david_tejeda	david_tejeda	*david.tejeda@efrei.net*		0	Unknown, Warning, Critical, Recovery, Flapping, Down, Unreachable, Unknown, Warning, Critical, Recovery, Flapping, Down, Unreachable, Recovery, Flapping, Downtime	Down, Unreachable, Recovery, Flapping, Downtime	24x7	24x7	notify-service-by-email	notify-host-by-email	Status Information, Non-Status Information
nagiosadmin	Nagios Admin	nagios@localhost		0	Unknown, Warning, Critical, Recovery, Flapping, Down, Unreachable, Recovery, Flapping, Downtime	Down, Unreachable, Recovery, Flapping, Downtime	24x7	24x7	notify-service-by-email	notify-host-by-email	Status Information, Non-Status Information
thomas_peugnet	thomas_peugnet	*thomas.peugnet@efrei.net*		0	Unknown, Warning, Critical, Recovery, Flapping, Down, Unreachable, Recovery, Flapping, Downtime	Down, Unreachable, Recovery, Flapping, Downtime	24x7	24x7	notify-service-by-email	notify-host-by-email	Status Information, Non-Status Information

**Reports**  
Availability Trends (Legacy)  
Alerts History Summary Histogram (Legacy)  
Notifications Event Log

**System**  
Comments Downtime Process Info Performance Info Scheduling Queue Configuration

Nous pouvons remarquer que, pour le moment, nous n'avons pas reçu de mail.

# Supervision Avancée

Nous créons le script custom suivant.

```
#!/bin/bash

# Check args
if [ "$#" -ne 3 ]; then
    echo "Usage: $0 <IP address> <warning threshold in ms> <critical threshold in ms>"
    exit 3
fi

IP=$1
WARNING_THRESHOLD=$2
CRITICAL_THRESHOLD=$3

# 10 pings to the host
OUTPUT=$(ping -c 10 $IP)
if [ $? -ne 0 ]; then
    echo "Ping failed, unable to reach host"
    exit 3
fi

# Regexp for getting the output
JITTER=$(echo $OUTPUT | grep -oP '\d+\.\d+/+\d+\.\d+/+\d+\.\d+/+\d+\.\d+' | awk -F'/' '{print $4}')
JITTER_ROUNDED=$(echo $JITTER | awk '{print int($1)})'

# Comparer la gigue aux seuils et définir le code de retour
if [ $JITTER_ROUNDED -le $WARNING_THRESHOLD ]; then
    echo "OK - Jitter = ${JITTER_ROUNDED} ms"
    exit 0
elif [ $JITTER_ROUNDED -le $CRITICAL_THRESHOLD ]; then
    echo "Warning - Jitter = ${JITTER_ROUNDED} ms"
    exit 1
else
    echo "Critical - Jitter = ${JITTER_ROUNDED} ms"
    exit 2
fi
```

Nous créons donc un nouveau `check_jitter.sh` dans le dossier `/opt/Custom-Nagios-Plugins/`, et y ajoutons le contenu de notre script. Nous ajoutons les permissions d'exécution avec la commande `chmod +x check_jitter.sh`.

Ensuite, nous ajoutons à notre fichier `commands.cfg` la définition de la commande `check_jitter`.

```
define command {
    command_name check_jitter
    command_line /opt/Custom-Nagios-Plugins/check_jitter.sh $HOSTADDRESS$ $ARG1$ $ARG2$
}
```

Enfin, nous créons une nouvelle assignation de service `check_jitter` à notre serveur FTP.

```
define service {
    use local-service
    host_name serveur-ftp
    service_description Jitter
    check_command check_jitter
    check_interval 1
    notifications_enabled 1
    first_notification_delay 0
    notification_interval 0
}
```

Notre fichier `ftp.cfg` est donc le suivant.

```
@UBUNTU ~/nagios/etc ⌚ 10:33:41
$ cat objects/ftp.cfg
define host {
    use linux-server
    host_name serveur-ftp
    address 192.168.1.137
}

define service {
    use local-service
    host_name serveur-ftp
    service_description FTP
    check_command check_ftp
    check_interval 1
    notifications_enabled 1
    first_notification_delay 0
    notification_interval 0
}

define service {
    use local-service
    host_name serveur-ftp
    service_description Jitter
    check_command check_jitter
    check_interval 1
    notifications_enabled 1
    first_notification_delay 0
    notification_interval 0
}

@UBUNTU ~/nagios/etc ⌚ 10:33:43
$ █
```

Nous allons vérifier que l'assignation au service fonctionne correctement depuis la WebUI.

The screenshot shows the Nagios web interface for a service named "serveur-ftp".

**Service Information:**

- Last Updated: Thu Feb 15 10:33:59 UTC 2024
- Updated every 90 seconds
- Nagios Core™ 4.5.0 - www.nagios.org
- Logged in as nageosadmin

**Service Jitter:**

- On Host: serveur-ftp (serveur-ftp)
- Member of: No servicegroups.

**Current Status:**

- View Information For This Host
- View Status Detail For This Host
- View Alert History For This Service
- View Trends For This Service
- View Alert Histogram For This Service
- View Availability Report For This Service
- View Notifications For This Service

**Service State Information:**

Current Status:	OK (for 0d 0h 1m 9s)
Status Information:	Ping OK - 12ms
Performance Data:	
Current Attempt:	4/4 (HARD state)
Last Check Time:	2024-02-15 10:33:50
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.004 seconds
Next Scheduled Check:	2024-02-15 10:34:50
Last State Change:	2024-02-15 10:32:50
Last Notification:	2024-02-15 10:32:50 (notification 2)
Is This Service Flapping?	NO (11.84% state change)
In Scheduled Downtime?	NO
Last Update:	2024-02-15 10:33:51 (0d 0h 0m 8s ago)

**Service Commands:**

- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Stop obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Send custom service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service
- Clear flapping state for this service

**Service Comments:**

Add a new comment | Delete all comments

Entry Time Author Comment Comment ID Persistent Type Expires Actions

This service has no comments associated with it

Visiblement, le ping fonctionne correctement. En éteignant le conteneur du serveur FTP, nous obtenons le résultat suivant.

The screenshot shows the Nagios web interface for the same service "serveur-ftp".

**Service Information:**

- Last Updated: Thu Feb 15 10:37:15 UTC 2024
- Updated every 90 seconds
- Nagios Core™ 4.5.0 - www.nagios.org
- Logged in as nageosadmin

**Service Jitter:**

- On Host: serveur-ftp (serveur-ftp)
- Member of: No servicegroups.

**Current Status:**

- View Information For This Host
- View Status Detail For This Host
- View Alert History For This Service
- View Trends For This Service
- View Alert Histogram For This Service
- View Availability Report For This Service
- View Notifications For This Service

**Service State Information:**

Current Status:	UNKNOWN (for 0d 0h 4m 25s)
Status Information:	Ping failed, unable to reach host
Performance Data:	
Current Attempt:	4/4 (HARD state)
Last Check Time:	2024-02-15 10:36:50
Check Type:	ACTIVE
Check Latency / Duration:	0.001 / 0.003 seconds
Next Scheduled Check:	2024-02-15 10:37:50
Last State Change:	2024-02-15 10:32:50
Last Notification:	2024-02-15 10:32:50 (notification 2)
Is This Service Flapping?	NO (11.05% state change)
In Scheduled Downtime?	NO
Last Update:	2024-02-15 10:37:11 (0d 0h 0m 4s ago)

**Service Commands:**

- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Stop obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Send custom service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service
- Clear flapping state for this service

**Service Comments:**

Add a new comment | Delete all comments

Entry Time Author Comment Comment ID Persistent Type Expires Actions

This service has no comments associated with it