

# HowTo install JFFNMS on Debian GNU Linux 3.1 (Sarge)

## **Goal of this document**

This document describes the steps to achieve the installation of JFFNMS on Debian GNU Linux 3.1 (aka Sarge).

## Changelog

Release	Date	Author	Object
1.0	02.15.2005	DLI	Document creation
1.1	04.18.2005	DLI	Missing stuff
1.2	12.12.2005	DLI	Various Fix, SnmpTrapd

# Table of contents

<b>1 GENERAL CONSIDERATIONS.....</b>	<b>3</b>
<b>2 INSTALLATION OF SARGE.....</b>	<b>4</b>
<b>3 DEPENDENTS PACKAGES FROM SARGE.....</b>	<b>5</b>
<b>4 SPECIFICS PACKAGES .....</b>	<b>6</b>
4.1 JFFNMS.....	6
4.2 TACACS.....	6
<b>5 CONFIGURATION.....</b>	<b>8</b>
5.1 MySQL.....	8
5.2 SYSLOG-NG.....	8
5.3 SNMP.....	9
5.3.1 <i>SNMPD</i> .....	9
5.3.2 <i>SNMPTRAPD</i> .....	9
5.3.3 <i>TESTS</i> .....	10
5.4 APACHE.....	10
5.5 PHP4.....	11
5.6 JFFNMS.....	11
5.7 TFTP.....	12
<b>6 TESTS.....</b>	<b>13</b>
<b>7 OPTIONAL INTEGRATION.....</b>	<b>14</b>

# 1 General considerations

---

The hardware requirements for JFFNMS are linked to the size of the network you want to manage. See this post on the JFFNMS list <http://marc.theaimsgroup.com/?l=jffnms-users&m=113081997606063&w=2> to have an idea about hardware requirement vs size of network .

CPU speed is not very important, you only have to be careful with the amount of memory and the hard drive performances, especially if the database logs lots of events from syslog or SNMP traps. In this case it is suitable to move the database to another box to limit I/O bottlenecks issues.

This guide is written and tested on Debian GNU Linux stable ( 3.1 aka Sarge) with JFFNMS package version 0.8.2.

## 2 Installation of SARGE

---

Install the Debian GNU Linux Sarge using any available source and/or method (cd, dvd, boot-floppies, Knoppix etc ...), you can find help on Debian web site (<http://www.debian.org>) or can read the excellent Debian reference guide (<http://qref.sourceforge.net/>) if you are not very familiar with Debian.

You can skip package configuration in the install process. For friendly use you can set up an X Server but it is not necessary because you can manage/configure JFFNMS with a web browser and a SSH client. Be sure to have enough disk space to store the database for performance statistics (RRD): "one year of 5 minutes interval statistics" is about 1MB.

### 3 Dependents packages from SARGE

---

JFFNMS is not yet packed for Debian Sarge release, only for etch (aka testing: <http://packages.debian.org/testing/web/jffnms>). To run JFFNMS you need to install several other softwares that comes with Debian, use your favorite package manager to download them.

```
# apt-get install apache fping nmap mysql-server php4-pear php4-gd2 php4-  
snmp php4-cgi php4-cli php4-odbc mysql-client php4-mysql rrdtool syslog-  
ng snmpd snmp graphviz libpng2 libgd2 tmpreaper tftpd ntp nmap
```

**Note:** if you want to download graphviz from apt (not 100% compatible with Debian GNU policy) you have to include the "non-free" to your apt configuration file..

```
deb ftp://ftp.nerim.net/debian/ sarge main non-free contrib  
deb-src ftp://ftp.nerim.net/debian/ sarge main non-free contrib  
deb http://security.debian.org/ sarge/updates main non-free contrib.
```

## 4 Specifics packages

---

### 4.1 JFFNMS

---

Download the latest stable release of JFFNMS from the official site (<http://www.jffnms.org>) and unpack it to a temporary folder.

```
# tar xfvz jffnms-0.8.xxx.tar.gz
# mv jffnms-0.8.xxx /opt/jffnms
```

Create a JFFNMS group for cron jobs and add it to Apache group

```
# groupadd jffnms
# useradd -g jffnms -d /opt/jffnms -c 'JFFNMS User' jffnms
# usermod -G jffnms www-data
# chown -R jffnms.jffnms /opt/jffnms/
```

Grant read/write permission on jffnms directory

```
# chmod 770 /opt/jffnms
# chmod -R ug+rw /opt/jffnms
```

You also have to set-uid the nmap binary if you want UDP port monitoring & discovery to work

```
# chmod +s /usr/bin/nmap
# chmod a+x /usr/bin/nmap
```

### 4.2 TACACS

---

Debian Tacplus package is already installed if you ran my apt-get command-line, but you have to modify some config and compilation options. Copy /opt/jffnms/doc/tac\_plus.conf to /etc/tac\_plus/tac\_plus.conf, remove the first line and recompile the sources.

```
# tar xfvz tac-plus-jffnms.tar.gz
# cd tac-plus
# make clean
# ./configure --with-db --with-mysql --prefix=/usr
```

If something fails, go to "/usr/include/mysql/mysql.h" and change the lines 249 and 250: "DB" becomes "db". Compile / install the package and start the process

```
# make tac_plus  
# make install  
# kill `pidof tac-plus`  
# /etc/init.d/tac_plus start
```

## 5 Configuration

---

### 5.1 MySQL

---

Setup the root password for MySQL and manually create the database "jffnms". Set the permissions and then import the schema and data.

```
# mysqladmin password xxxxxx
# mysql -u root mysql -p
# mysql> CREATE DATABASE jffnms;
# mysql> GRANT ALL PRIVILEGES ON jffnms.* TO jffnms@localhost
IDENTIFIED BY 'jffnms';
# mysql> FLUSH PRIVILEGES;
# mysql> quit
# mysql -u jffnms -pjffnms jffnms < /opt/jffnms/docs/jffnms-
0.8.xxx.mysql
```

### 5.2 SYSLOG-NG

---

Syslog-ng default configuration file has to be changed to insert Syslog messages into mysql. For this, we use a fifo for storing events, then we pass them to mysqld.

```
# mkfifo /opt/jffnms/mysql.pipe
```

```
## Accept Syslog and Kernel messages not only on localhost
source s_all { internal(); unix-stream("/dev/log"); file("/proc/kmsg"
log_prefix("kernel: ")); udp(); };

## Define the mysql pipe (change mysql access according to mysql jffnms
user)
destination jffnms_processing { program ("mysql -u jffnms -pjffnms jffnms <
/opt/jffnms/mysql.pipe"); };

destination d_jffnms { pipe ("/opt/jffnms/mysql.pipe" template("INSERT
INTO syslog (date, date_logged, host, message) VALUES ('$YEAR-$MONTH-$DAY
$HOUR:$MIN:$SEC', NOW\(\), '$FULLHOST', '$MSG');\n")
template-escape(yes)); };

## Optionally create some filters
filter f_jffnms { filter(f_jff_in) and not filter(f_jff_out); };
filter f_jff_in { level(warn..emerg); };
filter f_jff_out { ( program(sshd) and match("Did not receive") ) or
( program(snmpd) and match("line in /proc/stat") ) or
( program("syslog-ng") and match("STATS: dropped") ); };

## Finally add the log condition
log { source(s_all); filter(f_jffnms); destination(d_jffnms); };
```

Apply your settings by restarting Syslog-ng daemon

```
# /etc/init.d/syslog-ng reload
```

**Notes:**

- *If you type reload instead of restart you will not see your typos mistake*
- *disable Syslog-ng "xconsole" destination and log statements if you don't run an X server (without disabling, Syslog-ng will report some dropped STATS).*
- *notice that only events from warning to emerg severity are forwarded to JFFNMS database*
- *you can add a debug log file to see what syslog-ng send to JFFNMS Mysql database, just add*

```
destination df_jffdbin { file("/var/log/jffnms/db_in.log"); };  
log { source (s_all);  
filter (f_jffnms);  
destination (d_jffnms);  
destination (df_jffdbin);  
};  
  
.
```

## 5.3 SNMP

---

The snmp daemon has two modules: the snmp daemon who responds to snmp request on port udp:161 and the snmptrap daemon who intercept trap on port udp:162. You can individually control whether or not snmpd and snmptrapd are started as daemon by editing the "/etc/default/snmpd" file.

### 5.3.1 SNMPD

Configure your snmpd via snmpconf: "man snmpconf" for more details. For basic setup run this command and configure at least snmp read-only access for the nms himself.

```
# snmpconf -g basic_setup  
# mv snmpd.conf /etc/snmp/
```

### 5.3.2 SNMPTRAPD

If you want to be able to collect snmp traps, it is necessary to pass data to the trap collector.

```
# /etc/snmp/snmptrapd.conf  
traphandle default /opt/jffnms/engine/trap_receiver.sh
```

You need to re-open your snmpd configuration file and add « master agentx » to be able to receive traps, then reload the snmpd daemon.

Note: default after “traphandle” instruction tells snmptrapd to pass every trap (OID) to JFFNMS. If you want to disable specific OID to be stored into Mysql, simply add one more traphandle line, followed by the OID and redirect it on /dev/null or /bin/true

### 5.3.3 TESTS

First, you have to check if your snmp agent is running fine. This command will check R/O access the the host mib branch.

```
# snmpget -v1 -c <YOUR RO COMMUNITY> localhost system.sysName.0
system.sysName.0 = nms-dev
```

This command has to output the name of your box.

Second, you have to check that snmp traps are collected and then stored into the mysql table of JFFNMS. Check your syslog log file to see if the trap occurs, you can also test this when you finish the setup of JFFNMS, if everything is good you should see a message from your NMS in the “events” screen.

```
# snmptrap -v 1 -c public localhost "" "" 0 0 ""
# tail /var/log/messages | grep snmptrapd
nms-dev snmptrapd[5961]: 172.16.3.19: Cold Start Trap (0) ...
```

## 5.4 APACHE

---

Verify that the php4 module is launched by Apache (/etc/apache/modules.conf):

```
LoadModule php4_module /usr/lib/apache/1.3/libphp4.so
```

Configure Apache to serve JFFNMS pages under /opt/jffnms/htdocs (by symlink or virtual host)

```
# ln -s /opt/jffnms/htdocs /var/www/jffnms
```

## 5.5 PHP4

---

Add those lines (only for the ones that need) in your php.ini files and reload apache configuration

```
In /etc/php4/apache/php.ini
extension=gd.so
extension=mysql.so
extension=snmp.so
extension=odbc.so

In /etc/php4/cgi/php.ini
extension=mysql.so
extension=snmp.so
extension=odbc.so

In /etc/php4/cli/php.ini
extension=mysql.so
extension=gd.so
extension=snmp.so
extension=odbc.so
```

Verify these options on your Apache's php.ini (/etc/php4/apache/)  
register\_globals = On  
allow\_url\_fopen = On  
error\_reporting = E\_ALL & ~E\_NOTICE

Reload the process if necessary

```
# apachectl graceful
```

Check your apache logs to see if errors occur and verify that the php modules that you added before to your php.ini are loaded with "php -m" command.

## 5.6 JFFNMS

---

Create the crontab entries for the backend jobs of JFFNMS. Change the settings according to your needs and reload crond.

```
# crontab -u jffnms /opt/jffnms/docs/unix/crontab
# crontab -u jffnms -e
# /etc/init.d/cron reload
```

Debian does not have the tmpwatch package, it uses tmpreaper instead. Remove the tmpwatch line from the crontab and change “/etc/tmpreaper.conf” to delete temporary files in “/opt/jffnms/htdocs/images/temp”.

I recommend you to change the default path for logs (optional) and use logrotate .

```
# mkdir /var/log/jffnms
In /etc/logrotate.d/jffnms
/var/log/jffnms/* {
    daily
    rotate 7
    missingok
    notifempty
    compress
    nocreate
}
```

## 5.7 TFTP

---

The TFTP module of JFFNMS can backup Cisco devices configuration with a cron job, go to Cisco website for more information about settings (need read-write access to the device’s MIB).

/etc/inetd.conf

```
tftp dgram udp wait root /usr/sbin/tcpd /usr/sbin/in.tftpd
--tftpd-timeout 300 --retry-timeout 5 --no-multicast --verbose=5 --
logfile /var/log/tftpd.log /opt/jffnms/tftpd/
```

If you have another package for the tftp daemon, read the documentation for the settings. Don’t forget to fill the tftp field for each device in the host config interface of the GUI. You can also test the config by running a “running to tftp” copy from your Cisco device.

## 6 Tests

---

Finally open a browser and go to <http://yourhost/jfnms/>, fill each field with appropriate values and check if everything is ok (green). Don't forget to tick the last field when you finish the initial setup to protect configuration access.

After logging in with the default user and password (admin:admin), you will see the startup page of JFNMS is everything is good.

For more information about configuration, please read the official documentation pages, if you carefully read this guide, the doc but still have problems, drop a line to the list.

## 7 Optional integration

If you want to forward Windows event logs into JFFNMS you will need to run a little daemon on the windows box, to forward event logs the Syslog-ng server.

The daemon that I use is called ntsyslog, this is the only one (coupled with Syslog-ng) for me that can deals with special char sets.

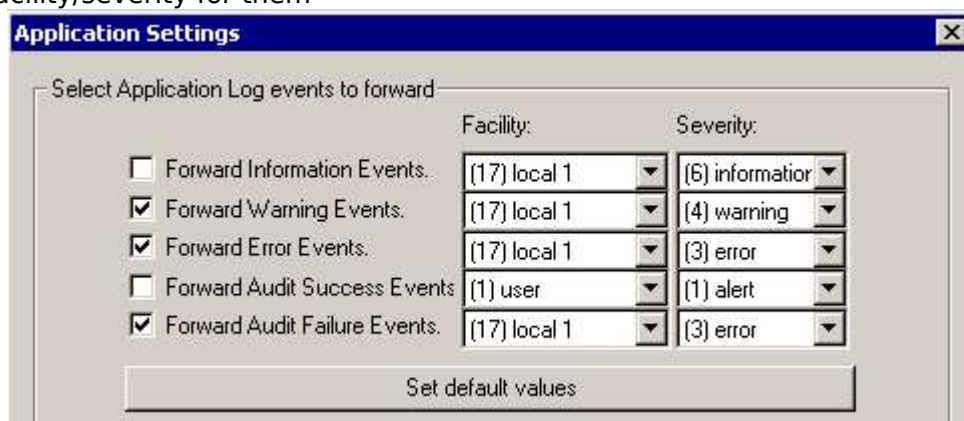
Download it on sf.net site <http://sourceforge.net/projects/ntsyslog/> and configure it to send messages to the JFFNMS host (with ntsyslogctrl.exe).

Here are some setup screenshots of NTSYLOG:

- Setup the name/ip of JFFNMS host



- Select the eventlog sources that you want to forward and choose the facility/severity for them



Apply settings by reloading ntsyslog daemon