Net/FSE Installation Guide

v1.0.1, 1/21/2008

About This Guide

This guide walks you through the installation of Net/FSE, the network forensic search engine. All support questions not answered in this guide should be posted to our User Community at http://www.packetanalytics.com/community or sent via email to *support@packetanalytics.com*.

Completing this guide will result in a fully functional Net/FSE server and web interface. Refer to the Administrator's guide (admin.pdf in the docs folder) for information on configuring sensors. Net/FSE does not automatically collect information from the network so after completing this guide you will need to start syslogging data to Net/FSE and (re)direct your NetFlow data streams to the Net/FSE server.

Hardware Requirements

Net/FSE is designed to run on commodity server hardware but as is always the case, the better the hardware, the better the system will run. A fast CPU, lots of RAM and large disk arrays help make Net/FSE run faster and store more data but even a modest Linux-based server will work very nicely.

Minimum hardware requirements:

- Pentium 4 2 Ghz or better
- 1 GB RAM
- 100 GB available storage, divided in two partitions: /var for PostgreSQL, /data for the remainder

Preferred hardware requirements:

- Dual Xeon 3 Ghz or better
- 2 GB RAM
- 1 TB available storage, divided into two partitions as above

---

Supported OSs

Net/FSE will in principal run on any POSIX compliant UNIX system with a Java 5 or higher runtime environment. The software has been developed on Mac OS X and deployed for over five years on Red Hat and Debian systems of various types. We have also had success with Ubuntu but as the basic Ubuntu distributions do not come with tools like make and gcc, the installation on these systems is more challenging.

Officially the following OSs are supported:

- Debian 4+
- Ubuntu Server 6+
- RedHat Enterprise Linux 3+
- Fedora 6+
- Gentoo 2007.0+
- Max OS X 10.4+

Getting Started

To get started on installing Net/FSE you will need to download the software distribution from Packet Analytics. Follow these steps to get Net/FSE:

1. Navigate your web browser to `http://www.packetanalytics.com/download.php`
2. Click the download button to start downloading the software
3. Copy the download package (`netfse1.0.tgz`) to the server you will use to run Net/FSE
4. From the directory containing the software package execute the following command: `tar -xzf netfse1.0.tgz`
5. You should now see the download directory, `netfse1.0`
6. If you are using Debian or Ubuntu run the following command:

```
apt-get install gcc g++ make bison flex
```

Installing PostgreSQL

PostgreSQL is used for a variety of tasks within Net/FSE. It can be built from source or installed using a package manager like yum or apt. Version 8.0 or higher is required for Net/FSE. If you plan to build from source you will need a variety of software tools (gcc, make, libtool among others) that may or may not be installed by default on your Linux system. The PostgreSQL documentation will walk you through the build process but installing a binary distribution of PostgreSQL is advised.

Install on RedHat/Fedora using RPM:

1. Navigate your web browser to http://www.postgresql.org/ftp/binary/v8.2.5/linux/rpms/
2. Find and download the RPM that is appropriate for your OS version
3. Install the RPM as root: `rpm -i rmp_name.rpm`
4. `service postgresql initdb`
5. `/etc/init.d/postgresql start`

Install on RedHat/Fedora using yum:

```
1. yum install postgresql postgresql-server
2. service postgresql initdb
3. /etc/init.d/postgresql start
```

Install on Debian/Ubuntu:

```
1. apt-get update
2. apt-get install postgresql-8.2
```

- As of the writing of this document, postgresql-8.2 was available. Depending on your build there may be an newer or earlier version available. If the above command does not work, try searching for "postgresql" using `dselect` to determine the correct package name.
- **Note:** your Ubuntu distribution may or may not have the proper sources to install PostgreSQL. Please check the user community for answers or contact *support@packetanalytics.com* if you are having trouble.

Building from source on the server:

1. Download the latest source distribution: http://www.postgresql.org/ftp/source/v8.2.5/postgresql-8.2.5.tar.gz
2. `tar -xzf postgresql-8.2.5.tar.gz ; cd postgresql-8.2.5`
3. Follow the instructions as per the INSTALL file
   - Note: your OS may or may not have the libraries and build tools necessary. Try a binary distribution is you have troubles.

Configuring PostgreSQL

Select a data directory for PostgreSQL that has a reasonable amount of storage (most installations use `/var` by default). Refer to the PostgreSQL documentation for information on how to set the data directory. How much storage is necessary will depend greatly on the amount of data being processed by Net/FSE. The recommended configuration is to determine how much storage can be allocated to Net/FSE and then configure your partitions or directory structures such that PostgreSQL's data directory has access to half of the allocated storage.

Most default PostgreSQL installations will be properly configured to run Net/FSE. RedHat and Fedora installations do not normally come configured correctly. If installing on RedHat or Fedora, edit the `pg_hba.conf` file by changing from `ident` to `trust` for the authentication method for the uncommented entries at the end of the file. Restart the PostgreSQL server after saving the file (`/etc/init.d/postgresql restart`).

PostgreSQL installations typically create a new system user named `postgres`. The install process also creates a default database user named `postgres`. To use Net/FSE you must either use the default `postgres` user or create a new user with the ability to create databases and tables from a database called metadata. In either case the user must

have a set password that Net/FSE can use to connect to the database server. The steps that follow walk you through basic configuration using the default `postgres` user.

Configuration Steps

1. Start the PostgreSQL database server (see PostgreSQL documentation)
2. `su postgres`
3. `createdb metadata`
4. `psql metadata`
5. `alter user postgres password 'new_password'`

Installing nfdump (Optional)

Net/FSE can function as a NetFlow collector by using `nfdump` to collect NetFlow data streams. The `nfdump-1.5.6` source distribution is found in the Net/FSE download directory in contrib. Like building PostgreSQL you will need a variety of software tools (gcc, make, flex, bison among others) installed. If you built PostgreSQL from source then this step should be easy. Follow the steps below to install `nfdump` from the Net/FSE download directory:

1. `su root` or `sudo su` (if not root already)
2. `cd contrib/nfdump-1.5.6`
3. `./configure`
4. `make`
5. `make install`

Configuring Syslog

In addition to collecting NetFlow data using `nfdump`, Net/FSE can receive data via `syslog`. Installation of `syslog-ng` is recommended but is not mandatory as all Linux distributions have `syslog` installed by default. Refer to the `syslog` or `syslog-ng` documentation for installation and configuration instructions.

Key Configuration Notes:

1. Be sure that your firewall is not blocking incoming `syslog` messages. The default port is usually UDP port 514.
2. Configure the `syslog` server to accept messages from remote hosts
3. Configure the `syslog` server timestamp format to be "Mmm, DD HH:MM:SS". Example: Jan 3 11:56:56

Installing Net/FSE

Installation of Net/FSE is performed by executing the `setup.sh` script found in the Net/FSE download directory. From the Net/FSE download directory follow these instructions:

1. `su root` or `sudo su`
2. Run the setup script passing the PostgreSQL user and password as the only parameters: `sh setup.sh psql_user psql_password`
3. The end user license agreement (EULA) will be presented. Enter YES to agree or NO to decline and stop installation. The EULA can also be found in the Net/FSE download folder (`agreement.txt`).
4. After accepting the license, the installer will attempt to connect to the PostgreSQL server and create that database structures needed by Net/FSE. The installer will exit if it cannot connect to the server. If you have troubles:
   - Check that the user and password given to the setup script are correct
   - Check to see that the server is running (`ps -awx | grep postmaster`) and that is configured to accept connections from `localhost` and `127.0.0.1` (the loopback interface).
   - Revisit the Installing PostgreSQL and Configuring PostgreSQL sections above.
   - Visit our User Community on the Packet Analytics website.
   - If all else fails, contact us at *support@packetanalytics.com* for assistance.
5. Next, the installer will prompt you for the location of the data directory. This should be an empty directory on a large disk partition. The more disk given to this partition, the longer Net/FSE will be able to store data. The default is `/data`.
6. The installer will finish by generating configuration files and copying the software to `/usr/local/nfse/`.

Data Support

Net/FSE natively supports NetFlow version 5 records via UDP (if `nfdump` is installed, see above) and free-form `syslog`. Free-form `syslog` data must contain an IP address represented as a dot quad (e.g. 1.2.3.4), which will be used as the source IP of the record. The first IP address found will be used as the source IP address.

Although using the free-form `syslog` data type is useful, Net/FSE's true strength comes from its ability to perform per-data type analytics on data streams. Net/FSE's architecture allows for highly customizable data type integration. Contact Packet Analytics at *support@packetanalytics.com* for more information on how additional data types can be integrated into Net/FSE.

The administrator's guide found in the Net/FSE download's `docs` folder (`admin.pdf`) describes how to configure sensors, `syslog` data streams and NetFlow data streams. Please refer to this document for additional information on Net/FSE data type support.