Wikiprint Book

Title: Installation instructions

Subject: ThirdEye - installation

Version: 31

Date: 09/15/14 11:43:08

Table of Contents

Installation instructions

Framework installation

Assume the installation directory to be **$HOME** (your home directory).

1. Make sure all dependencies are installed.
1. Download the desired version of **saf-vxxx.tar.gz**.
   Uncompressing the downloaded file will create a directory **SAF**.

```
 $ tar -xvzf saf-vxxx.tar.gz
$ cd $HOME/SAF
```

   Read more about the directory layout.

   Set the executable bit on the main executable **./saf.py**.

```
 $ chmod +x saf.py
```

   Typing **./saf.py** on the command line should produce help output as shown below without any errors.

```
 ##############################################
#    Semantic Analysis Framework - v0.1a    #
##############################################


./saf.py --db <dbname>  --model  <name> [optional args]

Optional Arguments
==================
       [--knowbase <knowledgebase dir> (default: ./knowbase)]
       [--inmem ]
       [--profile]
       [--pretty]
       [--nofail]
       [--verbose {debug|state|info|critical|error|state|fine|behavior}]

Description
===========
--inmem     Creates the temp database in memory
--showmdata Prints statistics about the events in the database
--pretty    Prints Pretty Tabular Output
--nofail    Dont show failures
--time      Print timing info for performance
--stats     Show statistics of input data
```

   Refer framework command line options to understand framework usage.

1. Finally, test the installation and working of SAF by running a few basic tests. There should be no failures reported

```
$ python runtests.py --s --data tests/sampledata/
```

Compiling and installing the p2db tool for normalizing packet data

Make sure all p2db dependencies are installed.

```
$ cd /path/to/SAF
$ cd plugins/p2db
$ make
$ make install
```

Test the installation by executing **p2db** and confirming that the usage is shown without errors.

```
$ p2db
Usage: p2db filename (outdb|"stats")

Options:
   filename    PCAP File to process.
   outdb       Sqlite database file for output.
   stats       Just display event stats.
```

Refer p2db command line options to understand tool usage.