

Data Analysis and Visualization Linux®

Release 2014

User Guide

**Author:**

Raffael Marty, [raffy@secviz.org](mailto:raffy@secviz.org)

Amanda Gellhouse, [amanda@gellhou.se](mailto:amanda@gellhou.se)

**Last Updated:**

May 11, 2014

Table of Contents

[Introduction 3](#_Toc387584095)

[Tools 4](#_Toc387584096)

[DAVIX Setup Guide 6](#_Toc387584097)

[Environment Requirements 6](#_Toc387584098)

[Installation 6](#_Toc387584099)

[DAVIX Use 7](#_Toc387584100)

[What the Installer Does 7](#_Toc387584101)

# Introduction

Need help understanding gigabytes of logs? Your OS performance metrics do not make sense? You want to analyze your SAP user permissions? Then DAVIX, the toolset for visualizing IT data, is your answer!

DAVIX – the Data Analysis & Visualization Linux® – brings the most important free tools for data processing and visualization to your desk. There is no hassle with installing an operating system or struggle to build the necessary tools to get started with visualization. You can completely dedicate your time to data analysis.

# Tools

DAVIX 2014 includes the following tools; user guides for each tool are maintained on the DAVIX Wiki at <https://github.com/secviz/davix/wiki>

| **Tool** | **Capture** | **Process** | **Visualize** | **Version** | **User Guide** |
| --- | --- | --- | --- | --- | --- |
| Afterglow |  |  |  | 1.6.4 | [User Guide: Afterglow](https://github.com/secviz/davix/wiki/User-Guide:-Afterglow) |
| Argus |  |  |  | 3.0.6.1 - server; 3.0.6.2 - client | [User Guide: Argus](https://github.com/secviz/davix/wiki/User-Guide:-Argus) |
| BroIDS |  |  |  | 2.2 | [User Guide: BroIDS](https://github.com/secviz/davix/wiki/User-Guide:-BroIDS) |
| Chaosreader |  |  |  | 0.94-4 | [User Guide: Chaosreader](https://github.com/secviz/davix/wiki/User-Guide:-Chaosreader) |
| ChartDirector |  |  |  | 5.1.1 | Not available. |
| Cytoscape |  |  |  | 3.0.2 | [User Guide: Cytoscape](https://github.com/secviz/davix/wiki/User-Guide:-Cytoscape) |
| dns-browse |  |  |  | 1.9-7 | [User Guide: dns-browse](https://github.com/secviz/davix/wiki/User-Guide:-dns-browse) |
| dnstop |  |  |  | 20120611-2 | [User Guide: dnstop](https://github.com/secviz/davix/wiki/User-Guide:-dnstop) |
| EtherApe |  |  |  | 0.9.12-1 | [User Guide: EtherApe](https://github.com/secviz/davix/wiki/User-Guide:-EtherApe) |
| EventLog |  |  |  | 0.2.4 | Not available. |
| FlowTag |  |  |  | 2.0.5 | [User Guide: FlowTag](https://github.com/secviz/davix/wiki/User-Guide:-FlowTag) |
| GeoIP |  |  |  | 20130813-1 | Not available. |
| Gephi |  |  |  | 0.8.2-beta | Not available. |
| GGobi |  |  |  | 2.1.10-4 | [User Guide: GGobi](https://github.com/secviz/davix/wiki/User-Guide:-GGobi) |
| glTail |  |  |  | 0.1.8 | [User Guide: glTail](https://github.com/secviz/davix/wiki/User-Guide:-glTail) |
| GNUplot |  |  |  | 4.6.3-2 | [User Guide: GNUplot](https://github.com/secviz/davix/wiki/User-Guide:-GNUplot) |
| Google Earth |  |  |  | 1.0.0 | [User Guide: Google Earth](https://github.com/secviz/davix/wiki/User-Guide:-Google%20Earth) |
| Graphviz |  |  |  | 2.26.3-15 | [User Guide: Graphviz](https://github.com/secviz/davix/wiki/User-Guide:-Graphviz) |
| GUESS |  |  |  | 1.0.3-beta | [User Guide: GUESS](https://github.com/secviz/davix/wiki/User-Guide:-GUESS) |
| INAV |  |  |  | 0.3.7 - server; | Not available. |
| InetVis |  |  |  | 0.9.3.1 | [User Guide: InetVis](https://github.com/secviz/davix/wiki/User-Guide:-InetVis) |
| LogStash |  |  |  | 1.4 | Not available. |
| Mondrian |  |  |  | 1.2 | [User Guide: Mondrian](https://github.com/secviz/davix/wiki/User-Guide:-Mondrian) |
| MRTG |  |  |  | 2.17.4-2 | [User Guide: MRTG](https://github.com/secviz/davix/wiki/User-Guide:-MRTG) |
| NetGrok |  |  |  | 20080928 | Not available. |
| netsed |  |  |  | 1.1-1 | [User Guide: netsed](https://github.com/secviz/davix/wiki/User-Guide:-netsed) |
| nfdump |  |  |  | 1.6.8p1-1 | [User Guide: nfdump](https://github.com/secviz/davix/wiki/User-Guide:-nfdump) |
| ngrep |  |  |  | 1.45.ds2-12 | [User Guide: ngrep](https://github.com/secviz/davix/wiki/User-Guide:-ngrep) |
| nmap |  |  |  | 6.40-0.1 | [User Guide: nmap](https://github.com/secviz/davix/wiki/User-Guide:-nmap) |
| nsm-console |  |  |  | 0.7 | [User Guide: nsm-console](https://github.com/secviz/davix/wiki/User-Guide:-nsm-console) |
| Octave |  |  |  | 3.6.4-3 | [User Guide: Octave](https://github.com/secviz/davix/wiki/User-Guide:-Octave) |
| p0f |  |  |  | 2.0.8-2 | [User Guide: p0f](https://github.com/secviz/davix/wiki/User-Guide:-p0f) |
| PADS |  |  |  | 1.2-11 | [User Guide: PADS](https://github.com/secviz/davix/wiki/User-Guide:-PADS) |
| Parvis |  |  |  | 0.3.1 | [User Guide: Parvis](https://github.com/secviz/davix/wiki/User-Guide:-Parvis) |
| PicViz |  |  |  | 0.5-1 | Not available. |
| Ploticus |  |  |  | 2.41-5 | [User Guide: Ploticus](https://github.com/secviz/davix/wiki/User-Guide:-Ploticus) |
| PRADS |  |  |  | 0.3.0-1 | [User Guide: PRADS](https://github.com/secviz/davix/wiki/User-Guide:-PRADS) |
| Processing |  |  |  | 2.1 | [User Guide: Processing](https://github.com/secviz/davix/wiki/User-Guide:-Processing) |
| R Project |  |  |  |  | [User Guide: R Project](https://github.com/secviz/davix/wiki/User-Guide:-R%20Project) |
| R Studio |  |  |  | 0.98.501 | [User Guide: R Studio](https://github.com/secviz/davix/wiki/User-Guide:-R%20Studio) |
| RRDTool |  |  |  | 1.4.7-2 | [User Guide: RRDTool](https://github.com/secviz/davix/wiki/User-Guide:-RRDTool) |
| RT Graph 3D |  |  |  | 0.1 | [User Guide: RT Graph 3D](https://github.com/secviz/davix/wiki/User-Guide:-RT%20Graph%203D) |
| rumint |  |  |  | 2.14 | [User Guide: rumint](https://github.com/secviz/davix/wiki/User-Guide:-rumint) |
| rsyslog |  |  |  | 5.8.11-2 | [User Guide: rsyslog](https://github.com/secviz/davix/wiki/User-Guide:-rsyslog) |
| Sagan |  |  |  | 0.2.1.r1-1 | Not available. |
| Scapy |  |  |  | 2.2.0-1 | [User Guide: Scapy](https://github.com/secviz/davix/wiki/User-Guide:-Scapy) |
| Seeds of Contempt |  |  |  | 0.6.0 | Not available. |
| Snort |  |  |  | 2.9.2.2-3 | [User Guide: Snort](https://github.com/secviz/davix/wiki/User-Guide:-Snort) |
| syslog-ng |  |  |  | 3.3.9-1 | Not available. |
| tcpdump |  |  |  | 4.4.0-1 | [User Guide: tcpdump](https://github.com/secviz/davix/wiki/User-Guide:-tcpdump) |
| tcpflow |  |  |  | 1.3.0+dfsg-2 | [User Guide: tcpflow](https://github.com/secviz/davix/wiki/User-Guide:-tcpflow) |
| tcpreplay |  |  |  | 3.4.4-2 | [User Guide: tcpreplay](https://github.com/secviz/davix/wiki/User-Guide:-tcpreplay) |
| tcpslice |  |  |  | 1.2a3-4 | [User Guide: tcpslice](https://github.com/secviz/davix/wiki/User-Guide:-tcpslice) |
| tcpstat |  |  |  | 1.5-7 | [User Guide: tcpstat](https://github.com/secviz/davix/wiki/User-Guide:-tcpstat) |
| tcpxtract |  |  |  | 1.0.1-8 | [User Guide: tcpxtract](https://github.com/secviz/davix/wiki/User-Guide:-tcpxtract) |
| Timesearcher 1 |  |  |  | 1.3.7 | [User Guide: Timesearcher 1](https://github.com/secviz/davix/wiki/User-Guide:-Timesearcher%201) |
| Tele Traffic Tapper |  |  |  | 1.7-3.3 | Not available. |
| tnv |  |  |  | 0.3.9 | [User Guide: tnv](https://github.com/secviz/davix/wiki/User-Guide:-tnv) |
| Treemap |  |  |  | 4.1.2 | [User Guide: Treemap](https://github.com/secviz/davix/wiki/User-Guide:-Treemap) |
| Tulip |  |  |  | 3.7.0dfsg-4b | [User Guide: Tulip](https://github.com/secviz/davix/wiki/User-Guide:-Tulip) |
| Walrus |  |  |  | 0.6.3 | [User Guide: Walrus](https://github.com/secviz/davix/wiki/User-Guide:-Walrus) |
| Wireshark |  |  |  | 1.10.2-1 | [User Guide: Wireshark](https://github.com/secviz/davix/wiki/User-Guide:-Wireshark) |
| ZenMap |  |  |  | 6.40-0.1 | Not available. |

# DAVIX Setup Guide

This guide describes the requirements and setup process of DAVIX using the installation scripts located in the “DAVIX Repository”: https://github.com/secviz/davix.

The installation scripts will install all of the core components necessary to run the tools in theDAVIX 2014 toolset and set up a davix user from which to run the tools. Note that we also modify a bunch of other things on your system (see below) and you will have to run these scripts as root.

We recommend that you create a clean virtual machine for this purpose to avoid compatibility issues.

## Environment Requirements

* Ubuntu 13.10 Desktop (saucy)
* root access to your Ubuntu instance

## Installation

Using root, from the command line download the davix-install-all script:

wget https://raw.githubusercontent.com/secviz/davix/master/install/davix-install-all.sh

Using root, from the command line run the script using root with the following command:

bash ./davix-install-all.sh

You will encounter a number of prompts throughout the process which you will have to respond to accordingly.

* You will be prompted to select either gdm or lightdm; defaults to “lightdm”.
* You will be prompted to accept EULAs or receive other prompts as the script runs; review and accept accordingly.
* You will be prompted to create a new password for the mysql root user; specify “davix” for the password.
* You will be asked if you want to make your MRTG config file readable only by root; defaults to “Yes”.
* You will be prompted for an IP address range when configuring snort; configure as desired or accept the default.
* You will be prompted to configure the prelude-manager database; defaults to “Yes”.
* You will then be prompted for the database to use with prelude-manager; choose mysql. Enter the password “davix” for mysql.
* You will be prompted about automatically configuring Chart Director; defaults to “yes”.
* You will be prompted to run a live test for Crypt library; accept default.

## DAVIX Use

Log in using the davix user account. The password is davix. Yes, just like the username.

## What the Installer Does

**We strongly recommend you do not run these scripts against your working environment.**

The installer does the following:

* Creates a davix user
* Fetches a series of packages from Ubuntu’s APT
* Installs a number of other tools
* Creates custom menus and directories for the DAVIX 2014 toolset
* Turns off a number of services to harden your install