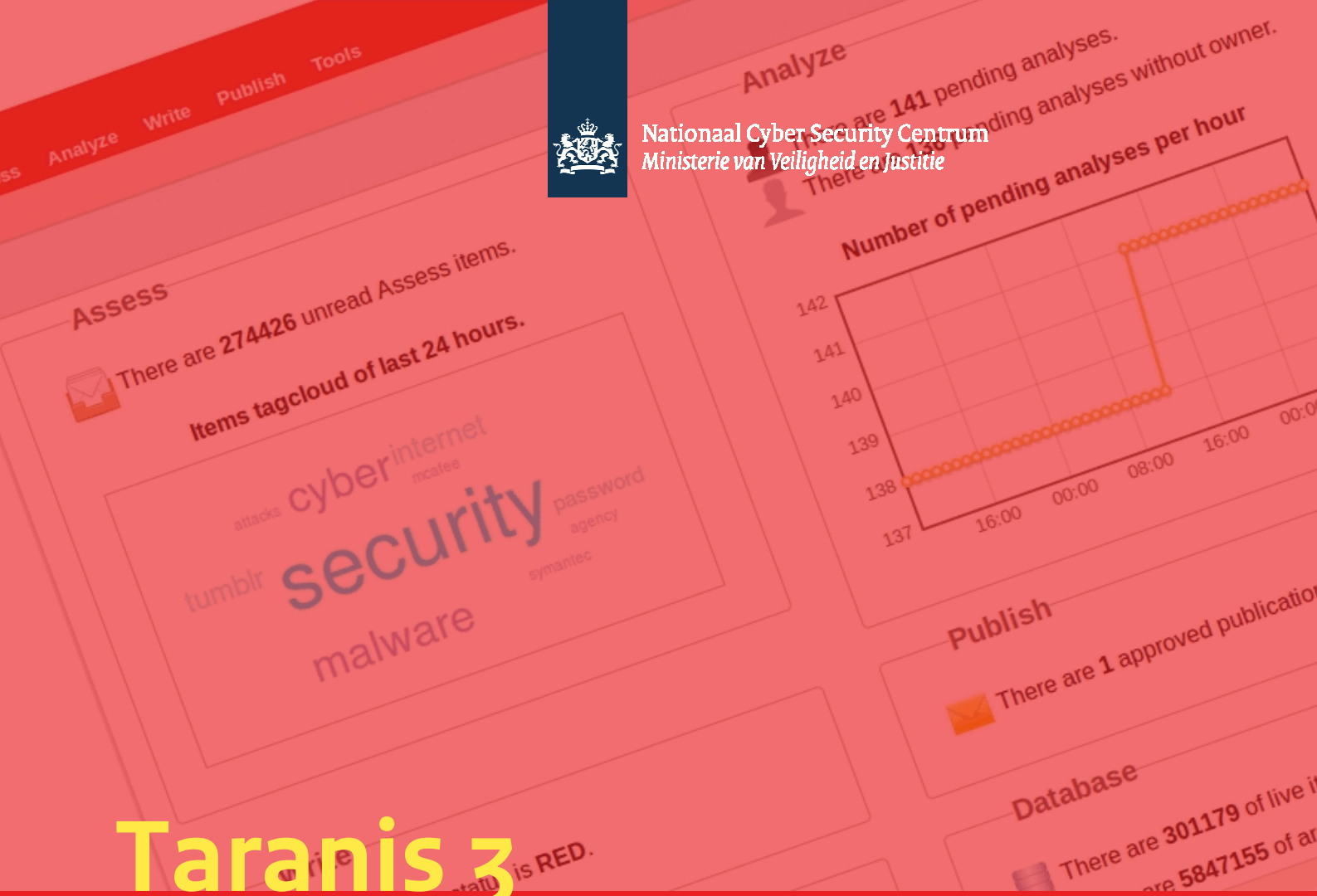


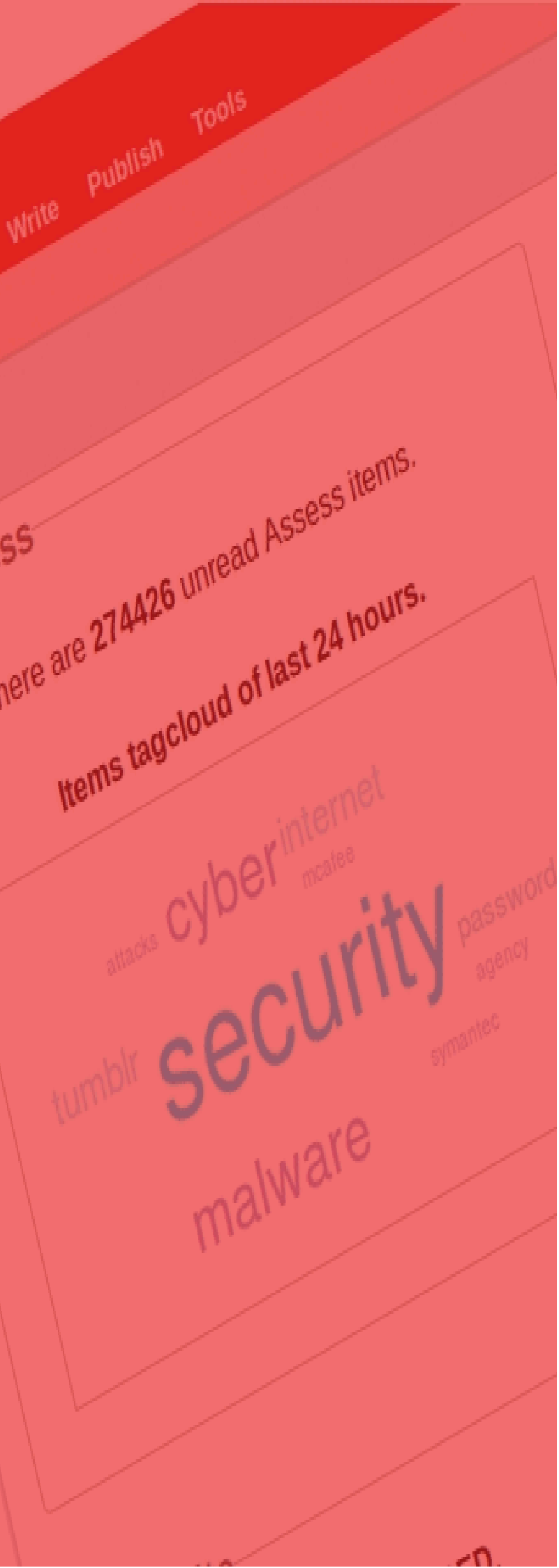
Taranis 3

Taranis 3.3.3 Installation Guide

Taranis 3

Installation Guide

National Cyber Security Centre
Turfmarkt 147 | 2511 DP The Hague
PO box 117 | 2501 CC The Hague
T +31 70 751 55 55 | F +31 70 888 75 50
www.ncsc.nl | info@ncsc.nl



Index

1 Introduction

NCSC-NL is the Dutch National Cyber Security Centre. NCSC-NL supports the Dutch government and Dutch critical infrastructure in preventing and dealing with ICT-related security incidents. For this purpose, NCSC-NL has a 24/7 watch team that scans the internet for digital threats and vulnerabilities in software and operating systems. They do so by daily keeping track of more than 1.000 sources like websites, public and private mailing lists and RSS-feeds.

Relevant news items and email messages are analyzed through analysis reports. Based on these news items, NCSC-NL publishes a number of products, each for its target audience: advisories, End-of-Week e-mails, End-of-Day e-mails, End-of-Shift e-mails and e-mails to an internal mailing list. The analysis reports also serve as input for a number of other products that NCSC-NL publishes, such as factsheets and white papers.

Processing and enriching these amounts of information and transforming them into various publications is an exacting task and can only be performed by using specialized tools. To ease this process, NCSC-NL developed Taranis. Taranis is completely developed in-house and is specifically designed to fit the workflow generally seen in a CERT organization, for collecting, analyzing and publishing information. Traceability and transparency have been constant considerations in the design and development of the application.

1.1 Goal of this document

The goal of this document is to explain the installation of Taranis on CentOS 7 (64 bit) or Ubuntu 16.04 LTS (64 bit) and how to configure the main settings.

1.2 References

Beside this 'Installation Guide', there are some additional documents that will help you use Taranis in your organization:

- The 'Taranis User Guide', aimed at end users of Taranis.
- The 'Taranis Administration Guide', aimed at functional and technical administrators of Taranis.
- The 'Migration Guide', describing how users of Taranis 3.1.2 can migrate their installation to Taranis 3.3.3 without losing data.
- The Release Notes that describe the differences between Taranis 3.1.2 and 3.3.3.

NOTE:

This installation guide is based on the use of CentOS 7 or Ubuntu 16.04 LTS. Installation on other Linux distributions mostly follows the same steps. The main difference is that not all packages mentioned will be available for your distribution.

1.3 Use of Taranis

NCSC-NL feels that Taranis can be a useful tool for other CERT organizations that more or less follow the same process. NCSC-NL first started sharing Taranis in 2009 and over the years, we have increasingly sought community involvement in discussing issues and bugs. More importantly, we have increasingly reached out to the growing Taranis community to determine which functionality would enrich the tool, while staying close to its goal of helping CERT-teams.

That's why NCSC-NL decided to make Taranis available to the community free of charge under the European Union Public License (EUPL). You can find more information on this license on the European Commission website[1].

[1] https://joinup.ec.europa.eu/software/page/eupl/licence-eupl

2 Installation

Taranis requires several components to be installed on the operating system. This chapter provides step-by-step descriptions on how to install the application. Some of the steps of the installation can be simplified by using ready-made scripts or configuration files; you will find these in subdirectory of the `install_scripts` directory inside the Taranis tar ball that corresponds to your OS. Every time a ready-made script or file is available, this is indicated by the  -icon.

2.1 Operating system

This document is written to facilitate the installation of Taranis on either the CentOS 7 distribution **with SELinux disabled**[2] or the Ubuntu 16.04 LTS distribution. The described steps to install Taranis are based on a clean, minimal install of the OS and assume you run commands under root privileges. This installation guide doesn't describe the basic steps required to get your server connected and up-and-running. In other words: it assumes you have a server running with access to the internet.

2.2 Unpacking Taranis

As the first step, unpack the Taranis tar ball in `/opt` and make sure it can be found in `/opt/taranis`:

1. Unpack the Taranis tarball in `/opt` (this creates a directory `/opt/taranis-v3.3.3`):

```
# cd /opt
# tar zxvf <sourcedir>/taranis-v3.3.3.tar.gz
```

2. Softlink the newly created directory to `/opt/taranis`:

```
# ln –s /opt/taranis-v3.3.3 /opt/taranis
```

2.3 CentOS: repositories

Some of the required packages are not part of the default CentOS 7 repositories. To ease the installation of these packages we advise you to add an additional yum-repository to your CentOS-installation: EPEL (Extra Packages for Enterprise Linux). This step does not apply to installation on Ubuntu.

2.3.1 Add EPEL

You add EPEL by following the steps below ( `epel_install.sh`):

```
# yum install epel-release.noarch
```

2.4 Packages

In order to run Taranis, several applications and libraries need to be installed on the system. Run `os_packages.sh` to install these.

2.5 Additional Perl modules

Some of the required Perl modules cannot be installed by use of the distributions' package repositories. These need to be installed by use of CPAN. Run  `cpan_modules.sh` to install them (this will take a while). The modules will be placed in a subdirectory called `local_libraries` within the Taranis installation.

2.6 Taranis

In order to configure the underlying infrastructure, perform the following steps.

2.6.1 Create a Taranis-user

Create a user-account called `taranis` for the Collector:

```
# useradd taranis
# passwd taranis
Enter new UNIX password: <password>
Retype new UNIX password: <password>
```

2.6.2 Filesystem permissions

Set the correct permissions on the various files and directories within Taranis by running  `taranis_permissions.sh`.

2.6.3 Apache2 configuration

Configure Apache (2.4) to be able to serve the Taranis-scripts. A typical Taranis-Apache configuration is available in

2 By default SELinux is enabled on CentOS. To view the SELinux-status on your system perform the command 'sestatus'. You can change the SELinux-settings through the /etc/selinux/config file

`taranis_apache.conf`. Note that restarting apache at yields an error. This will be corrected later on.

2.6.4 CentOS 7: Apache modules and firewall

This paragraph applies only to CentOS 7; for Ubuntu 16.04 LTS, please see the next paragraph.

Make sure the "Headers"-, "Rewrite"- and "Perl"-modules are loaded by Taranis.
You can enable these by making sure the following two lines are part of the `/etc/httpd/conf.modules.d/00-base.conf` file (this is true by default):

```
LoadModule headers_module modules/mod_headers.so
LoadModule rewrite_module modules/mod_rewrite.so
```

CentOS will block access to the webserver by default.In CentOS 7 uses FirewallD instead of the iptables service. To use the iptables service instead of FirewallD:

```
# systemctl disable firewalld
# systemctl stop firewalld
# yum install iptables-services
# systemctl start iptables
# systemctl enable iptables
```

Make sure you edit the default iptables-rules so that access to the server is enabled. You could do so by adding the following rule to `/etc/sysconfig/iptables`:

```
-A INPUT –m state --state NEW –m tcp –p tcp --dport 80 –j ACCEPT
```

Restart iptables for the changes to take effect:

```
# systemctl restart iptables
```

Restart Apache for the changes to take effect and make sure this service is automatically started on boot:

```
# systemctl restart httpd
# systemctl enable httpd
```

2.6.5 Ubuntu 16.04 LTS: Apache modules

This paragraph applies only to Ubuntu 16.04 LTS; for CentOS 7, please see the previous paragraph.

Make sure the "Headers"- , "Rewrite"-modules and "Perl"-modules are loaded by Taranis. You can enable these modules by linking to it from the "mods-enabled"-directory and then restarting Apache:

```
# ln –sf /etc/apache2/mods-available/headers.load
/etc/apache2/mods-enabled/headers.load
# ln –sf /etc/apache2/mods-available/perl.load
/etc/apache2/mods-enabled/perl.load
# ln –sf /etc/apache2/mods-available/rewrite.load
/etc/apache2/mods-enabled/rewrite.load
```

2.7 Initial configuration

Create the Taranis configuration file from the template provided:

```
# cp /opt/taranis/conf/taranis.conf.xml-dist
/opt/taranis/conf/taranis.conf.xml
# chown taranis:apache /opt/taranis/conf/taranis.conf.xml
```

Make sure you set the `session_secure_cookie` flag to the appropriate value. If you use HTTPS it should be `yes`, otherwise it should be `no`.

2.8 PostgreSQL

The PostgreSQL database management system is used to store the data as it is collected by Taranis. The PostgreSQL configuration for Taranis is done by performing the following steps:

2.8.1 CentOS 7: base configuration of PostgreSQL

On CentOS 7 only, initialize PostgreSQL first by issuing the commands below:

```
# systemctl enable postgresql
# postgresql-setup initdb
Initializing database:                    [ OK ]
# systemctl start postgresql
```

2.8.2 Create the Taranis database-user

Create the user `rss` that allows Taranis to communicate with PostgreSQL:

```
# su - postgres
# createuser –P -d rss
Enter password for new role: <password>
Enter it again: <password>
```

Configure PostgreSQL to allow inbound connections from the local host. Edit (or create) the file `pg_hba.conf`, which can be found in:

- CentOS 7: `/var/lib/pgsql/data`
- Ubuntu 16.04 LTS: `/etc/postgresql/9.5/main`

The `pg_hba.conf` file should contain the rules as shown below (`taranis_postgresql.conf`):

```
#TYPE  DB    USER   CIDR-ADDRESS   METHOD
local  all   all                   trust
host   all   all    127.0.0.1/32   md5
host   all   all    ::1/128        md5
host   all   all    0.0.0.0/0      reject
host   all   all    ::0/0          reject
```

After having made these changes, please restart the PostgreSQL daemon:

CentOS 7:
```
# systemctl restart postgresql
```

Ubuntu 16.04 LTS:
```
# service postgresql restart
```

2.8.3 *Create the database*

Create the database and enable lo (large object) support for the new database:

```
# psql postgres postgres
Type "help" for help.
postgres=# CREATE DATABASE rss WITH OWNER = rss;
CREATE DATABASE
postgres=# \c rss;
You are now connected to database "rss" as user "postgres".
rss=# CREATE EXTENSION lo;
CREATE EXTENSION
rss=# \q
```

Login as user `rss` to run the create script for the created database:

```
# psql rss rss
rss=> \i /opt/taranis/database_alterations/rss-schema.sql
[...]
rss=> \i
/opt/taranis/database_alterations/Taranis_initial_inserts.sql
[...]
```

The database `rss` should now be created. Check this by running:

```
# \d
[...]
# \q
```

2.8.4 *CentOS 7: set iptables rules for PostgreSQL*

CentOS will block access to PostgreSQL by default. For CentOS only, edit the default iptables-rules so that access to the server is enabled.
You could do so by adding the following rule to `/etc/sysconfig/iptables`:

```
-A INPUT –m state --state NEW –m tcp –p tcp –s 127.0.0.1/32 --
dport 5432 –j ACCEPT
```

Then restart iptables for the changes to take effect:

```
# systemctl restart iptables
```

2.8.5 *Set the database credentials in the Taranis configuration*

Set the database user (dbuser) and password (dbpasswd) in the `/opt/taranis/conf/taranis.conf.xml` configuration file to the values that were chosen previously.

Restart Apache2 for the change to take effect:

CentOS 7:
```
# systemctl restart httpd
```

Ubuntu 16.04 LTS:
```
# service apache2 restart
```

After restarting Apache, you should see the Taranis login screen when opening the Taranis homepage (`http://<ip-address>/taranis/`). If not, please review the logs to find out what's going wrong.

You can login to the Taranis webinterface by using the default administrator credentials:

- username: admin
- password: admin

Note that the dashboard page will show an error. This will be fixed later.

NOTE:

Make sure you immediately change the password of the admin-user by clicking on the 'User settings and preset searches' link on top of the screen after first login.

3 Configuration

Taranis can be configured on many different aspects. This chapter will guide you through the configuration options you should take a look at after installing Taranis.

3.1 The main Taranis configuration file

Most of the settings of Taranis can be changed in the file `/opt/taranis/conf/taranis.conf.xml`. You can keep much of the default settings in this file, but not all of them. Please see §4.2 of the Administration Guide for a list of the settings that you should review at this time.

3.2 Connecting one or more collectors

Taranis 3.3.2 introduces the ability to disconnect the Taranis Collector from the main Taranis system. This allows you to place the Collector on a separate system and/or to connect multiple distributed collectors to Taranis. You should at least configure one Collector as collecting information from your sources forms the basis of your Taranis installation.

3.2.1 Create the first Collector

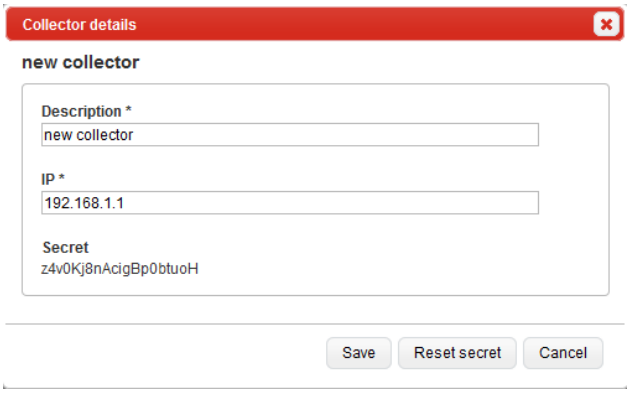
To define a Collector, login to the Taranis web interface and then click "Add new collector" in the "Taranis Configuration" → "Collectors" section. A popup will then allow you to specify this Collector based on a description and an IP address (figure 3-1).

Figure 3-1 Add a new collector

If you want to run the Collector on the same machine as the rest of your Taranis installation, you can specify `127.0.0.1` as the IP address.

To save the new Collector definition, just click "Save". Taranis will then automatically create a secret that you'll need on the Collector side to successfully create a connection to the Taranis server. You can always lookup this secret again by opening the details of the newly created Collector from the Taranis web interface. As you will see, next to the Description and the IP, also the Secret will now show up in the screen (figure 3-2).

Figure 3-2 Looking up the Collector secret



You can always reset the secret by clicking the "Reset secret" button. To enable the Collector to successfully communicate with the Taranis installation, you must specify the secret in the main Taranis configuration file (`taranis.conf.xml`). So if you want to add the Collector from figure 3-2 to the Taranis configuration, you should make sure the following line is in the configuration file:

```
<collector_secret>z4v0Kj8nAcigBpobtuoH</collector_secret>
```

3.3 Running the Collector and Dashboard scripts automatically

In order to have Taranis collect information from pre-defined sources, the `/opt/taranis/collector/collector.pl` script needs to be run with the privileges of the taranis-account you created. A cronjob that runs the collector periodically will ensure that the most up-to-date information is available to the Taranis user.

As soon as the collector has run, the webinterface will show the collected news-items. You can manually start the collector by issuing the following command (su to the user `taranis` before doing so!):

```
# su - taranis
# /opt/taranis/collector/collector.pl
```

The dashboard information information is generated by the dashboard background-script. You can start this script in the same way you started the collector:

```
# su - taranis
# /opt/taranis/dashboard/dashboard_background.pl
```

Make sure you run the collector and dashboard scripts at least once to correctly initialize the database.

In order to run these scripts automatically, we advise you to create a cronjob for these scripts under the taranis-account. You can do this as follows:

```
# su - taranis
# crontab -e
(add the following entries to the crontab):
*/1 * * * * sleep 10;
/opt/taranis/dashboard/dashboard_background.pl >/dev/null
*/20 * * * * /opt/taranis/collector/collector.pl >/dev/null
(Enter ':wq<enter>' to close the crontab)
crontab: installing new crontab
```

If you add the lines above to your crontab, the dashboard script will run every minute (*/1) and the collector every 20 minutes (*/20). Of course you can change this to any value that serves your purpose.

By default, Taranis has no sources configured in the database. However, the Taranis-package comes with around 380 example sources that you can import to quickly get up-to-speed with Taranis. See the Administration Guide for more information on how to do this.

3.4 ChartDirector

Taranis optionally offers extensive statistics on all the information stored and produced. These statistics can be shown through different types of charts like pie charts and bar charts. Taranis makes use of ChartDirector to produce these graphs.

3.4.1 Binaries

Taranis doesn't include the ChartDirector libraries. You must buy and download the appropriate library from the website (http://www.advsofteng.com/download.html) in order to be able to use the ChartDirector functionality. The table below lists the libraries available:

Unpack the archive somewhere on your system, copy the ChartDirector directory to `/opt/taranis`:

```
# cd /tmp
# wget
http://download2.advsofteng.com/chartdir_perl_linux_64.tar.gz
# tar -xf ./chartdir_perl_linux_64.tar.gz
# cp -R /tmp/ChartDirector /opt/taranis/
```

3.4.2 License

If you want to make use of these statistics, you are required to buy a ChartDirector license ($99) through the website of Advanced Software Engineering (ASE): http://www.advsofteng.com/purchase.html.

After you purchased a license, you must create the license file `chartdir.lic` with the license key you received and place it under the following directory:

```
/opt/taranis/ChartDirector/lib/chartdir.lic
```

If you don't purchase a license, you will see a message on the bottom of every statistic you generate.

After installing ChartDirector, run `taranis_permissions.sh` again to make sure it has the right permissions.

3.5 PhantomJS

Instead of collecting new items with text only, Taranis also offers the ability to collect screenshots of new items. For this Taranis uses the open source third-party software PhantomJS. In the `/opt/taranis/phantomjs` folder there are two JS files which are the link between Taranis and PhantomJS. But PhantomJS itself does not come with Taranis.

You can download PhantomJS from `http://phantomjs.org/download.html` After downloading the compressed file, the bin folder and its contents should be placed in the phantomjs folder `/opt/taranis/phantomjs/`
Here we use version 2.1.1, but any later version should work.

```
# cd /tmp
# wget
https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-
2.1.1-linux-x86_64.tar.bz2
# tar -xf ./phantomjs-2.1.1-linux-x86_64.tar.bz2
```

```
# cp -R /tmp/ phantomjs-2.1.1-linux-x86_64/bin
/opt/taranis/phantomjs
```

After installing PhantomJS, run `taranis_permissions.sh` again to make sure it has the right permissions.

3.6 CVE-descriptions and mapping

Import CVE-descriptions and CVE-CPE mappings by running the following two administration scripts on the command-line:

```
# su - taranis
# /opt/taranis/admin_scripts/cve_descriptions.pl
# /opt/taranis/admin_scripts/cpe_download.pl
```

WARNING:

Both of these scripts require a lot of system resources. It's known that running these scripts on servers with little memory can cause system instability.

To periodically refresh the CVE descriptions you can create a cronjob:

```
# su - taranis
# crontab -e
(add the following entries to the crontab):
00 17 * * * /opt/taranis/admin_scripts/cve_descriptions.pl &>
/dev/null
 (Enter ':wq<enter>' to close the crontab)
crontab: installing new crontab
```

3.7 Web-based configuration

After you've performed all the basic configuration steps as outlined in this chapter it is time to login to the Taranis webinterface and start adding sources, parsers, users, etc. Please refer to the 'Taranis Administration Guide' for more information about the different configuration options Taranis offers.

We advise you to at least configure the following items in Taranis before actual use. See the Administration Guide for details on these items:

- Start adding sources to your installation.
- Compile a list of possible damage descriptions if you plan to use the advisory-functionality of Taranis.
- Import the latest list of hard- and software from NIST.
- Create at least one constituent type, followed by at least one constituent group, one constituent role and one constituent individual.
- Create another Taranis-user. You'll need at least two users to be able to approve any product (advisory, End-of-Week).