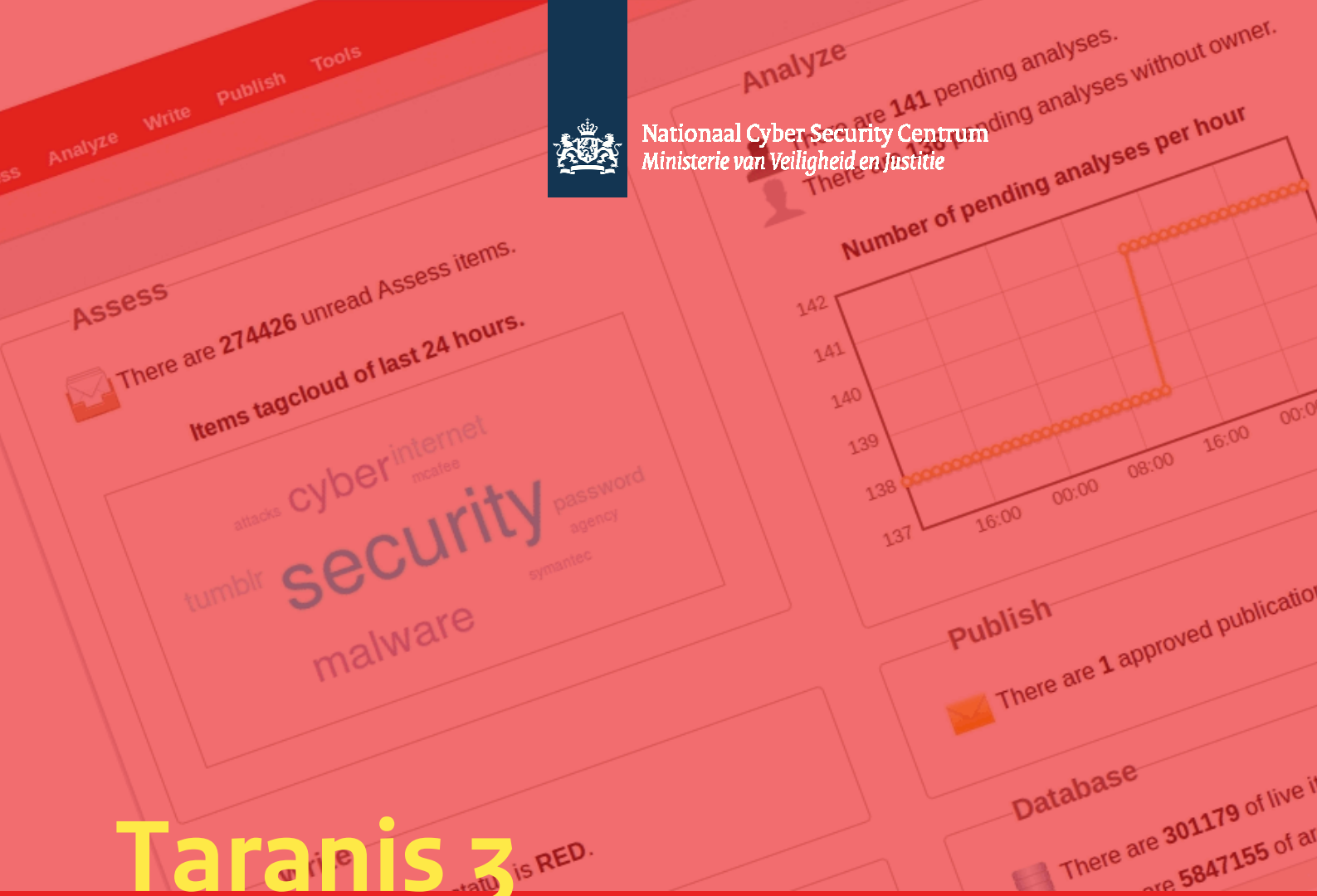


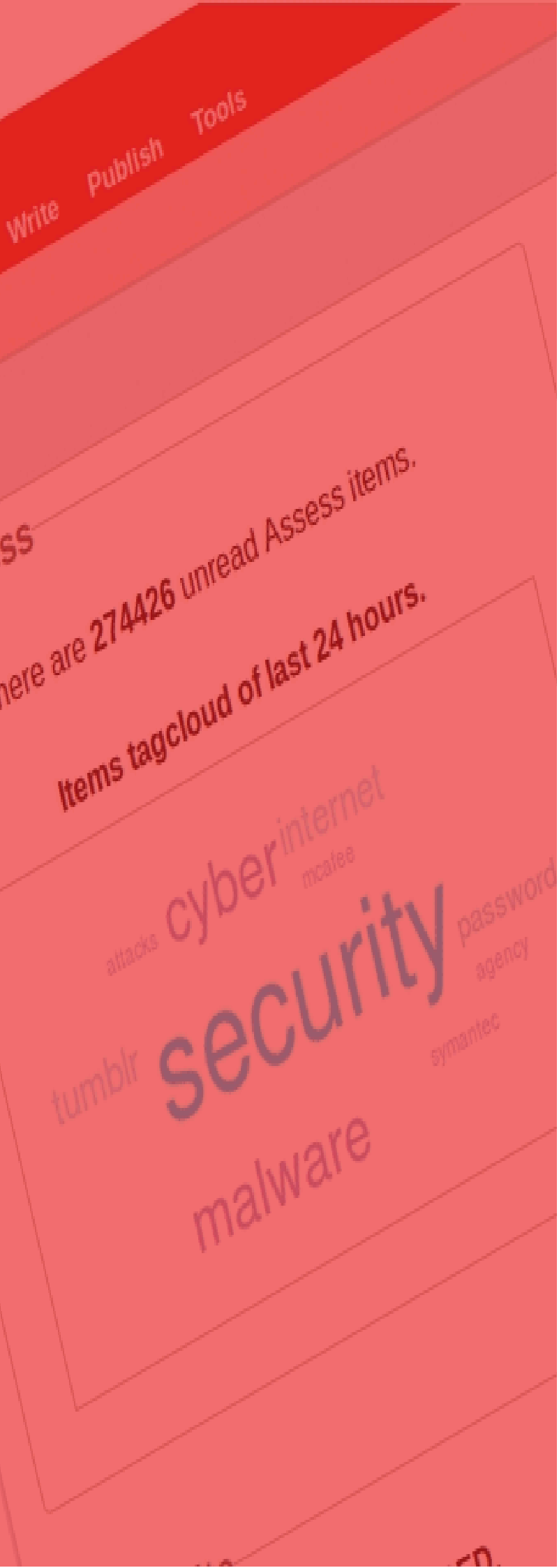
Taranis 3

Taranis 3.1.2 to 3.3.3 Migration Guide

Taranis 3

Taranis 3.3.3 Migration 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 Before you begin

This guide will help you migrate from Taranis 3.1.2 to Taranis 3.3.3 with step-by-step actions.

If you're currently using Taranis 3.1.X you can upgrade to 3.3.3 directly. If you're using an older version of Taranis (pre 3.1.X) you first have to upgrade your Taranis installation one version at the time (e.g. from 2.2.0 to 3.0.0, then from 3.0.0 to 3.1.0 and finally from 3.1.0 to 3.3). Please contact us on info@ncsc.nl for more information should that be the case.

Please be advised that due to database updates the total time of updating Taranis can be **several hours** depending on the size of your database!

1.1 Disable collectors

Collectors should be stopped and disabled before anything else. You can disable your collector(s) by preceding the collector entry in the crontab file with a # (hash).

```
# crontab -u taranis -e
#*/20 * * * * /opt/taranis/collector/collector.pl 1>/dev/null
2>/dev/null
(Enter ':wq<enter>' to close the crontab)
crontab: installing new crontab
```

You can check if a collector is running with:

```
# ps aux | grep collector.pl
```

If there are entries with collector.pl (other than grep) you can either wait until the collector is finished or kill the collector process.

1.2 Make backups

We advise you to backup several files and directories, which are installation specific, to a location outside of /opt/taranis/:

- configuration files in /opt/taranis/conf/
- source icons in /opt/taranis/webinterface/images/icons/
- cookie jar in /opt/taranis/collector/cookie_jar.txt
- your custom created tools. The files of Taranis tools can be located in several places:
  - /opt/taranis/backend_tools/
  - /opt/taranis/scripts/mod_tools/
  - /opt/taranis/templates/
  - /opt/taranis/webinterface/

Note that tools which are included in Taranis are:

- Whois
- Phishing checker
- Taranis announcements
- Feed digest
- BigScreen Streams
- Access tokens cleanup
- Dossier reminders
- Report reminders

These tools will be updated with Taranis 3.3.3.

2 Source files and dependencies

As code cleanup is also part of Taranis 3.3.3 it's recommended to start with a new Taranis installation. Taranis 3.3.3 also comes with some new dependencies which need to be installed.

2.1 Copy new source files

Before copying the Taranis 3.3.3 source files, move the old /opt/taranis to a backup directory.

```
# mv /opt/taranis /opt/taranis-3.1.2
```

Unpack the Taranis tar file.

```
# cp <sourcedir>/taranis-3.3.3.tar.gz /opt/
# tar zxvf ./taranis-3.3.3.tar.gz
# mv taranis-3.3.3 taranis
```

2.2 Install packages

Taranis 3.3.3 has new dependencies that can be installed via the packagemanager of you operating system. We recommend using the installscript available in /opt/taranis/install_scripts. For example for Ubuntu:

```
# /opt/taranis/install_scripts/ubuntu/os_packages.sh
```

2.3 Install new Perl modules

Taranis 3.3.3 comes with some new Perl module dependencies. These dependencies can be installed using the cpan_modules.sh installscript in /opt/taranis/install_scripts.
For example for Ubuntu:

```
# /opt/taranis/install_scripts/ubuntu/cpan_modules.sh
```

2.4 Add large objects (lo) support to PostgreSQL

Taranis 3.3.3 stores screenshots and uploaded files as large objects in PostgreSQL, which is not included in the default PostgreSQL installation. Adding support for large objects is done in three steps.

First, install package postgresql-contrib with *apt* (Ubuntu) or *yum* (CentOS).
Second, restart the postgresql service:

```
# service postgresql restart
```

Finally, add lo support to the rss database.

PostgreSQL 8.x:

```
# psql -U postgres -d rss -f /usr/share/pgsql/conftrib/lo.sql
```

PostgreSQL 9.x:

```
# psql rss postgres
rss=# CREATE EXTENSION "lo";
CREATE EXTENSION
rss=# \q
```

2.5 Update database

NOTE: this database update may take several hours!.

The database update consists of running a number of SQL update scripts.

The update can be performed by running each script separately or by using one script which includes all update scripts within a transaction.

Update in a single transaction:

```
# cd /opt/taranis/database_alterations/
# psql -f V333_from_312_transaction_update.sql rss rss
```

Update manually:

```
# cd /opt/taranis/database_alterations/
# psql -f V3_9_collector_update.sql rss rss
# psql -f V3_10_phishchecker_update.sql rss rss
# psql -f V3_11_user_action_update_and_bugfix_cpe_import.sql rss rss
# psql -f V3_12_phone_numbers_update.sql rss rss
# psql -f V3_13_minor_updates.sql rss rss
# psql -f V3_14_add_dossier.sql rss rss
# psql -f V3_15_password_update.sql rss rss
# psql -f V3_17_add_advisory_forward.sql rss rss
# psql -f V3_18_add_source_wordlists.sql rss rss
# psql -f V3_19_add_tool_feed_digest.sql rss rss
# psql -f V3_16_bigscreen_update.sql rss rss
# psql -f V3_20_add_additional_config_sources.sql rss rss
# psql -f V3_21_increase_link_length.sql rss rss
# psql -f V3_22_add_source_rating.sql rss rss
# psql -f V3_23_CVE_descritions_update.sql rss rss
# psql -f V3_24_CVE_templates.sql rss rss
# psql -f V3_25_collector_update.sql rss rss
# psql -f V3_26_phishingchecker_update.sql rss rss
# psql -f V3_27_endofshift_to_endofday.sql rss rss
# psql -f V3_28_new_endofshift.sql rss rss
# psql -f V3_29_add_entitlment.sql rss rss
# psql -f V3_30_mtbc_random_delay_max.sql rss rss
# psql -f V3_31_cve_links_change.sql rss rss
```

2.6 Restore backup files

Restore the files you saved in *1.2 Make backups*:

- restore source icons to /opt/taranis/webinterface/images/icons/
- restore cookie jar to /opt/taranis/collector/cookie_jar.txt
- restore your custom tools

Updating configuration files

We recommend to use the new default configuration files and merge the changes you made to the old configuration files manually. This is the most efficient and robust way to update the configuration files.

```
# cp /opt/taranis/conf/taranis.conf.xml-dist
/opt/taranis/conf/taranis.conf.xml
```

The next sections describe which configuration settings have been added and deleted in the new version of Taranis.

2.7 Updating taranis.conf.xml

The following settings have been **added** to /opt/taranis/conf/taranis.conf.xml:

Setting/description	Change?
collector_threads Number of threads the collector can use.	Yes
collector_secret The collector secret helps to identify the collector for statisics. The secret can be created when adding a collector in the Taranis GUI. Go to 'Taranis Configuration' → 'Collectors' → 'Add new collector'.	Yes
collector_alerter_to_address Email address that /collector/alerter.pl sends notifications to.	Yes
mail_from_address Sender FROM email address which is used in /collector/alerter.pl and backend scripts dossier_reminders.pl, feeddigest_mailings.pl and report.pl.	Yes
rt_ticket_url Direct RT URL to a ticket, but without the ticket ID; used in Taranis Dossiers.	Yes
screenshot_module Perl module to use for creating screenshots of webpages. You can change this setting if you want to use something other than PhantomJS for creating screenshots. Should be set to **"Taranis::Screenshot::Phantomjs".**	No
access_token_default_expiry Default expiry in minutes of access tokens. Defaults to **60** minutes if left blank.	Yes
dbsslmode PostgreSQL SSL mode options are: disable, allow, prefer and require. Defaults to **prefer**.	Yes
screen_width The width of the 'portal view'. This can be **px** or **%**. Defaults to **960px** which is also the advised minimum.	Yes
phishreferencemandatory Setting for the phishing tool to set if reference is mandatory. Can be set to **ON** or **OFF**.	Yes
phishreferencepattern Setting for the phishing tool to set a regex pattern for the reference.	Yes
publish_eod_from Specifies the 'from' e-mail address when sending End-of-Day.	Yes
publish_eod_to Specifies the 'to' e-mail address where to send the End-of-Day to (this can only be 1 address!).	Yes
publish_eod_to_public Specifies the 'to' e-mail address where to send the End-of-Day public to (this can only be 1 address!).	Yes
publish_eos_user An existing Taranis user which will be used to create and send End-of-Shift.	Yes
shifts End-of-Shift settings for shift **start**, **end**, **orange** and **red** times. **shifts** can have multiple **shift** elements and each shift has a shift **start**, **end**, **orange** and **red** setting. Example: `<shifts> <shift> <start>0700</start> <end>1430</end> <orange>1400</orange> <red>1430</red> </shift> <shift> <start>1430</start> <end>2200</end> <orange>2130</orange> <red>2200</red> </shift> </shifts>`	Yes

The following settings have been **removed** from /opt/taranis/conf/taranis.conf.xml:

```
<announcementsconfig></announcementsconfig>
<publish_eos_to_public></publish_eos_to_public>
<ssl_proxy_host></ssl_proxy_host>
<absroot></absroot>
```

```
<icondirectory_relative></icondirectory_relative>
<icondirectory_absolute></icondirectory_absolute>
```

2.8 Updating taranis.conf.entitlements.xml

The following settings have been **added** to /opt/taranis/conf/taranis.conf.entitlements.xml:

```
<entitlement id="assess_dialogs">
  <use_entitlement>items</use_entitlement>
</entitlement>
<entitlement id="collector">
  <menuitem>1</menuitem>
  <use_entitlement>configuration_generic</use_entitlement>
</entitlement>
<entitlement id="dossier">
  <menuitem>1</menuitem>
  <use_entitlement>dossier</use_entitlement>
</entitlement>
<entitlement id="dossier_note">
  <use_entitlement>dossier</use_entitlement>
</entitlement>
<entitlement id="dossier_pending">
  <use_entitlement>dossier</use_entitlement>
</entitlement>
<entitlement id="dossier_timeline">
  <use_entitlement>dossier</use_entitlement>
</entitlement>
<entitlement id="user_actions">
  <use_entitlement>admin_generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="forward">
  <use_entitlement>publication</use_entitlement>
</entitlement>
<entitlement id="publish_forward">
  <menuitem>1</menuitem>
  <use_entitlement>publication</use_entitlement>
</entitlement>
<entitlement id="feed_digest">
  <menuitem>1</menuitem>
  <use_entitlement>tools</use_entitlement>
</entitlement>
<entitlement id="wordlist">
  <use_entitlement>configuration_generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="access_token">
  <use_entitlement>configuration_generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="announcements">
  <menuitem>1</menuitem>
  <use_entitlement>generic</use_entitlement>
</entitlement>
<entitlement id="stream">
  <menuitem>1</menuitem>
  <use_entitlement>tools</use_entitlement>
</entitlement>
<entitlement id="cve">
  <use_entitlement>configuration_generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="cve_template">
  <use_entitlement>configuration_generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="contact_log">
  <menuitem>1</menuitem>
  <use_entitlement>report</use_entitlement>
</entitlement>
<entitlement id="incident_log">
  <menuitem>1</menuitem>
  <use_entitlement>report</use_entitlement>
</entitlement>
<entitlement id="special_interest">
  <menuitem>1</menuitem>
  <use_entitlement>report</use_entitlement>
</entitlement>
<entitlement id="todo">
  <menuitem>1</menuitem>
  <use_entitlement>report</use_entitlement>
</entitlement>
<entitlement id="report">
  <menuitem>1</menuitem>
   <use_entitlement>report</use_entitlement>
</entitlement>
<entitlement id="eod">
  <use_entitlement>publication</use_entitlement>
</entitlement>
<entitlement id="publish_eod">
  <menuitem>1</menuitem>
  <use_entitlement>publication</use_entitlement>
</entitlement>
<entitlement id="publish_eod_public">
  <menuitem>1</menuitem>
  <use_entitlement>publication</use_entitlement>
</entitlement>
```

The following settings have been **changed** in /opt/taranis/conf/taranis.conf.entitlements.xml:

```
<entitlement id="constituent_types">
  <menuitem>1</menuitem>
  <use_entitlement>constituent_groups</use_entitlement>
</entitlement>
<entitlement id="configuration">
  <use_entitlement>configuration_generic</use_entitlement>
  <use_entitlement>admin_generic</use_entitlement>
  <use_entitlement>constituent_groups</use_entitlement>
  <use_entitlement>photo_import</use_entitlement>
 <use_entitlement>constituent_individuals</use_entitlement>
  <use_entitlement>damage_description</use_entitlement>
  <use_entitlement>software_hardware</use_entitlement>
  <use_entitlement>publication_template</use_entitlement>
  <use_entitlement>configuration_parser</use_entitlement>
  <use_entitlement>configuration_strips</use_entitlement>
  <use_entitlement>sources_items</use_entitlement>
  <use_entitlement>tools</use_entitlement>
  <use_entitlement>users</use_entitlement>
  <use_entitlement>user_role</use_entitlement>
</entitlement>
```

The following settings have been **removed** from /opt/taranis/conf/taranis.conf.entitlements.xml:

```
<entitlement id="screen_settings">
  <use_entitlement>generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="get_screen">
  <use_entitlement>generic</use_entitlement>
  <menuitem>1</menuitem>
</entitlement>
<entitlement id="screen_announcements">
  <use_entitlement>generic</use_entitlement>
</entitlement>
<entitlement id="publish_eos_public">
  <menuitem>1</menuitem>
  <use_entitlement>publication</use_entitlement>
</entitlement>
<entitlement id="publish_eos_status">
  <use_entitlement>generic</use_entitlement>
</entitlement>
```

2.9 Updating taranis.conf.dashboard.xml

The following settings have been **added** to /opt/taranis/conf/taranis.conf.dashboard.xml:

```
<item>
  <module>Assess</module>
  <dataProcessor>oldestUnreadItem</dataProcessor>
  <showMinified>1</showMinified>
</item>
<item>
  <module>Write</module>
  <dataProcessor>endOfDayStatus</dataProcessor>
  <showMinified>1</showMinified>
</item>
<item>
  <module>Admin</module>
  <dataProcessor>latestUserActions</dataProcessor>
  <showMinified>0</showMinified>
</item>
```

2.10 Updating other configuration files

All configuration files can be found in /opt/taranis/conf/.

The following adjustments have been made:

- **removed** all <target> tags in taranis.conf.stats.xml
- **deleted** files taranis.conf.announcements.xml and taranis.conf.bigscreen.xml
- **replaced** file taranis.conf.publication.templates.xml
- **added** file taranis.conf.rest.routes.xml

3 System adjustments

Before logging into the GUI some steps need to be taken:

3.1 PhantomJS

For screenshot support download (http://phantomjs.org/download.html) and unpack phantomjs into /opt/taranis/phantomjs/. Note that PhantomJS must be accessible to the **apache** and **taranis** users!

Alternatively, PhantomJS might be installed via the packagemanager of the operating system if it is available. Make sure to create the correct symlinks

3.2 File permissions

Set file permissions of all files in /opt/taranis/ with taranis_permissions.sh, which can be found in the install_scripts folder.

3.3 Restart and Refresh

Apache needs to be restarted before you log in to the GUI.

```
# service apache restart
```

After restarting apache, users who are logged in need to log out and log in again.

Also, in some cases the browser has cached Taranis javascript files, which can lead to strange behavior. In that case please refresh the page (CTRL+SHIFT+R).

4 Post installation

After installing Taranis 3.3.3, a user with admin rights should complete the following actions:

- Add a collector (under Configuration) in GUI and add the generated secret to taranis.conf.xml. After adding the collector_secret to taranis.conf.xml, you will need to restart apache again.
- Set for all sources (under configuration) a collector to use; sources without collector will not be checked! If you have only added one collector, you can set all sources to use this collector with the admin script /admin_scripts/set_collector_for_sources.pl
- For each user-role, the rights for new entitlements 'dossier' and 'report' have to be set.
- [optional] Add publication type 'Advisory (forward)' to constituents types and constituents individuals in the GUI (for those who would like to receive it).
- [optional] Add report reminders tool to tools (under Configuration):
  name: Report Reminders
  webscript: dummy
  backend script: report.pl
- [optional] Add Access Tokens Cleanup tool to tools (under Configuration):
  name: Access Tokens Cleanup
  webscript: dummy
  backend script: access_tokens_cleanup.pl
- [optional] Add Feed Digests tool to tools (under Configuration):
  name: Feed Digests
  webscript:
  tools/feed_digest/displayFeedDigests/tool=feed_digest/
  backend script: feeddigest_mailings.pl
- [optional] Add Dossier Reminders tool to tools (under Configuration):
  name: Dossier Reminders
  webscript: dummy
  backend script: dossier_reminders.pl
- [optional] Add publication template for the new End-of-Shift:
  name: End-of-Shift (email)
  type: End-of-Shift (email)
  Below is an example template:

```
<publication>
<template><![CDATA[
====================
End-of-Shift report
====================
Timeframe:  _fld_timeframe_begin_ &minus;
_fld_timeframe_end_
Handler:    _fld_handler_

_fld_notes_

============
Contact log
============
_fld_contact_log_

=============
Incident log
=============
_fld_incident_log_

==========
To-do list
==========
_fld_todo_

================
Special interest
================
_fld_special_interest_

==============================
Resolved, deleted and expired
==============================
_fld_done_


]]></template>

<fields>
  <fld_timeframe_begin type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select_date_Dutch"
column="timeframe_begin">publication_endofshift</tbl>
  </fld_timeframe_begin>
  <fld_timeframe_end type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select_date_Dutch"
column="timeframe_end">publication_endofshift</tbl>
```

```
  </fld_timeframe_end>
  <fld_handler type="database">
    <tbl type="select" column="fullname"
alias="handler">users</tbl>
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="join1"
column="handler">publication_endofshift</tbl>
    <tbl type="join2" column="username">users</tbl>
  </fld_handler>
  <fld_notes type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select"
column="notes">publication_endofshift</tbl>
  </fld_notes>
  <fld_contact_log type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select"
column="contact_log">publication_endofshift</tbl>
  </fld_contact_log>
  <fld_incident_log type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select"
column="incident_log">publication_endofshift</tbl>
  </fld_incident_log>
  <fld_todo type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select"
column="todo">publication_endofshift</tbl>
  </fld_todo>
  <fld_special_interest type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select"
column="special_interest">publication_endofshift</tbl>
  </fld_special_interest>
  <fld_done type="database">
    <tbl type="key" column="id">publication_endofshift</tbl>
    <tbl type="select"
column="done">publication_endofshift</tbl>
  </fld_done>
</fields>
</publication>
```

For the new **BigScreen** the following actions should be taken:

- Edit 'Big Screen' setting in tools (under Configuration):
  name: Announcements
  webscript:
  tools/announcements/displayAnnouncements/tool=announcements/
- Add Taranis Stream tool to tools under Configuration):
  name: Taranis Stream
  webscript: tools/stream/displayStreams/tool=streams/
- Add user 'guest' (and maybe guest role) in Taranis for new BigScreen guest logon:
- For the new BigScreen an extra virtualhost must be created which uses mod_proxy.
  Apache conf can be found in:
  /apache_configuration4debian-ubuntu/taranis4u_apache_conf
  Source code can be found in: /taranis4u

By default the Taranis Stream functionality supports the following Displays:

```
Latest Headlines
News in waitingroom
Assess News TagCloud
Advisories Ready For Review
Pending Advisories
Pending Analyses
It's all about numbers
End-Of-Shift Status
To-do Lists
Lists
Announcements
```

5 Important notes

Please read the notes below:

- A check_passwords script is added to admin_scripts for checking which users are not updated to the new salted SHA-512 password. The script can also be used to disable accounts which are not updated yet.
- pg_dump will not add Postgres BLOBs automatically: *"-b --blobs Include large objects in the dump. This is the default behavior except when --schema, --table, or --schema-only is specified, so the -b switch is only useful to add large objects to selective dumps."* Also see http://www.postgresql.org/docs/8.4/static/app-pgdump.html
- When running the collector the SSL proxy is set as environment variable, so when multiple collectors are run on 1 host with different proxies, the collectors should be run by different system users.
- Sources with redirects from http to https don't work anymore. These sources should now be configured with https.
- By default the collector will use taranis.conf.xml, for extra collectors the file taranis.conf.collector.extra.xml can be used as an example. The extra collector should be started with --config like so:

```
# ./collector.pl --config
/opt/taranis/conf/taranis.conf.collector.extra.xml
```

- When using multiple collectors it's wise to run 1 collector in full mode and others with several functions disabled like so:

```
# ./collector.pl --nostats --noclustering --nobackend
```

- Extra collectors must have a different pidfiles, you can do this by changing the setting <pidfile> in the configuration.
- Even if only 1 collector is used, the collector needs to be added in GUI!