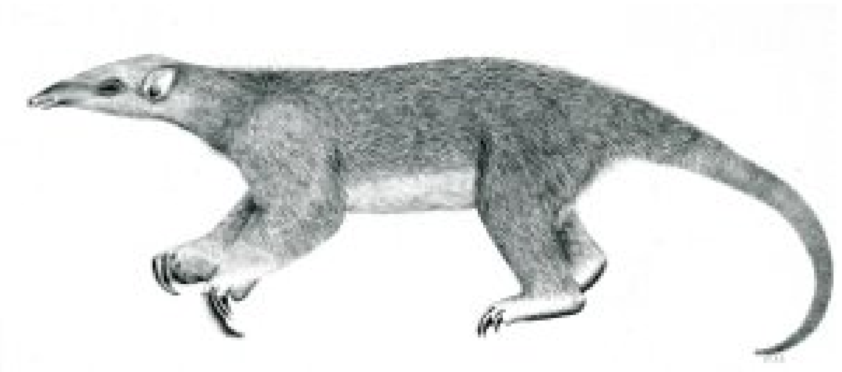
Tranalyzer2

psqlSink

PostgreSQL



Tranalyzer Development Team

Contents

Copyright © 2008–2019 by Tranalyzer Development Team

1 psqlSink

1.1 Description

The psqlSink plugin outputs flow files to PostgreSQL database.

1.2 Dependencies

1.2.1 External Libraries

This plugin depends on the **libpq** library.

Ubuntu: `sudo apt-get install libpq-dev`

Arch: `sudo pacman -S postgresql-libs`

Mac OS X: `brew install postgresql`

1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
PSQL_OVERWRITE_DB	2	0: abort if DB already exists 1: overwrite DB if it already exists 2: reuse DB if it already exists
PSQL_OVERWRITE_TABLE	2	0: abort if table already exists 1: overwrite table if it already exists 2: append to table if it already exists
PSQL_TRANSACTION_NFLOWS	40000	0: one transaction > 0: one transaction every *n* flows
PSQL_QRY_LEN	32768	Max length for query
PSQL_HOST	"127.0.0.1"	Address of the database
PSQL_PORT	5432	Port of the database
PSQL_USER	"postgres"	Username to connect to DB
PSQL_PASS	"postgres"	Password to connect to DB
PSQL_DBNAME	"tranalyzer"	Name of the database
PSQL_TABLE_NAME	"flow"	Name of the table

1.4 Post-Processing

The following queries can be used to analyze bitfields in PostgreSQL:

- Select all A flows:
```
SELECT to_hex("flowStat"::bigint), *
FROM flow
WHERE ("flowStat"::bigint & 1) = 0::bigint
```

Copyright © 2008–2019 by Tranalyzer Development Team

- Select all IPv4 flows:

```
SELECT *
FROM flow
WHERE ("flowStat"::bigint & x'4000'::bigint) != 0::bigint
```

- Select all IPv6 flows:

```
SELECT to_hex("flowStat"::bigint), *
FROM flow
WHERE ("flowStat"::bigint & x'8000'::bigint) != 0::bigint
```

Copyright © 2008–2019 by Tranalyzer Development Team