pgAudit Analyze - Open Source PostgreSQL pgAudit Analyzer

Contents

pgAudit Analyze Open Source PostgreSQL pgAudit Analyzer

Introduction

The PostgreSQL Audit extension (pgAudit) provides detailed session and/or object audit logging via the standard PostgreSQL logging facility. However, logs are not the ideal place to store audit information. The PostgreSQL Audit Log Analyzer (pgAudit Analyze) reads audit entries from the PostgreSQL logs and loads them into a database schema to aid in analysis and auditing.

Installation

- Install pgAudit following the instructions included with the extension.
- Update the log settings in `postgresql.conf` as follows:

```
log_destination = 'csvlog'
logging_collector = on
log_connections = on
```

  The log files must end with `.csv` and follow a naming convention that ensures files will sort alphabetically with respect to creation time. Log location is customizable when calling pgAudit Analyze.

- Install pgAudit Analyze:

Copy the bin and lib directories to any location you prefer but make sure they are in the same directory.

- Execute audit.sql in the database you want to audit as `postgres`:

```
psql -U postgres -f sql/audit.sql <db name>
```

Running

pgAudit Analyze is intended to be run as a daemon process.

```
./pgaudit_analyze --daemon /path/to/log/files
```

Testing

A `Vagrantfile` has been included in the test directory which gives the exact steps needed to get the regression rests running on `CentOS 7`. After logging on to the `vagrant` box simply run:

```
/pgaudit_analyze/test/test.pl
```

Regression tests will be run on PostgreSQL 10 by default. Specify `--pgsql-bin=/usr/pgsql-9.6/bin` to run tests on PostgreSQL 9.6 and use the same pattern for 9.5 testing.

Caveats

- The pgaudit.logon table contains the logon information for users of the database. If a user is renamed they must also be renamed in this table or the logon history will be lost.
- Reads and writes to the pgAudit schema by the user running pgAudit Analyze are never logged.

Author

The PostgreSQL Audit Log Analyzer was written by David Steele.