cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9-stig-overlay

InSpec profile overlay to validate the secure configuration of AWS RDS PostgreSQL 9 against DISA's PostgreSQL 9.x STIG Version 1 Release 1 tailored for CMS ARS 3.1 for CMS systems categorized as Moderate.

Getting Started

It is intended and recommended that InSpec run this profile from a **"runner"** host (such as a DevOps orchestration server, an administrative management system, or a developer's workstation/laptop) against the target.

For the best security of the runner, always install on the runner the *latest version* of InSpec and supporting Ruby language components.

The latest versions and installation options are available at the InSpec site.

Git is required to download the latest InSpec profiles using the instructions below. Git can be downloaded from the Git site.

The following attributes must be configured in an attributes file for the profile to run correctly. More information about InSpec attributes can be found in the InSpec Profile Documentation.

```
# description: 'Postgres OS user (e.g., 'postgres').'
pg_owner: 'postgres'

# description: 'Postgres OS group (e.g., 'postgres').'
pg_group: 'postgres'

# description: 'Postgres OS user password'
pg_owner_password: ''

# description: 'Postgres database admin user (e.g., 'root').'
pg_dba: 'root'

# description: 'Postgres database admin password ('password').'
pg_dba_password: 'password'

# description: 'Postgres normal user'
pg_user: ''

# description: 'Postgres normal user password'
pg_user_password: ''

# description: 'Postgres database hostname'
pg_host: ''
```

```
# description: 'Postgres database port'
pg_port: '5432'

# description: 'Postgres database name ('test')'
pg_db: 'test'

# description: 'Postgres database table name'
pg_table: ''

# description: 'User on remote database server'
login_user: ''

# description: 'Database host ip'
login_host: ''

# description: 'Database version'
pg_version: '9.5'

# description: 'Data directory for database (e.g., '/var/lib/pgsql/9.5/data')'.
pg_data_dir: ''

# description: 'Configuration file for the database ('/var/lib/pgsql/9.5/data/postgresql.con
pg_conf_file: ''

# description: 'User defined configuration file for the database (e.g., '/var/lib/pgsql/9.5/
pg_user_defined_conf: ''

# description: 'Configuration file to enable client authentication (e.g., '/var/lib/pgsql/9.
pg_hba_conf_file: ''

# description: 'Configuration file that maps operating system usernames and database usernam
pg_ident_conf_file: ''

# description: 'List of shared directories (e.g., pg_shared_dirs: ['/usr/pgsql-9.5', '/usr/p
pg_shared_dirs: []

# description: 'Database configuration mode (e.g., 0600)'
pg_conf_mode: '0600'

# description: 'Postgres ssl setting (e.g., 'on').'
pg_ssl: ''

# description: 'Postgres log destination (e.g., 'syslog').'
pg_log_dest: ''
```

```
# description: 'Postgres syslog facility (e.g., ['local0']).'
pg_syslog_facility: []

# description: 'Postgres syslog owner (e.g., 'postgres').'
pg_syslog_owner: ''

# description: 'Postgres audit log items (e.g., ['ddl','role','read','write']).'
pgaudit_log_items: []

# description: 'Postgres audit log line items (e.g. ['%m','%u','%c']).'
pgaudit_log_line_items: []

# description: 'Postgres super users (e.g., ['postgres']).'
pg_superusers: []

# description: 'Postgres users'
pg_users: []

# description: 'Postgres replicas (e.g. ['192.168.1.3/32']).'
pg_replicas: []

# description: 'Postgres max number of connections allowed (e.g., 100).'
pg_max_connections: 0

# description: 'Postgres timezone (e.g., 'UTC').'
pg_timezone: ''
```

Running This Overlay

When the **"runner"** host uses this profile overlay for the first time, follow these
steps:

```
mkdir profiles
cd profiles
git clone https://github.com/mitre/aws-rds-crunchy-data-postgresql-9-stig-baseline.git
git clone https://github.cms.gov/ispg/cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9
cd cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9-stig-overlay
bundle install
cd ..
inspec exec cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9-stig-overlay --attrs=<pat
```

For every successive run, follow these steps to always have the latest version of
this overlay and dependent profiles:

```
cd profiles/aws-rds-crunchy-data-postgresql-9-stig-baseline.git
git pull
cd ../cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9-stig-overlay
```

```
git pull
bundle install
cd ..
inspec exec cms-ars-3.1-moderate-aws-rds-crunchy-data-postgresql-9-stig-overlay --attrs=<pat
```

Viewing the JSON Results

The JSON results output file can be loaded into **heimdall-lite** for a user-interactive, graphical view of the InSpec results.

The JSON InSpec results file may also be loaded into a **full heimdall server**, allowing for additional functionality such as to store and compare multiple profile runs.

Getting Help

To report a bug or feature request, please open an issue.

Authors

- Eugene Aronne
- Danny Haynes

Special Thanks

- Aaron Lippold

License

- This project is licensed under the terms of the Apache 2.0 license.

NOTICE

This software was produced for the U. S. Government under Contract Number HHSM-500-2012-00008I, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data-General.

No other use other than that granted to the U. S. Government, or to those acting on behalf of the U. S. Government under that Clause is authorized without the express written permission of The MITRE Corporation.

For further information, please contact The MITRE Corporation, Contracts Management Office, 7515 Colshire Drive, McLean, VA 22102-7539, (703) 983-6000.