

# Securing Your Database in Amazon RDS

Sarah Conway

September 17, 2015

# Agenda

- Intro
  - What is Amazon RDS?
  - Features
  - Pricing
  - Setting Up & Connecting Tutorial
  - Data Ownership
  - PCI Compliance Certifications
- User & Database Management
  - Best User Management Practices
  - Database Management
- Network Management
  - Encryption
  - VPC Security Groups

## Agenda cont.

- Auditing & Monitoring
  - Auditing
  - Analyzing Logs
  - Monitoring
- Backups & Recovery
  - Automated Backups
  - DB Snapshots
- End
  - Questions

# What is Amazon RDS?

- Amazon Relational Database Service
- Managed service
- Good for DBA's, DevOps, Sysadmin, etc
- Versions 9.3.1 - 9.4.4 available
- <https://www.expeditedssl.com/aws-in-plain-english>

# Features

- PostGIS
- Language Extensions (PL/V8, PL/Perl, PL/Python)
- Full Text Search Dictionaries
- HStore, JSON Data Types
- pg\_stat\_statements
- postgres\_fdw
- auto-minor-version-upgrade
- Multi-AZ

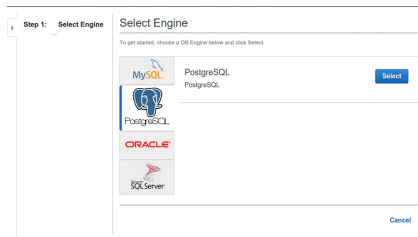
# Cons

- Limited control
- Can't force SSL connections
- Not a solution for a company with extensive privacy needs

# Pricing

- Varies depending on additional services selected
- Priced by usage
- Online cost calculator  
<http://calculator.s3.amazonaws.com/index.html>
- Billing alerts and notifications  
<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/monitor-charges.html>

# Setting up a RDS Instance



# Setting up a RDS Instance

Step 1: Select Engine

**Step 2: Production?**

Step 3: Specify DB Details

Step 4: Configure Advanced Settings

Do you plan to use this database for production purposes?

For databases used in production or pre-production we recommend:

- **Multi-AZ Deployment** for high availability (99.95% monthly up time SLA)
- **Provisioned IOPS Storage** for fast, consistent performance

Billing is based upon the **RDS pricing** table.  
An instance which uses these features is not eligible for the **RDS Free Usage Tier**.

☒ **Yes**, use Multi-AZ Deployment and Provisioned IOPS Storage as defaults while creating this instance

☐ **No**, this instance is intended for use outside of production or under the **RDS Free Usage Tier**

Cancel

Previous

Next Step

# Setting up a RDS Instance

Step 1: [Select Engine](#)

Step 2: [Production?](#)

**Step 3: Specify DB Details**

Step 4: [Configure Advanced Settings](#)

Your current selection is eligible for the free tier.

[Learn More.](#)

### Specify DB Details

Instance Specifications

DB Engine

postgres

License Model

postgresql-license

DB Engine Version

9.4.4

DB Instance Class

db.t2.micro — 1 vCPU, 1 GB RAM

Multi-AZ Deployment

No

Storage Type

General Purpose (SSD)

Allocated Storage\*

5 GB

Provisioning less than 100 GB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. [Click here](#) for more details.

Settings

DB Instance Identifier\*

middle-earth

Master Username\*

sruman

Master Password\*

.....

Confirm Password\*

.....

Select Yes to have Amazon RDS maintain a synchronous standby replica in a different Availability Zone than the DB instance. Amazon RDS will automatically fail over to the standby in the case of a planned or unplanned outage of the primary. [Learn More.](#)

\* Required

[Cancel](#) [Previous](#) [Next Step](#)

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBInstanceClass.html>

[http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

# Setting up a RDS Instance

VPC\*

Subnet Group

Publicly Accessible

Availability Zone

VPC Security Group(s)

Database Options

Database Name


Database Port

DB Parameter Group

Option Group

Copy Tags To Snapshots ☐

Enable Encryption

 The selected Engine or DB Instance Class does not support storage encryption.

Backup

Backup Retention Period  days

Backup Window

Maintenance

Auto Minor Version Upgrade

Maintenance Window

Select the number of days, between 1 and 35, that Amazon RDS should retain automatic backups of this DB Instance. The backup retention period determines the period for which you can perform a point-in-time recovery. Select 0 to disable backups. [Learn More.](#)

# Setting up a RDS Instance

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Security Group Delete Security Group

Filter All security groups Search Security Groups and IP

Name tag	Group ID	Group Name	VPC	Description
	sg-32d5a757	default	vpc-2a02ab4f (172.31.0.0/...	default VPC security group
	sg-c47d02a1	lsengard-server-sg1	vpc-2a02ab4f (172.31.0.0/...	lsengard-server-sg1

sg-c47d02a1

Summary Inbound Rules Outbound Rules Tags

Cancel Save

Type	Protocol	Port Range	Source	Remove
ALL TCP	TCP (6)	ALL	sg-c47d02a1	
SSH (22)	TCP (6)	22		

Add another rule

# Setting up a RDS Instance

```
[root@ip-10-10-10-10 ~]# psql -h middle-earth.rds.amazonaws.com -p 5432 -U saruman -d isengard
Password for user saruman:
psql (9.2.13, server 9.4.4)
WARNING: psql version 9.2, server version 9.4.
         Some psql features might not work.
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256)
Type "help" for help.

isengard=>
```

# Setting up a RDS Instance

sg-c47d02a1

Summary Inbound Rules Outbound Rules Tags

Edit

Type	Protocol	Port Range	Source
ALL TCP	TCP (6)	ALL	
ALL TCP	TCP (6)	ALL	sg-c47d02a1
SSH (22)	TCP (6)	22	

# Setting up a RDS Instance

```
cohen@rapture ~/Documents $ psql -h middle-earth.123456789012.us-east-1.rds.amazonaws.com -p 5432 -U saruman -d isengard
Password for user saruman:
psql (9.3.5, server 9.4.4)
WARNING: psql major version 9.3, server major version 9.4.
         Some psql features might not work.
SSL connection (cipher: ECDHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

isengard=>
```

# Data Ownership & Privacy

- 8.1 Your Content. As between you and us, you or your licensors own all right, title, and interest in and to Your Content.
- 3.2 Data Privacy. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities.

<https://aws.amazon.com/agreement>

# PCI Compliance Certifications

- Certified PCI Service Provider
- [http://d0.awsstatic.com/whitepapers/compliance/AWS\\_Anitian\\_Wookbook\\_PCI\\_Cloud\\_Compliance.pdf](http://d0.awsstatic.com/whitepapers/compliance/AWS_Anitian_Wookbook_PCI_Cloud_Compliance.pdf)

<http://aws.amazon.com/compliance/pci-dss-level-1-faqs/>

# Create an IAM Role

## Create Role

- Step 1: Set Role Name
- Step 2: Select Role Type
- Step 3: Establish Trust
- Step 4: Attach Policy
- Step 5: Review

## Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name

RDS-Admin

Maximum 64 characters. Use alphanumeric and <=, @, \_ characters

# Create an IAM Role

## Create Role

Step 1: Set Role Name

**Step 2: Select Role Type**

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

## Select Role Type

**AWS Service Roles**

<b>Amazon EC2</b> Allows EC2 instances to call AWS services on your behalf.	Select
<b>AWS Directory Service</b> Allows AWS Directory Service to manage access for existing directory users and groups to AWS services.	Select
<b>AWS Lambda</b> Allows Lambda Function to call AWS services on your behalf.	Select
<b>AWS Config</b> Allows AWS Config to call AWS services and collect resource configurations on your behalf.	Select
<b>AWS SWF</b> Allows SWF workflows to invoke Lambda functions on your behalf.	Select
<b>Role for Cross-Account Access</b>	
<b>Role for Identity Provider Access</b>	

# Create an IAM Role

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

## Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

Filter: Policy Type  Showing 150 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AdministratorAccess	0	2015-02-06 10:39 PST	2015-02-06 10:39 PST
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	2015-07-09 10:34 PDT	2015-07-09 10:34 PDT
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 10:36 PDT	2015-07-09 10:36 PDT
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonCognitoDeveloperAuthenticatedIdentities	0	2015-03-24 10:22 PDT	2015-03-24 10:22 PDT
<input type="checkbox"/>	AmazonCognitoPowerUser	0	2015-03-24 10:14 PDT	2015-03-24 10:14 PDT
<input type="checkbox"/>	AmazonCognitoReadOnly	0	2015-03-24 10:06 PDT	2015-03-24 10:06 PDT
<input type="checkbox"/>	AmazonDRSVPManagement	0	2015-09-01 17:09 PDT	2015-09-01 17:09 PDT
<input type="checkbox"/>	AmazonDynamoDBFullAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonDynamoDBFullAccesswithDataPipeline	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonDynamoDBReadOnlyAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	0	2015-03-19 11:45 PDT	2015-06-17 16:33 PDT
<input type="checkbox"/>	AmazonEC2ContainerServiceFullAccess	0	2015-04-24 09:54 PDT	2015-04-24 09:54 PDT
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	0	2015-04-09 09:14 PDT	2015-04-09 09:14 PDT
<input type="checkbox"/>	AmazonEC2FullAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input checked="" type="checkbox"/>	AmazonEC2ReadOnlyAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonFC2ReadOnlyAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST

# Create an IAM Role

## Create Role

- [Step 1: Set Role Name](#)
- [Step 2: Select Role Type](#)
- [Step 3: Establish Trust](#)
- [Step 4: Attach Policy](#)
- Step 5: Review**

## Review

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

<b>Role Name</b>	RDS-Admin	<a href="#">Edit Role Name</a>
<b>Role ARN</b>	arn:aws:iam::220427277352:role/RDS-Admin	
<b>Trusted Entities</b>	The identity provider(s) ec2.amazonaws.com	
<b>Policies</b>	am.aws.iam.:aws.policy\AmazonRDSFullAccess am.aws.iam.:aws.policy\AmazonVPCReadOnlyAccess am.aws.iam.:aws.policy\CloudWatchReadOnlyAccess am.aws.iam.:aws.policy\AmazonEC2ReadOnlyAccess	<a href="#">Edit Policies</a>

## User Management - Best Practices

- Create and use unprivileged users rather than master user
- Grant least privilege
- Make use of the policy generator
- Enable AWS CloudTrail to get logs of API calls
- Configure a strong password policy
  - Multi-Factor Authentication
  - Password expiration/rotation/reuse
- Remove unused security credentials that aren't needed

<http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html>

## rds\_superuser

```
# postgres=> create role testuser with password 'testuser' login;  
# CREATE ROLE  
# postgres=> grant rds_superuser to testuser;  
# GRANT ROLE  
# postgres=>
```

# Password Policy

Dashboard

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

- ☒ Require at least one uppercase letter ⓘ
- ☒ Require at least one lowercase letter ⓘ
- ☒ Require at least one number ⓘ
- ☒ Require at least one non-alphanumeric character ⓘ
- ☒ Allow users to change their own password ⓘ
- ☒ Enable password expiration ⓘ
- Password expiration period (in days):
- ☒ Prevent password reuse ⓘ
- Number of passwords to remember:
- ☒ Password expiration requires administrator reset ⓘ

Apply password policy

Delete password policy

# Managing PostgreSQL Object Privileges

```
# postgres=> revoke all on database <database name> from public;  
# REVOKE  
# test=> grant connect on database test to mytestuser;  
# GRANT
```

## Parameter Groups

- Equivalent to postgresql.conf
- Change values with ALTER DATABASE, ALTER ROLE, SET
- Need to create new parameter group else default settings are used
- Use safe practices when altering database parameters

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.PostgreSQL.CommonDBATasks.html>

## Viewing Parameter Settings

```
# select name, setting, boot_val, reset_val, unit  
# from pg_settings  
# order by name;
```

<http://www.postgresql.org/docs/9.3/static/view-pg-settings.html>

# sslinfo

```
# postgres=> create extension sslinfo;
# CREATE EXTENSION
# postgres=> select ssl_is_used();
# ssl_is_used
# -----
# t
# (1 row)
# postgres = > show ssl;
# ssl
# ----
# on
# (1 row)
```

## Accessing Instances with SSL

- Download public key at `http://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem`
- Import certificate
- Append `sslmode=require` to connection string
- Reference public key using `sslrootcert` parameter (`sslrootcert=rds-ssl-ca-cert.pem`)
- Verify endpoints using `sslmode=verify-full`
- Note: Use `"-"` instead of `"."` in bucket names for SSL

## Viewing Encryption Status

```
# Password for user master:
# psql (9.3.1)
# SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
# Type "help" for help.
#
# postgres=>
```

# AWS KMS

- Managed encryption service
- Create keys with a unique alias and description
- Define which IAM users and roles can manage keys
- Define which IAM users and roles can use keys to encrypt and decrypt data
- Choose to have AWS KMS automatically rotate keys annually
- Temporarily disable or reenale keys
- Audit use of keys through CloudTrail

<http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

# VPC Security Groups

- Virtual firewall
- Permissive only rules
- Changes automatically applied
- Rules modifiable at any time

## Default Groups

- Named default
- Allows inbound traffic only from other instances associated with default group
- Allows all outbound traffic from instance
- Can be modified but not deleted

## VPC Best Practices

- Have proper naming conventions
  - "AWS Region + Environment Code + OS Type + Tier + Application Code"
    - NA-D-LWB424
  - Don't make names self-explanatory! (UbuntuWebCRMProd)
  - Detect security group names for information revealing names
- Enable alerts for security groups
- Take advantage of CloudTrail
- Do not create least restrictive security groups like 0.0.0.0/0
- Don't have SSH port set to public (for EC2 instances)
- Don't use default security groups

# CloudTrail

- Provides full history of API calls
- Access control to log files using IAM
- Alerts for log files
- Compliant with internal policies and regulatory standards (PCI DSS v2.0, FedRAMP, etc)
- Important: Create IAM group for CloudTrail

[http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_LogAccess.Concepts.PostgreSQL.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_LogAccess.Concepts.PostgreSQL.html)

## Analyzing Logs with Garden Mammals

- pgbadger <http://sourceforge.net/projects/pgbadger/>
- Written in Perl
- Autodetects log file format (syslog, stderr or csvlog)
- Can parse huge log files inc. gzip
- <http://dalibo.github.io/pgbadger/>
- <https://github.com/sportngin/rds-pgbadger>
- <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.PostgreSQL.CommonDBATasks.html>
- Not to be confused with the honey badger

# CloudWatch

- Free
- Can set up alerts
- Subscribe to Amazon RDS events
- Detailed monitoring
- [https://github.com/Netflix/security\\_monkey](https://github.com/Netflix/security_monkey)

# Automated Backups

- On by default
- PITR
- Database & transaction logs stored
- Retention period can be configured up to 35 days

[http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_CommonTasks.BackupRestore.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_CommonTasks.BackupRestore.html)

# DB Snapshots

- User initiated backups
- Stored until manually deleted
- Create instance from snapshot at any time
- Can copy across regions

## Questions?

Thank You!