Automated Safeguards for Relational Database Service (RDS) & Aurora

Overview

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

RDS is available on several instance types, such as memory or CPU optimized, and provides familiar database engines to choose from. The following database engines are HIPAA-eligible and can process and host Protected Health Information (PHI)

- MySQL
- PostgreSQL
- Oracle
- Aurora (PostgreSQL or MySQL Engine)
- Microsoft SQL Server

All storage used by RDS must be encrypted at rest. ClearDATA utilizes AWS KMS keys to ensure data stored at rest in the underlying storage system is encrypted. Additionally all connections to the RDS database must be encrypted. Each database engine has a specific configuration method for encrypted connections. In addition, all databases must be backed up to ensure data is always available and all available auditing should be used to ensure regulatory requirements are met.

ClearDATA recommends that all Amazon RDS database instances that contain ePHI or other sensitive data be configured a Multi-AZ configuration. The Amazon RDS Multi-AZ feature automatically creates a primary database instance, and synchronously replicates data to a standby instance in a different Availability Zone, which is a separate physical location. The Multi-AZ feature also performs immediate failover in the event of infrastructure failure, helping to ensure a highly available and fault tolerant database. This helps healthcare customers conform with HIPAA Technical Safeguard 45 CFR § 164.308 (a)(ii)(7)(c), ensuring “continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.“ If customers do not utilize the Multi-AZ feature, this administrative safeguard can have partial compliance with using data backups (meeting 164.308(a)(7)(ii)(a-b), however the business requirements of “continuation of critical business processes” may not tolerate the time necessary to restore a database in the event of an infrastructure failure. ClearDATA recommends customers review their business and compliance requirements and ensure there are appropriate controls in place.

You pay only for what you use for each database instance. You are billed based on the following:

- DB instance hours – Based on the class (e.g. db.t2.micro, db.m4.large) of the DB instance consumed. Partial DB instance hours consumed are billed as full hours.
- Storage (per GB per month) – Storage capacity you have provisioned to your DB instance. If you scale your provisioned storage capacity within the month, your bill will be pro-rated.
- I/O requests per month – Total number of storage I/O requests you have (for Amazon RDS Magnetic Storage and Amazon Aurora only)
- Provisioned IOPS per month – Provisioned IOPS rate, regardless of IOPS consumed (for Amazon RDS Provisioned IOPS (SSD) Storage only)
- Backup Storage – Backup storage is the storage associated with your automated database backups and any customer-initiated database snapshots. Increasing your backup retention period or taking additional database snapshots increases the backup storage consumed by your database.
- Data transfer – Internet data transfer in and out of your DB instance.

Compliance Guidance

ClearDATA Automated Safeguards for RDS ensure that all of the compliance requirements are met for all newly created RDS instances. ClearDATA reviews newly created databases to ensure the database storage is encrypted, the RDS Parameter or Option Group enforces an encrypted database connection and necessary audit logging, backups are enabled, and the RDS instance is not publicly available. If these settings are not properly configured, the database instance will be deleted shortly after creation.

Encrypted Storage

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption addressable standard strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all storage must be encrypted.

Remediation

If the encryption settings are not properly selected when the database is provisioned it will be immediately deleted.

Encrypted Connections

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption addressable standard strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all connections to the RDS databases must use a TLS encrypted connection, ensuring the data transmitted from client to and from database is encrypted. All of the RDS database types listed above, with the exception of MySQL, can enforce a TLS connection through either a Parameter Group or Option Group to ensure only encrypted connections are allowed. Please see Working with DB Parameter Groups for details on how to configure Parameter Groups. ClearDATA has provided CloudFormation template snippets for Parameter Groups later in this article.

Remediation

If the encryption settings are not properly selected when the database is provisioned it will be immediately deleted.

Automated Backups

HIPAA Technical Safeguard 45 CFR §164.308(a)(7)(ii)(B) requires a Covered Entity to "establish (and implement as needed) procedures to restore any loss of data." The automated backup feature of Amazon RDS enables point-in-time recovery of your DB instance. When automated backups are turned on for your DB Instance, Amazon RDS automatically performs a full daily snapshot of your data (during your preferred backup window) and captures transaction logs (as updates to your DB Instance are made). When you initiate a point-in-time recovery, transaction logs are applied to the most appropriate daily backup in order to restore your DB instance to the specific time you requested. Amazon RDS retains backups of a DB Instance for a limited, user-specified period of time called the retention period, which by default is 7 days but can be set to up to 35 days. You can initiate a point-in-time restore and specify any second during your retention period, up to the Latest Restorable Time. You can use the DescribeDBInstances API to return the latest restorable time for you DB instance, which is typically within the last five minutes. The backups are replicated across multiple physical locations to ensure the data is available.

Remediation

If the backup retention is not set to a value greater than 7 when the database is provisioned it will be immediately deleted.

Audit Logging

HIPAA Technical Safeguard 45 CFR § 164.312(b) requires a Covered Entity to “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred. ClearDATA recommends our customers utilize auditing in the application that will record the activity against PHI records. Database audit logs are available for all RDS database types and can be enforced through either a Parameter Group or Option Group. Further details about RDS logging is available at http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_LogAccess.html.

Remediation

If the Parameter or Option Group is not properly configured when the database is provisioned, the database may be immediately deleted.

Public Access

HIPAA Technical Safeguard 45 CFR § 164.312(e)(1) requires implementation technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. ClearDATA monitors the RDS instances to ensure they are not publicly accessible, which could lead to unintended data access. Please see Working with an Amazon RDS DB Instance in a VPC for details regarding RDS Subnet Groups.

Remediation

If the public access settings, or the Database Subnet Group, are not properly selected when the database is provisioned it will be immediately deleted.

Shared Responsibility

ClearDATA will ensure that all RDS instances created in accounts with Automated Safeguards meet the requirements outlined above under Compliance Guidance. If an RDS instance is created and found to violate any of the items listed, the instance will be terminated and an alert will be sent to the ClearDATA SNS topic with details of the violation.

Customers are responsible for adhering the to guidelines listed above when creating RDS instances that may contain sensitive data. ClearDATA has provided CloudFormation template snippets below to help customers deploy databases that adhere to the guidelines.

Customers are also responsible for ensuring all MySQL clients use an encrypted connection to any MySQL RDS databases. MySQL database cannot enforce the use of TLS connections from the database side, therefore clients must ensure they are using a TLS connection.

Exclusion

Disabling automated remediation at done the instance level. Please contact ClearDATA Support to request that an exclusion be placed to allow for the instance to be created.

Below are CloudFormation Template snippets to help customers build proper Parameter Groups to meet the guidance requirements.

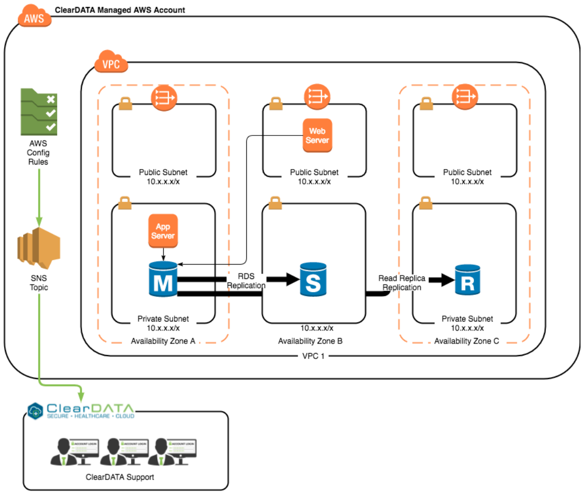
```
DBParamGroup:
    Type: AWS::RDS::DBParameterGroup
    Properties:
      Description: Database Parameter Group for MSSQL
      Parameters:
        rds.force_ssl: 1
        rds.sqlserver_audit: fedramp_hipaa
```

```
  DBParamGroup:
    Type: AWS::RDS::DBParameterGroup
    Properties:
      Description: Database Parameter Group for PostgreSQL
      Parameters:
        rds.force_ssl: 1
```

```
  DBOptionGroup:
    Type: AWS::RDS::OptionGroup
    Properties:
      OptionGroupDescription: Database Option Group for Oracle
      OptionConfigurations:
        - OptionName: NATIVE_NETWORK_ENCRYPTION
          OptionSettings:
            - Name: SQLNET.ENCRYPTION_SERVER
              Value: REQUIRED
```

You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS.

Users can be added to the **DPHI-RDS** group to gain access to create and manage RDS instances.



Item	ClearDATA	Customer
Ensure encryption connection is configured at the client for all database connections to any MySQL RDS instances	IC	RA
Instance & database creation	IC	RA
Database administration	IC	RA
Database restore	IC	RA
Ensure any service excluded from automated remediation does not contain any PHI/PII	IC	RA
Enforcement of Automated Safeguards	RA	IC