Automated Safeguards for DynamoDB

Amazon DynamoDB is a nonrelational database that delivers reliable performance at any scale. It's a fully managed, multi-region, multi-master database that provides consistent single-digit millisecond latency, and offers built-in security, backup and restore, and in-memory caching.

Data Storage
DynamoDB charges per GB of disk space that your table consumes. The first 25 GB consumed per month is free, and prices start from $0.25 per GB-month thereafter.

Write Capacity Unit
One write capacity unit (WCU) provides up to one 1 KB write request per second. Writing larger items requires additional WCUs. For example, if your item size were 2 KB, you would require 2 WCUs to sustain one write request per second.

Read Capacity Unit
One read capacity unit (RCU) provides up to two eventually consistent 4 KB reads per second or one strongly consistent 4 KB read per second. Reading larger items requires additional RCUs. For example, if your item size were 8 KB, you would require 2 RCUs to sustain one strongly consistent read per second or 1 RCU if you choose eventually consistent reads.

Capacity Planning
You should round up to the nearest KB when estimating how many capacity units to provision. For example, if your item size were 7.5 KB, you would round up to 8 KB. As a result, you would require 8 WCUs to sustain one write request per second to that item, and 2 RCUs to sustain one strongly consistent read per second.

Continuous backups and point-in-time recovery
Point-in-time recovery (PITR) provides continuous backups of your DynamoDB table data. ClearDATA Automated Safeguard enables PITR for all DynamoDB tables to ensure the data is backed up in accordance with the necessary regulations. DynamoDB maintains continuous backups of your table for the preceding 35 days. PITR is charged based on the current size of each DynamoDB table (table data, local secondary indexes) where it is enabled. AWS will continue to bill you until you disable PITR on each table.

See the DynamoDB Pricing Page for full details and examples.

Architecture

DynamoDB is a fast and flexible nonrelational database service for any scale. DynamoDB enables customers to offload the administrative burdens of operating and scaling distributed databases to AWS so that they don't have to worry about hardware provisioning, setup and configuration, throughput capacity planning, replication, software patching, or cluster scaling. DynamoDB is a fully managed cloud service that you access via API. Applications running on any operating system (such as Linux, Windows, iOS, Android, Solaris, AIX, and HP-UX) can use DynamoDB. We recommend using the AWS SDKs to get started with DynamoDB.

DynamoDB is a feature rich product that can be used in a wide variety of scenarios. ClearDATA recommends reviewing the DynamoDB documentation listed below for a description of the service, how it works, and how it can be used.

DynamoDB Features

DynamoDB Frequently Asked Questions

DynamoDB: How it Works

Best Practices for DynamoDB

DynamoDB Integration with Other AWS Services

DynamoDB Guide

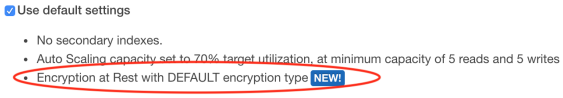
The ClearDATA Automated Safeguards for DynamoDB ensure that all tables meet the technical requirements necessary to store sensitive data. DynamoDB tables are interrogated upon creation to ensure that the table is encrypted and Point-in-time-recovery (PITR) backups are enabled. If the table is not encrypted, ClearDATA will update the table to use encryption, if that option is available (the feature to encrypt existing tables is not yet available in all regions or accounts). If the table is not able to be updated with encryption at rest, the table will be deleted moments after creation. The Automated Safeguard will also enable Point-in-time-recovery backups on all tables to ensure sensitive data is being backed up. There will be a cost associated with PITR backups based on the size of the table.

Compliance Guidance

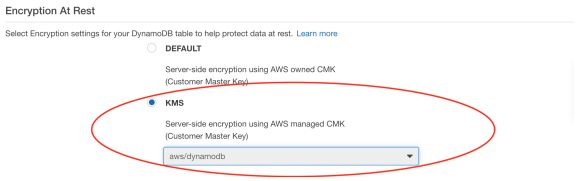
Encrypted Storage

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requiring 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, and therefore the Automated Safeguards do not allow unencrypted DynamoDB tables.

Amazon Web Services automatically encrypts all DynamoDB tables using a centrally managed encryption key. This key is known as DEFAULT in the DynamoDB console.



Because this key is centrally managed by AWS and not tied to an individual account ClearDATA does not consider the use of the DEFAULT key to be compliant. In ClearDATA's opinion the use of the DEFAULT key is relying too heavily on the compensating controls associated with the protection of the single key. ClearDATA requires that customers use a KMS key.



Remediation

If the DEFAULT encryption key is selected when the table is provisioned, the table is immediately deleted.

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 Point-in-time recovery feature of Amazon DynamoDB helps protect Amazon DynamoDB tables from accidental write or delete operations. With point-in-time recovery, customers can restore a table to any point in time during the last 35 days. DynamoDB maintains incremental backups of the table.

Remediation

ClearDATA automatically, and transparently, enables backups of all Dynamo tables.

Shared Responsibility

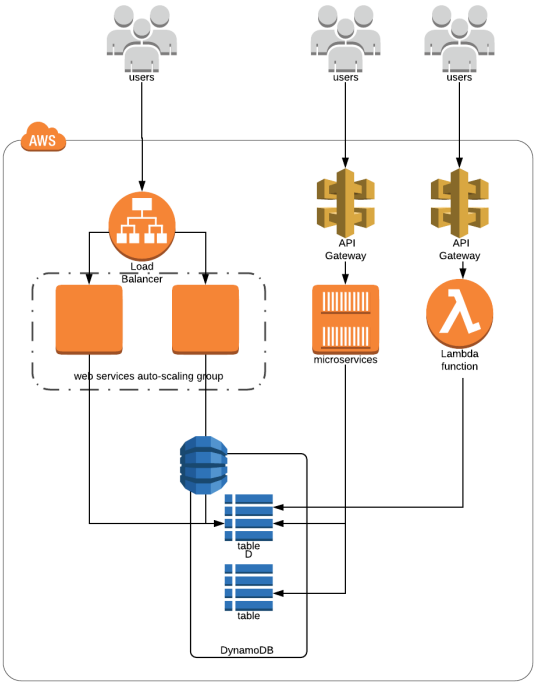
Connections to Amazon DynamoDB containing PHI must use endpoints that accept encrypted transport (HTTPS). For a list of regional endpoints, see http://docs.aws.amazon.com/general/latest/gr/rande.html#ddb_region. Customers must use HTTPS endpoints wherever referenced.

Customers must use a KMS key for encrypting the DynamoDB table, not the DEFAULT key as outlined in Encrypted Storage above.

Please contact your ClearDATA team for a copy of the Responsibilities Matrix.

Exclusion

Disabling automated remediation at done the table level. Please contact ClearDATA Support to request that an exclusion be placed on the table.



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

Item	ClearDATA	Customer
Ensure encrypted endpoints are used	IC	RA
Architect, design, create, & maintain DynamoDB tables	IC	RA
Configure connections to DynamoDB tables	IC	RA
Restore DynamoDB tables, if required	IC	RA
Configure Global Tables, if required	IC	RA
Enforcement of Automated Safeguards	RA	IC