AWS Cloud ServCertification: Amazon DynamoDB

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Service Status**   |  |  |  | | --- | --- | --- | | Pass | Review | Remediate | | **Vendor Status** | **Vendor Notes** |
| 1 | External Certification | DynamoDB is covered as part of the SOC 1, 2 & 3 reports in the following regions: US East, US West, Canada, EU (Ireland, Frankfurt, London) Asia Pacific (Singapore, Sydney, Tokyo, Seoul, Mumbai), and South America (São Paulo) | All reports can be downloaded from AWS Artifact. | <https://aws.amazon.com/compliance/services-in-scope/> |
| 2 | Authentication | IAM is leveraged to handle authentication. | Bank is likely to use IAM roles which will be mapped to on premise Active Directory Groups | <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/authentication-and-access-control.html> |
| 3 | Authorization | IAM is leveraged to handle authorization.  DynamoDB offers very granular policy enforcement, providing that ability to restrict access not only at the [table](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_dynamodb_specific-table.html), but also the [column](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_dynamodb_columns.html) and [row](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_dynamodb_rows.html) level via IAM policies.  User permissions can be scoped down to tables and items.  Resource based policies are not supported for DynamoDB. |  | <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/authentication-and-access-control.html> |
| 4 | Encryption At Rest | DynamoDB supports encryption-at-rest encryption for the following regions   * US East (Ohio) * US East (N. Virginia) * US West (Oregon) * US West (N. California) * Canada (Central) * South America (São Paulo) * EU (Ireland) * EU (London) * EU (Frankfurt) * Asia Pacific (Mumbai) * Asia Pacific (Tokyo) * Asia Pacific (Seoul) * Asia Pacific (Singapore) * Asia Pacific (Sydney)   CMKs are not supported by the SSE utilised by DynamoDB; you can only make use of service default keys. These keys are created by DynamoDB for every region where it is used if they do not already exist.  You can also use client side encryption, using KMS, to encrypt data before it is stored in DynamoDB. |  | <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html> |
| 5 | Encryption In Transit | DynamoDB provides a dedicated “Encryption Client” which developers and operators can make use of to encrypt data. This can transparently encrypt data client side.  DynamoDB supports the use of TLS backed endpoints.  DynamoDB does not have the notion of resource based policies; restrictions to the transport type (e.g. HTTPS only) can be attached to user policies to prevent them from using plain HTTP connections. | It is not possible to enforce or monitor clients using the encryption client.  It is possible to enforce and monitor clients using encrypted service endpoints.  The following policy statement, when applied to a policy and attached to a principle, will prevent the use of DynamoDB over HTTP  {  "Action": "dynamodb:\*",  "Effect": "Deny",  "Resource": "arn:aws:dynamodb:\*:\*:\*/\*",  "Condition": {  "Bool": {  "aws:SecureTransport": "false"  }  }  } | <https://docs.aws.amazon.com/dynamodb-encryption-client/latest/devguide/client-server-side.html> |
| 6 | Underlying OS | DynamoDB is a managed service. The underlying technologies are not configurable by Customer. | DynamoDB is in-scope for SOC and PCI. | https://aws.amazon.com/compliance/services-in-scope/ |
| 7 | CSP access | Access to the DynamoDB data store can be controlled via IAM policy and encryption using KMS. | The AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The Amazon Corporate network relies on user IDs, passwords, and Kerberos, while the AWS Production network requires SSH public-key authentication through a bastion host. AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager [1]  Details of these controls and how they are validated by an independent 3rd party are available via AWS Artifact (SOC 2 - Security, Availability & Confidentiality Report) [2] | AWS Security Whitepaper <https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf>   AWS SOC FAQs: <https://aws.amazon.com/compliance/soc-faqs/> |
| 8 | Endpoint Localization | You can use VPC endpoints to keep traffic between your Amazon VPC and DynamoDB from leaving the Amazon network. |  | https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html |
| 9 | Storage/Process Isolation | The DynamoDB platform is serverless and makes use of a shared-tenancy host model - there are no physical hosts to set up or manage. |  |  |
| 10 | Supporting Services | KMS, VPC, CloudTrail, CloudWatch, IAM | DynamoDB is a managed service and other services can be used to augment or provide greater security/compliance control. They are not required for base functionality. |  |

## Summary

This document provides a compiled list of security controls and best practices for DynamoDB to assist security teams in assessing DynamoDB’s fitness for use.

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling. Also, DynamoDB offers encryption at rest, which eliminates the operational burden and complexity involved in protecting sensitive data. For more information, see [Amazon DynamoDB Encryption at Rest](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html).

This table maps common security concerns to the corresponding controls and architectural best practices as documented in AWS’ public documentation, white papers, and blog posts. For additional AWS security, compliance, penetration testing, Security Bulletins, resources, etc, please visit [AWS Cloud Security](https://aws.amazon.com/security/) website.

| Security Need | AWS Control & Architectural Options | References |
| --- | --- | --- |
| Network Isolation | As a managed service, DynamoDB is protected by the AWS global network security procedures as described in the “Network Security” section of the [AWS Security Whitepaper](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) and in more detail in [compliance reports](https://aws.amazon.com/compliance/resources/) and 3rd party audit findings available to AWS customers.  While these APIs are callable from any network location, DynamoDB supports [resource-level](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/api-permissions-reference.html) and [item-level](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/specifying-conditions.html) access policies that can be applied to identities that have DynamoDB access. | [AWS Security Whitepaper](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf)  [AWS compliance reports](https://aws.amazon.com/compliance/resources/) |
| Inter-network traffic privacy (VPC to DynamoDB) | Amazon DynamoDB supports VPC endpoints. This means that DynamoDB can be provisioned as service within your AWS VPC. This means that resources within your VPC (e.g. EC2 instances) do not need to use publically available endpoints to reach DynamoDB.  By default when you create a VPC endpoint for DynamoDB, a default endpoint policy is attached to the endpoint. The default policy allows access by any user or service within the VPC, using credentials from any AWS account, to any DynamoDB resource. You can restrict this and lock down access to a subset of tables and API actions. An example of a locked down policy is shown below:  {  "Statement": [  {  "Sid": "AccessToSpecificTable",  "Principal": "\*",  "Action": [  "dynamodb:Batch\*",  "dynamodb:Delete\*",  "dynamodb:DescribeTable",  "dynamodb:GetItem",  "dynamodb:PutItem",  "dynamodb:Update\*"  ],  "Effect": "Allow",  "Resource": "arn:aws:dynamodb:*us-east-1*:*123456789012*:table/BobbyDropTables"  }  ]  }  There are additional restrictions that apply if you choose to use VPC endpoints for access to DynamoDB   * DynamoDB does not support resource-based policies (for example, on tables). Access to DynamoDB is controlled though the endpoint policy and IAM policies for individual IAM users and roles. * You cannot access Amazon DynamoDB Streams through a VPC endpoint. * Endpoints currently do not support cross-region requests—ensure that you create your endpoint in the same region as your DynamoDB tables. * If you use AWS CloudTrail to log DynamoDB operations, the log files contain the private IP address of the EC2 instance in the VPC and the endpoint ID for any actions performed through the endpoint. * The source IPv4 addresses from instances in your affected subnets change from public IPv4 addresses to the private IPv4 addresses from your VPC. An endpoint switches network routes, and disconnects open TCP connections. Your tasks are interrupted during the changeover, and any previous connections using public IPv4 addresses are not resumed. We recommend that you do not have any critical tasks running when you create or modify an endpoint; or that you test to ensure that your software can automatically reconnect to DynamoDB after the connection break. |  |
| Encryption of data at-rest | You can transparently encrypt data stored in Amazon DynamoDB in 15 regions (at time of publication), allowing you to protect your data. This feature makes use of KMS to provide a consistent experience. CMKs are not supported by this feature, however. If upon first use the service default key does not exist, one will be created for you. The following are encrypted:   * DynamoDB base tables * Local secondary indexes * Global secondary indexes   You can choose to use client side encryption to encrypt data before it is sent to DynamoDB. | [Amazon DynamoDB Encryption at Rest](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html) |

|  |  |  |
| --- | --- | --- |
| Encryption of data in-transit | When service clients use HTTPS to send data, Amazon DynamoDB encrypts data in-flight between clients which protects against someone eavesdropping on data items being transferred.  You may also make use of the DynamoDB Data Encryption Client to encrypt you payload before it’s transmitted to the service endpoint. | <https://docs.aws.amazon.com/dynamodb-encryption-client/latest/devguide/client-server-side.html> |
| Encryption Key Management | Where enabled, Amazon DynamoDB supports Server-Side Encryption using AWS Key Management Service (AWS KMS) to encrypt DynamoDB data items using the service default key. The key material for this key is managed by AWS; users of the service do not have access to it. | <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.howitworks.html> |
| Isolation of physical hosts | Amazon DynamoDB platform is a serverless platform that runs on shared tenancy, like other serverless platforms. |  |
| Restricting administrative access to certain individuals within the company | Administrative Access   * Use AWS Identity & Access Management (IAM) to create administrative users with appropriate permissions to Amazon DynamoDB * Alternatively, you can federate users from an on-premise (i.e. Microsoft Active Directory, or LDAP) to AWS IAM Roles   DynamoDB does not support resource based policies, administrative access is determined using IAM permissions only. | [IAM Best Practices](http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)  [Identify Federation in the AWS Cloud](https://aws.amazon.com/identity/federation/)  [Enabling Federation to AWS Using Windows Active Directory, ADFS, and SAML 2.0](https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/) |
| Authentication and authorization of corporate users via Active Directory for access to Amazon DynamoDB | You can federate users from an on-premise (i.e. Microsoft Active Directory, or LDAP) to AWS IAM Roles.  It is possible to restrict access at a very granular level to DynamoDB column and row level data, by using IAM policies: [Specifying Conditions](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/specifying-conditions.html). | [Identify Federation in the AWS Cloud](https://aws.amazon.com/identity/federation/)  [Enabling Federation to AWS Using Windows Active Directory, ADFS, and SAML 2.0](https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/) |
| Auditing of all Interactions with Amazon DynamoDB | Amazon DynamoDB is integrated with AWS CloudTrail, which captures API calls made by or on behalf of Streams and delivers the log files to the Amazon S3 bucket that you specify. The API calls can be made indirectly by using the console or directly by using the DynamoDB API. Using the information collected by CloudTrail, you can determine what request was made to DynamoDB, the source IP address from which the request was made, who made the request, when it was made, and so on.  CloudTrail currently logs the following API commands:   * [CreateBackup](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_CreateBackup.html) * [CreateGlobalTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_CreateGlobalTable.html) * [CreateTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_CreateTable.html) * [DeleteBackup](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DeleteBackup.html) * [DeleteTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DeleteTable.html) * [DescribeBackup](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DescribeBackup.html) * [DescribeContinuousBackups](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DescribeContinuousBackups.html) * [DescribeGlobalTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DescribeGlobalTable.html) * [DescribeLimits](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DescribeLimits.html) * [DescribeTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DescribeTable.html) * [DescribeTimeToLive](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_DescribeTimeToLive.html) * [ListBackups](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_ListBackups.html) * [ListTables](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_ListTables.html) * [ListTagsOfResource](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_ListTagsOfResource.html) * [ListGlobalTables](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_ListGlobalTables.html) * [RestoreTableFromBackup](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_RestoreTableFromBackup.html) * [TagResource](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_TagResource.html) * [UntagResource](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_UntagResource.html) * [UpdateGlobalTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_UpdateGlobalTable.html) * [UpdateTable](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_UpdateTable.html) * [UpdateTimeToLive](http://docs.aws.amazon.com/amazondynamodb/latest/APIReference/API_UpdateTimeToLive.html) * DescribeReservedCapacity * DescribeReservedCapacityOfferings * PurchaseReservedCapacityOfferings | [Working with CloudTrail Log Files](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-working-with-log-files.html)  [AWS CloudTrail User Guide](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/)  <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/logging-using-cloudtrail.html> |
| Compliance Framework reference material for Amazon DynamoDB | For compliance documents related to AWS please visit [AWS Artifact](https://aws.amazon.com/artifact/). | <https://aws.amazon.com/compliance/services-in-scope/> |
| Alerting and Incident Management | Any low-level API calls made to DynamoDB actions are tracked in log files. DynamoDB records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on a time period and file size.  Full details on the actions that are logged to CloudTrail by DynamoDB can be found here: [Logging DynamoDB Operations using CloudTrail](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/logging-using-cloudtrail.html)  If DDB tables are provisioned on behalf of users of tables, i.e. administrators of tables are different from the users, the following CloudTrail events should be monitored:  - DeleteTable  - DeleteBackup  - CreateTable  Users, Roles, and Groups with policies that have DynamoDB access restricted to a subset of tables & attributes should be monitored for changes that make them more permissive than before. | <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/logging-using-cloudtrail.html>  <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery_Howitworks.html> |
| Cross-region replication/key management. | DynamoDB supports Global Tables (multi-region/multi-master) in 6 regions (as of May 2018), which encrypts data at rest using the service default key for the region. The following regions are supported for GlobalTables - US East (N.Virginia & Ohio), US West (Oregon), Asia Pacific (Singapore), EU (Frankfurt), EU(Ireland) |  |
| Update/Patch/Hardening for Amazon DynamoDB | DynamoDB is a managed service and there are no components that can be patched or updated by the customer. |  |