MongoDB®

Configuring MongoDB Atlas for PROTECTED Information Classification Level

Details and technical references to help comply with Australian Government PROTECTED level requirements

September 2023

AU/NZ 1300 103 899 • info@mongodb.com.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

Table of Contents

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

Introduction

The purpose of this whitepaper is to provide details and technical references demonstrating how MongoDB customers, such as Federal Government Organisations and ISVs, can use MongoDB Atlas to comply with PROTECTED information classification level requirements.

What is MongoDB Atlas?

MongoDB Atlas is a multi-cloud database service built and run by the same people behind MongoDB. MongoDB Atlas simplifies deploying and managing your databases while offering the versatility you need to build resilient and performant global applications on the cloud provider(s) of your choice. MongoDB Atlas supports a wide range of use cases such as transactional workloads, time series data, full-text search, and petabyte data storage. MongoDB Atlas also includes all the capabilities and services to allow organisations to achieve PROTECTED information classification level for their applications. These capabilities include always-on authentication, authorization, encryption in transit and at rest, and no access to MongoDB deployments from the Internet by default. Additionally, MongoDB Atlas provides automated patching of the underlying infrastructure and MongoDB deployments with zero downtime. MongoDB Atlas is architected to provide automated database resilience and mitigate the downtime risks associated with hardware failures or unintended actions.

Achieve PROTECTED Information Classification Faster

The Australian Signals Directorate (ASD) Information Security Manual (ISM) has hundreds of controls for achieving PROTECTED level compliance. Configuring a self-managed environment in accordance with these controls can be a significant effort. MongoDB Atlas has strived to take the maximum burden of these requirements so customers can focus on application development and business requirements. Specifically, customers are only responsible for configuring a small subset of the total ISM controls to minimise effort. If you would like to request a copy of the Infosec Registered Assessors Program (IRAP) Cloud Security Assessment Report for MongoDB Atlas, please reach out to your MongoDB Account Team or contact the team here.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

Definitions

The following are terms that are used throughout this document. Any capitalised terms that are not defined in this document have the meaning described in your MongoDB Atlas Agreement.

1. **“Control Plane”** means the Atlas UI or API that users leverage to manage their MongoDB deployments.

2. **“Customer Data”** means any data you or your end users upload into the data plane of MongoDB Atlas.

3. **“Data Plane”** refers to your MongoDB Atlas database deployments and the access to the data within them.

4. **“MongoDB Atlas Deployment”** means each replica set or sharded cluster of data-bearing nodes running the MongoDB database software that is managed by MongoDB Atlas, subject to your selected configurations.

5. **“MongoDB Atlas Project”** is a container within the MongoDB Atlas platform that holds one or multiple MongoDB deployments and other resources in an organised and isolated manner.

6. **“MongoDB Atlas Organisation”** is a top-level management layer that manages and controls access to multiple Atlas projects and resources.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

MongoDB Atlas for PROTECTED Information Classification Level

Customer Responsibilities Table

This table outlines the IRAP controls under the applicable ISM guidelines along with relevant information and MongoDB links, highlighting the actions that your engineering team needs to take to achieve PROTECTED level compliance using MongoDB Atlas.

Guidelines for System Management - System Administration
You should consider system management activities when using MongoDB applications.
You are responsible for deploying your MongoDB Atlas Databases within Cloud Service Provider (CSP) data centres based on operational needs. Australian government agencies are recommended to deploy in Australian regions on their chosen CSP. IRAP assessed cloud provider regions within Australia supported by MongodB Atlas include: AWS: - Sydney Region (ap-southeast-2) - Melbourne Region (ap-southeast-4) Azure: - Canberra Region 1 (Australia Central) - Canberra Region 2 (Australia Central 2) - Sydney Region (Australia East) - Melbourne Region (Australia Southeast) GCP: - Sydney Region (Australia-southeast1) - Melbourne Region (Australia-southeast2)
You are responsible for authorising direct access to resources within your Atlas deployments for MongoDB personnel to perform maintenance and support activities.
You are responsible for creating and destroying Atlas deployments within your dedicated MongoDB Atlas Organisation.
Guidelines for System Hardening - Authentication hardening
You are responsible for the management of your MongoDB Atlas deployments and for ensuring you have appropriate controls in place relating to access to your systems and resources.
You can configure Federation Authentication using SAML for the control plane.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

You are responsible for enabling two-factor authentication for your account and configuring MFA for network access to non-privileged accounts.

You are responsible for disabling inactive accounts if you use MongoDB Federated Authentication.

You are responsible for configuring authentication for data plane users using supported authentication types:

- For human access to the data plane, we recommend that you use AWS-IAM or OpenID Connect.
- For programmatic access to the data plane, we recommend that you use SCRAM, X.509, or AWS-IAM.

Guidelines for Personnel Security - Access to systems and their resources

You are responsible for the management of your MongoDB Atlas deployments and for ensuring you have appropriate controls in place relating to access to your systems and resources.

You are responsible for managing user access and other account management activities for both the control plane and data plane:

For the control plane:

You are responsible for creating Project(s) to your Organisation(s) within Atlas and assigning Project and Organisation roles to teams.

You are responsible for creating Admin API keys and managing Atlas role assignment to these API keys.

For the data plane:

You are responsible for managing database users within a MongoDB Atlas Project and assigning them built-in or custom database roles for managing access to the stored data and the operations they can do to said data.

You are responsible for configuring users, rotating passwords, and implementing access controls on all instances of in-scope Atlas services in the Control and Data Plane. If you are using your own identity provider, you are responsible for configuring password reuse.

You can configure network connectivity to your Atlas database deployments via IP access lists, VPC peering, or Private Endpoints.

Guidelines for System Monitoring - Event logging and monitoring

You must consider system monitoring for their cloud tenancy where feasible.

Atlas monitors your deployment out-of-the-box. You are responsible for configuring your alerts to your organisations specifications. If you are using external tooling for monitoring your alerts, you must configure your account to send alerts for monitoring those different systems.

You are responsible for monitoring Project and Organisation Activity Feed and Database Access History as well as enabling fine-grained database auditing and ingesting the database audit logs into your SIEM via API.

Guidelines for System Management - Data backup and restoration

You should consider data backup and restore activities when using MongoDB Atlas.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

You are responsible for enabling cloud backups for your database deployments during cluster creation or during the modification of an existing cluster, configuring backup policies, including frequency intervals, and duration of the retention.

Optional Security Features Table

These are optional additional security configurations that are not needed for PROTECTED level compliance, but they provide an additional level of security for your Atlas deployments.

Guidelines for Cryptography - Cryptographic fundamentals
Atlas uses encrypted volumes at rest for customer MongoDB deployments. Atlas provides the ability to use a CSP KMS service (AWS, Azure or GCP) to encrypt and decrypt data stored in MongoDB's storage engine. The database storage engine encryption can be configured in addition to MongoDB Atlas' always-on volume encryption. MongoDB provides the optional ability to encrypt sensitive data fields in your application before you send it over the network to MongoDB using Client-Side Field Level Encryption (CSFLE) or Queryable Encryption (QE). With CSFLE or QE enabled, your MongoDB Atlas deployment does not have access to your data in an unencrypted form. Your employees (DBAs) also do not have access to the encrypted fields unless they have access to the encryption key.
Guidelines for System Management - Data backup and restoration
Atlas also supports an optional Backup Compliance Policy that can be tailored to meet organisational requirements. When you enable such a Policy, no Atlas Organization user, regardless of their role within your Atlas Organization, can modify the policy without MongoDB support involvement. You can download backups of your deployments into an S3 bucket that you manage. You can also configure your backups to be stored in a region other than the region of your deployment to support organisation data restoration and business continuity requirements.
Guidelines for System Management - System patching
System patching is inherited by MongoDB Atlas and the underlying cloud service providers, and MongoDB Atlas automatically patches all database deployments.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

However, you may set a maintenance window for when Atlas deploys patches to your deployments. Atlas performs maintenance automatically in a rolling manner to preserve continuous availability. Note: Atlas performs urgent maintenance activities such as security patches as soon as they are needed without regard to scheduled maintenance windows.

MongoDB Default Controls Table

This table provides information on inherited IRAP controls under the applicable ISM guidelines for PROTECTED level compliance. More detailed controls that are implemented by MongoDB can be found in our IRAP Cloud Security Assessment Report.

Guidelines for Cyber Security Roles
MongoDB is responsible for the implementation of this control, although, organisations should have their own cyber security roles effectively implemented.
Guidelines for Cyber Security Incidents
MongoDB is responsible for the implementation of this control. Organisations should ensure their incident response processes can integrate with MongoDB's policies and procedures. However, as per control **ISM-0140**, customers are responsible for reporting incidents to ACSC in alignment with their own incident response process.
Guidelines for Physical Security
Physical security controls for MongoDB are inherited from the underlying cloud service provider.
Guidelines for Communications Infrastructure - Cabling infrastructure
Cabling infrastructure controls for MongoDB are handled by the underlying cloud service provider.
Guidelines for ICT Equipment
ICT Equipment controls for MongoDB are handled by the underlying cloud service providers.
Guidelines for Media
Media security controls for MongoDB are handled by the underlying cloud service providers.
Guidelines for System Hardening - Operating system hardening

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

MongoDB is responsible for hardening the operating system on which customer Atlas deployments are run.
Only privileged users are present within the MongoDB production environment.
Media management controls are inherited from the cloud service provider.
Guidelines for System Hardening - Application hardening
MongoDB is responsible for hardening the control plane and data plane software as used by customers.
Guidelines for System Hardening - Virtualisation hardening
Virtualisation hardening is inherited by MongoDB Atlas' underlying cloud service providers.
Guidelines for System Hardening - System patching
System patching is inherited by MongoDB Atlas and the underlying cloud service providers.
Atlas performs urgent maintenance activities such as security patches as soon as they are needed.
Guidelines for System Hardening - Authentication hardening
MongoDB Atlas provides single sign-on (SSO) integration options with both control and data plane, which requires customer configuration.
The built-in MongoDB Atlas “Organisation Owner” role has the capability to require all MongoDB Atlas users within their Organisation to enable multi-factor authentication for their account.
Built-in and user-defined roles can be leveraged by application users.
MongoDB provides always-on role-based access controls (RBAC) with predefined roles for both the control and data plane. MongoDB provides the ability to create custom roles for the control plane and data plane.
Guidelines for Software Development
MongoDB develops the software in accordance with the IRAP guidelines.
Guidelines for Networking - Network design and configuration
MongoDB Atlas deployments are deployed in a dedicated VPC for an Atlas Project. This VPC is managed by MongoDB. This mechanism provides a level of network isolation among different tenants of Atlas.
All data communicated over MongoDB Atlas network infrastructure is encrypted with HTTPS/TLS.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.

Guidelines for Networking - Service continuity for online services
MongoDB is responsible for the service continuity of Atlas clusters in accordance with the service level agreement.
MongoDB leverages services offered by AWS, GCP and Azure for hosting the Atlas cloud service. Customers can select and configure their clusters to their choice of CSP and the CSP regions.
Guidelines for Cryptography
All data at rest is encrypted with AES-256 encryption on AWS, Azure and GCP server instances.

© 2023 MongoDB, Inc. MongoDB and the MongoDB leaf logo are registered trademarks of MongoDB, Inc.