MongoDB Ops Manager Interview Questions and Answers

# Section 1: Basic Level

* Q: What is MongoDB Ops Manager? How is it different from MongoDB Atlas?

A: Ops Manager is an on-premise management platform for MongoDB Enterprise, offering automation, monitoring, and backup. Atlas is a fully managed cloud DBaaS.

* Q: Which MongoDB editions support Ops Manager?

A: Ops Manager is supported only on MongoDB Enterprise Edition.

* Q: What are the core features of Ops Manager?

A: Core features include automation of deployments, performance monitoring, backup and point-in-time restore, alerting, and integration with enterprise security systems.

* Q: How do you install Ops Manager on-prem?

A: By downloading the Ops Manager package from MongoDB Enterprise downloads, installing required dependencies (MongoDB, backup daemon), and configuring the application using the config files.

* Q: What are the components of Ops Manager architecture?

A: Components include the Application Server, MongoDB backing databases (Ops Manager DBs), Automation Agents, Monitoring Agents, and Backup Daemons.

# Section 2: Intermediate Level

* Q: How does Ops Manager backup MongoDB data?

A: It uses continuous incremental backups stored in blockstore with optional snapshot creation. The head database tracks the latest backup metadata.

* Q: What are the types of backups Ops Manager supports?

A: Continuous backup and scheduled snapshot backups. PITR is available in continuous mode.

* Q: Explain how Ops Manager handles replica set failover.

A: Ops Manager can monitor replica set status and initiate elections, reconfigure secondaries, or alert admins depending on policies.

* Q: What is the role of Automation Agents?

A: Automation Agents apply configuration changes like version upgrades, user/role changes, or replica set/sharded cluster creation.

* Q: How do you upgrade MongoDB versions using Ops Manager?

A: By selecting the deployment, choosing the new version, and letting the Automation Agent perform a rolling upgrade.

# Section 3: Advanced Level

* Q: Explain the lifecycle of a backup in Ops Manager.

A: Backup begins with an initial sync, then Ops Manager takes continuous incremental snapshots using the backup daemon and stores changes in blockstore.

* Q: What is the role of the blockstore and head database in backups?

A: Blockstore stores compressed data blocks. The head DB stores metadata to map and track latest versions of backups.

* Q: How would you scale Ops Manager for 100+ MongoDB clusters?

A: By using high availability Ops Manager setup with dedicated backup daemons, sharded blockstore, and scaled MongoDB infrastructure for the Ops Manager databases.

* Q: Can Ops Manager be used in air-gapped environments?

A: Yes. Download all dependencies manually, use offline packages, and configure internal repositories for MongoDB binaries and Ops Manager agents.

* Q: Describe Ops Manager's internal MongoDB deployment.

A: It includes Ops Manager Application Database (App DB), Backup Daemon’s Head DB, and optionally, a separate blockstore instance for storing backup data.

# Section 4: Real-time Case Study Questions

* Q: You are managing a 3-node sharded cluster using Ops Manager. A backup job is failing continuously. How do you approach troubleshooting?

A: Check backup daemon logs, verify head DB and blockstore availability, confirm Ops Manager agent version compatibility, and inspect disk space and network errors.

* Q: Your Ops Manager UI is down. What are the immediate steps you will take?

A: Check if the MongoDB App DB is running, inspect Ops Manager logs (`/var/log/mongodb-mms`), restart services, and validate config files.

* Q: You need to perform a PITR restore to 1 hour ago for a sharded cluster. Walk through the steps.

A: Identify the cluster and timestamp, use the Ops Manager UI to select point-in-time, perform restore to staging or original cluster, validate data consistency.

* Q: Explain how you handled a major Ops Manager upgrade in production.

A: Prepared rollback plan, took full backup, upgraded one Ops Manager node at a time in HA setup, verified monitoring/backup post-upgrade, applied patches as needed.