Course Overview

View Discussion

Final Exam

## Question 6

Back to the Question

Let's take a moment to examine each of the choices:

- Internal authentication via X.509 certificates will enable MongoDB's role-based access control authorization system.

  This is true! Whether you use X.509 certificates or a shared keyfile, internal authentication automatically enabled authorization on MongoDB.

- The localhost exception applies to a replica set and sharded cluster environments.

  This is true! It does not matter if your `mongod` is standalone, an arbiter, or a secondary, if authorization is enabled and there are no users in the local database then the localhost exception applies. It is a best practice to create an administrative user on every `mongod` in your production environment. This will disable the localhost exception and in general will give you added security over your MongoDB deployment.

- Audit logs can go to one of four locations: the system log, the console, to another MongoDB member, or to a file.

  This is false. Audit logs can go to one of **three** locations: the system log, the console, or to a file.

- Encryption at rest is a four step process: generate a master key, generate keys for each database, encrypt each database with the database keys, and encrypt the database keys with the master key.

  This is true! It's important to keep in mind that the database keys are stored (encrypted) inside MongoDB. This is totally fine as long as you keep your master key safe and rotate it on a regular basis.

- When you enable encryption at rest, transport encryption between replicating members is automatically enabled.

  This is false! This answer makes no sense. Did SSL certificates magically appear on all of your servers? Of course not! If you'd like to utilize transport encryption you'll need to issue certificates and enable it.

Proceed to next section