



Course Overview



View Discussion

Final Exam

Question 7

[Back to the Question](#)

Let's look at each of these potential answers one by one:

- The subject of a client certificate acts as the "user" when authenticating with X.509 certificates.

This is true! Whenever we connect to a **mongod** over TLS the server will need to take a look at our certificate. When we authenticate the server will check the subject of the certificate that it has already verified against the subject you've provided.

- The **preferSSL** SSL mode allows the server to accept both TLS and non-TLS connections between *both* clients and other members.

This is false. The name of this command-line option argument isn't very descriptive, so it's important to remember what purpose it serves. The **preferSSL** SSL mode allows the server to accept both TLS and non-TLS connections from clients **but requires a TLS connection for members of the cluster**.

- When enabling internal authentication between the members of a replica set both certificate and key must be present in the CA, client, and server PEM files.

This is false. The client and server PEM files need to contain both the certificate and corresponding public key, but the CA PEM file need only contain the certificate of the certificate authority

- MongoDB stores user-defined role information in the **system.roles** collection in the **admin** database.

This is true! While it's unlikely (and generally not recommended) that you'll ever need to modify **system.roles** it's useful to know where this data exists from a backup/restore perspective.

- When auditing is enabled on MongoDB Enterprise, the **--auditFormat BSON** option has much better performance than the **--auditFormat JSON** option.

This is true! It takes more time than you'd think to serialize JSON to disk. BSON is already in a binary format, so it takes some extra CPU cycles to convert BSON to JSON.