6.5.2 Configure Role-Based Access Control

Create roles that define the exact access a set of users needs. Follow a principle of least privilege. Then create users and assign them only the roles they need to perform their operations. A user can be a person or a client application.

Create a user administrator first, then create additional users. Create a unique MongoDB user for each person and application that accesses the system.

See *Authorization* (page 324), *Create a Role* (page 388), *Create a User Administrator* (page 384), and *Add a User to a Database* (page 386).

6.5.3 Encrypt Communication

Configure MongoDB to use TLS/SSL for all incoming and outgoing connections. Use TLS/SSL to encrypt communication between `mongod` and `mongos` components of a MongoDB client as well as between all applications and MongoDB.

See *Configure mongod and mongos for TLS/SSL* (page 342).

6.5.4 Limit Network Exposure

Ensure that MongoDB runs in a trusted network environment and limit the interfaces on which MongoDB instances listen for incoming connections. Allow only trusted clients to access the network interfaces and ports on which MongoDB instances are available.

See the `bindIp` setting, and see *Configure Linux iptables Firewall for MongoDB* (page 335) and *Configure Windows netsh Firewall for MongoDB* (page 339).

6.5.5 Audit System Activity

Track access and changes to database configurations and data. MongoDB Enterprise[88] includes a system auditing facility that can record system events (e.g. user operations, connection events) on a MongoDB instance. These audit records permit forensic analysis and allow administrators to verify proper controls.

See *Auditing* (page 330) and *Configure System Events Auditing* (page 398).

6.5.6 Encrypt and Protect Data

Encrypt MongoDB data on each host using file-system, device, or physical encryption. Protect MongoDB data using file-system permissions. MongoDB data includes data files, configuration files, auditing logs, and key files.

6.5.7 Run MongoDB with a Dedicated User

Run MongoDB processes with a dedicated operating system user account. Ensure that the account has permissions to access data but no unnecessary permissions.

See *Install MongoDB* (page 5) for more information on running MongoDB.

[88] http://www.mongodb.com/products/mongodb-enterprise?jmp=docs