Confirm FIPS mode is running Check the server log file for a message FIPS is active:

```
FIPS 140-2 mode activated
```

6.3.2 Security Deployment Tutorials

The following tutorials provide information in deploying MongoDB using authentication and authorization.

Deploy Replica Set and Configure Authentication and Authorization **(page 353)** Configure a replica set that has authentication enabled.

Deploy Replica Set and Configure Authentication and Authorization

Overview

With *authentication* (page 320) enabled, MongoDB forces all clients to identify themselves before granting access to the server. *Authorization* (page 324), in turn, allows administrators to define and limit the resources and operations that a user can access. Using authentication and authorization is a key part of a complete security strategy.

All MongoDB deployments support authentication. By default, MongoDB does not require authorization checking. You can enforce authorization checking when deploying MongoDB, or on an existing deployment; however, you cannot enable authorization checking on a running deployment without downtime.

This tutorial provides a procedure for creating a MongoDB *replica set* (page 559) that uses the challenge-response authentication mechanism. The tutorial includes creation of a minimal authorization system to support basic operations.

Considerations

Authentication In this procedure, you will configure MongoDB using the default challenge-response authentication mechanism, using the `keyFile` to supply the password for *inter-process authentication* (page 323). The content of the key file is the shared secret used for all internal authentication.

All deployments that enforce authorization checking should have one *user administrator* user that can create new users and modify existing users. During this procedure you will create a user administrator that you will use to administer this deployment.

Architecture In a production, deploy each member of the replica set to its own machine and if possible bind to the standard MongoDB port of `27017`. Use the `bind_ip` option to ensure that MongoDB listens for connections from applications on configured addresses.

For a geographically distributed replica sets, ensure that the majority of the set's `mongod` instances reside in the primary site.

See *Replica Set Deployment Architectures* (page 572) for more information.

Connectivity Ensure that network traffic can pass between all members of the set and all clients in the network securely and efficiently. Consider the following:

- Establish a virtual private network. Ensure that your network topology routes all traffic between members within a single site over the local area network.
- Configure access control to prevent connections from unknown clients to the replica set.
- Configure networking and firewall rules so that incoming and outgoing packets are permitted only on the default MongoDB port and only from within your deployment.