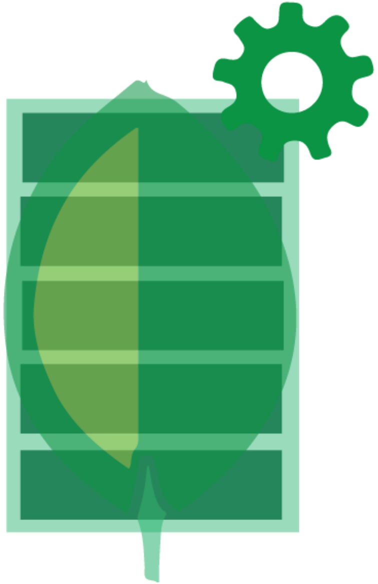


MODULE-8
PROJECT, ADDITIONAL CONCEPTS AND CASES STUDIES

Course Topics

→ Module 1
  - » Design Goals, Architecture and Installation

→ Module 2
  - » CRUD Operations

→ Module 3
  - » Schema Design and Data Modelling

→ Module 4
  - » Administration

→ Module 5
  - » Scalability and Availability

→ Module 6
  - » Indexing and Aggregation Framework

→ Module 7
  - » Application Engineering and MongoDB Tools

→ Module 8
  - » **Project, Additional Concepts and Case Studies**

Objectives

At the end of this module, you will be able to

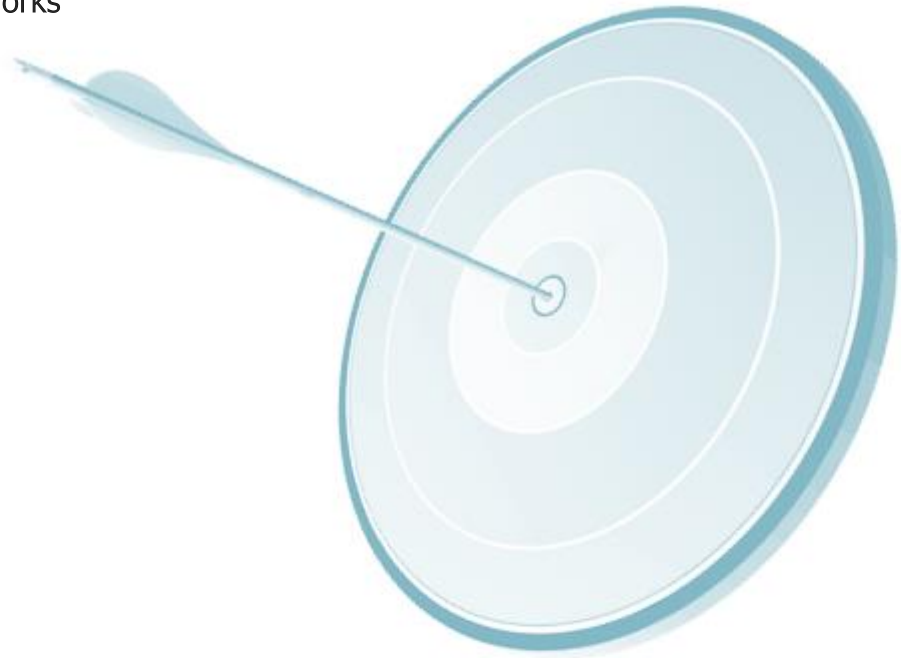
→ Know security concepts in MongoDB®

→ Understand how Authentication and Authorization works

→ Integrate MongoDB® with Java

→ Integrate MongoDB® with Jaspersoft

→ Apply MongoDB® in a real life project



Annie’s Question

What could be the maximum size of shard key?

Annie’s Answer

A shard key cannot exceed 512 bytes.

Annie's Question

Can we change the shard key after creating it?

Annie’s Answer

You cannot change a shard key after sharding the collection.

Annie's Question

Is Database name case sensitive in MongoDB ?

Annie’s Answer

Database names are case sensitive even if the underlying file system is case insensitive.
MongoDB does not permit database names that differ only by the case of the characters.

Annie’s Question

How to access MongoDB through browser?

Annie's Answer

http://localhost:28017/database_name/collection_name/

Annie's Question

What could be the maximum size of namespace in MongoDB?

Annie’s Answer

Namespace files can be no larger than 2047 megabytes. By default namespace files are 16 megabytes. You can configure the size using the nssize option.

Annie’s Question

What level of nesting of documents is possible in MongoDB?

Annie's Answer

MongoDB supports no more than 100 levels of nesting for BSON documents.

Annie’s Question

To use Rest API (HTTP protocol) we need to start database with which option?

--config

--replSet

--rest

Annie’s Answer

Ans: C (--rest)

Annie’s Question

In below list which one is responsible for metadata:
Shard Server
Replica Set
Config Server

Annie’s Answer

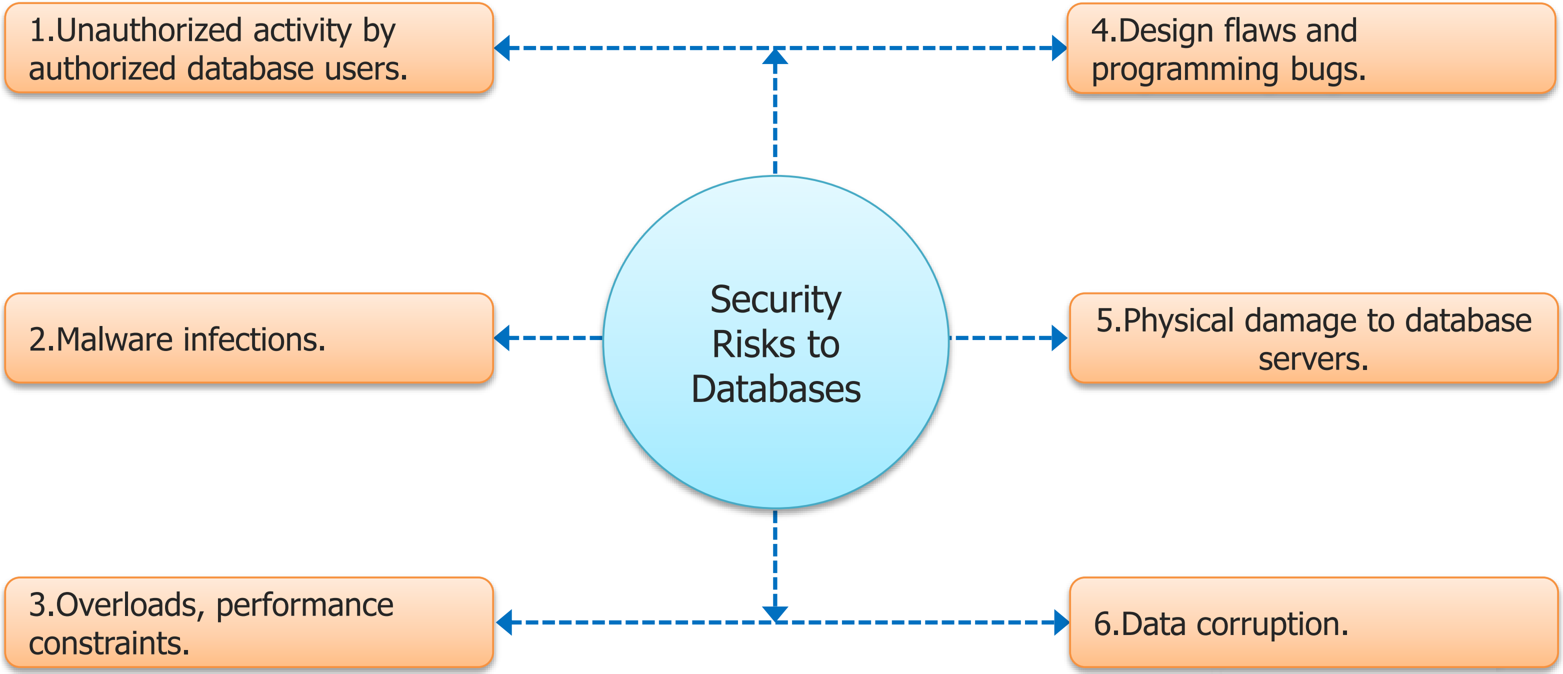
Ans: C- Config Server

MongoDB Security Introduction

- → Database security concerns the use of a broad range of information security controls to protect databases.
- → Security - Monitors all database activity, alerting and blocking any unauthorized behavior or database attacks.

Security Risks to Databases

edureka!



Security Risks to Databases

1.Unauthorized activity by authorized database users.

2.Malware infections.

3.Overloads, performance constraints.

4.Design flaws and programming bugs.

5.Physical damage to database servers.

6.Data corruption.

Security Risks to Databases (Contd.)

1. Unauthorized or unintended activity or misuse by authorized database users(DBA's, Network/systems managers) or by unauthorized users or hackers.

2. Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services.

3. Overloads, performance constraints and capacity issues resulting in the inability of authorized users to use databases as intended.

4. Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities, data loss/corruption, performance degradation etc.

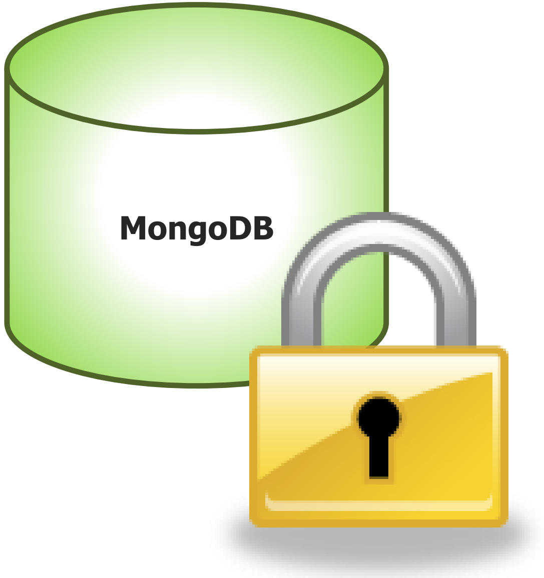
5. Physical damage to database servers caused by computer room fires or floods, overheating, lightning, accidental liquid spills, static discharge, electronic breakdowns/equipment failures and obsolescence.

6. Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage etc.

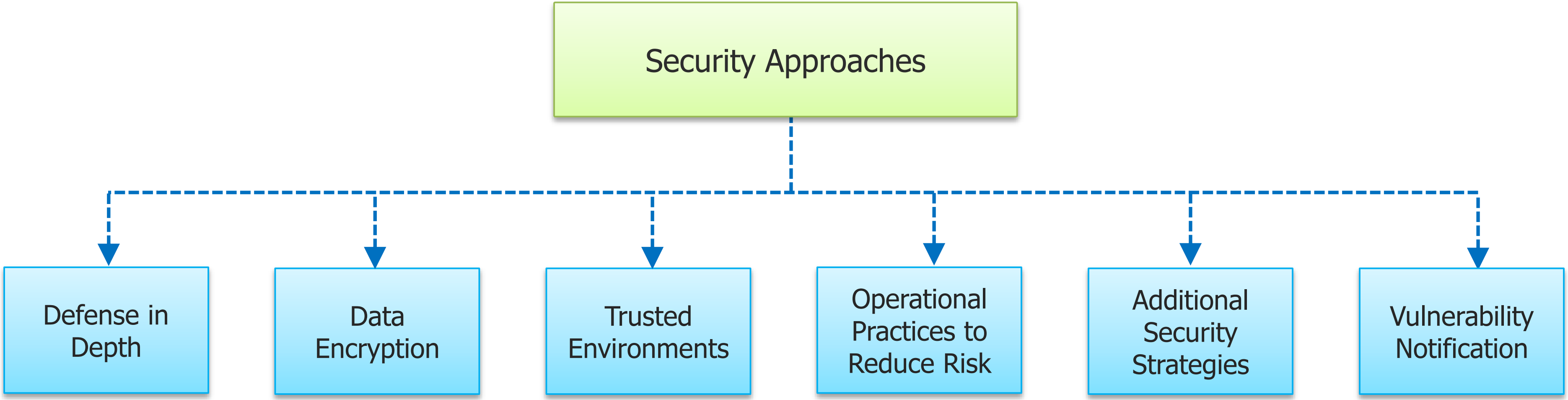
MongoDB Security Introduction

→ The intent of a Defense In Depth approach is to ensure there are no exploitable points of failure in your deployment that could allow an intruder or un-trusted party to access the data stored in the MongoDB database.

→ The easiest and most effective way to reduce the risk of exploitation is to run MongoDB in a trusted environment, limit access, follow a system of least privilege, and follow best development and deployment practices.



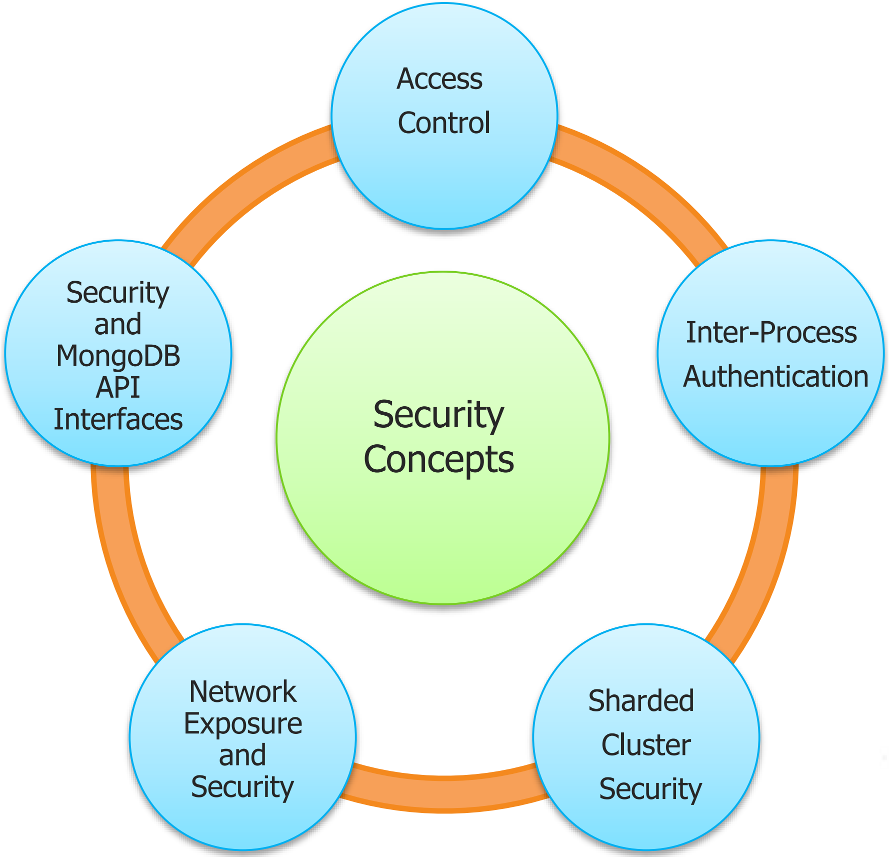
Security Approaches



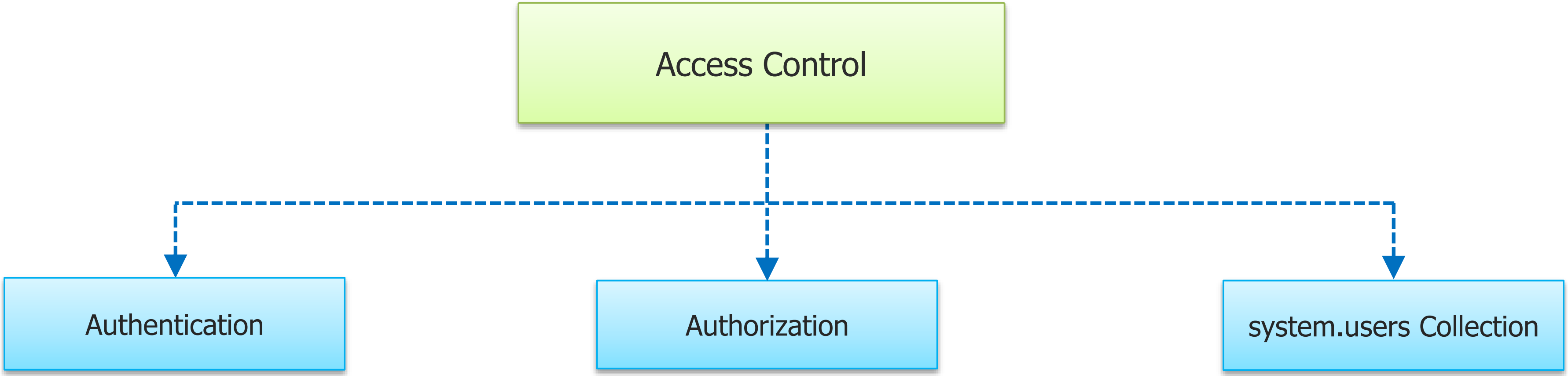
Security Approaches

- Defense in Depth
- Data Encryption
- Trusted Environments
- Operational Practices to Reduce Risk
- Additional Security Strategies
- Vulnerability Notification

Security Concepts


Access Control
Inter-Process Authentication
Sharded Cluster Security
Network Exposure and Security
Security and MongoDB API Interfaces
Security Concepts

Access Control



Authentication

→ MongoDB provisions authentication, or verification of the user identity, on a per-database level.

→ Authentication disables anonymous access to the database.

→ For basic authentication, MongoDB stores the user credentials in a database's system.users collection.

→ Authentication is disabled by default. To enable authentication for a given mongod or mongos instance, use the auth and keyFile configuration settings.

Authorization

→ MongoDB provisions authorization, or access to databases and operations, on a per-database level.

→ MongoDB uses a role-based approach to authorization, storing each user's roles in a privilege document in a database's system.users collection.

→ To assign roles to users, you must be a user with administrative role in the database.

System.users

→ A database’s system.users collection stores information for authentication and authorization to that database.

→ Specifically, the collection stores user credentials for authentication and user privilege information for authorization.

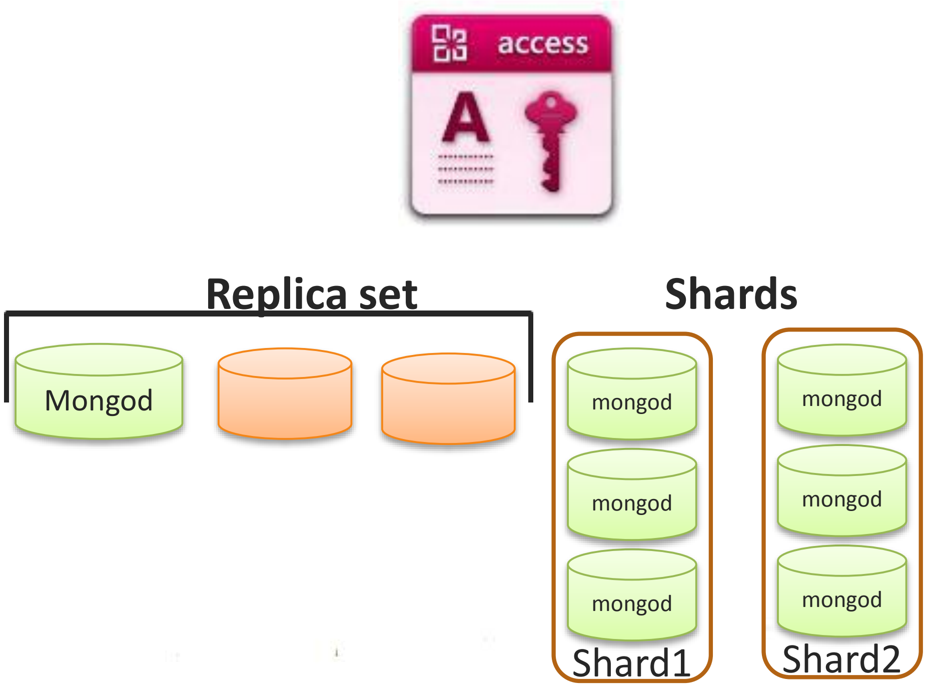
→ MongoDB requires authorization to access the system.users collection in order to prevent privilege escalation attacks.

→ To access the collection, you must have either userAdmin or userAdminAnyDatabase role.

Inter-Process Authentication

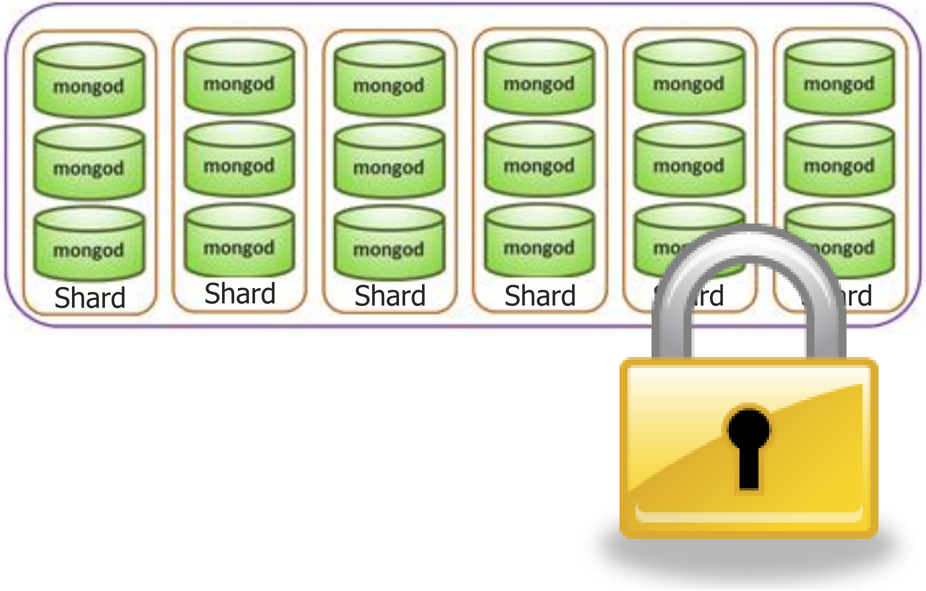
- → Your network configuration will allow every member of the replica set to contact every other member of the replica set.
- → If you use MongoDB's authentication system to limit access to your infrastructure, ensure that you configure a keyFile on all members to permit authentication.
- → Example of Intercrosses authentication is access of replica sets and shards

Example of Inter- Process authentication



Sharded Cluster Security

- → In most respects security for sharded clusters similar to other MongoDB deployments. However, there are additional considerations when using authentication with sharded clusters.
- → In sharded clusters, MongoDB provides separate administrative privileges for the sharded cluster and for each shard.
- → To access a sharded cluster as an authenticated user, from the command line, use the authentication options when connecting to a mongos.
- → Sharded clusters have restrictions on the use of localhost interface.



Network Exposure and Security

→ You can limit the network exposure with the following mongod and mongos configuration options: nohttpinterface, rest, bind_ip, and port.

→ You can use a configuration file to specify these settings.

→ The nohttpinterface setting for mongod and mongos instances disables the "home" status page, which would run on port 28017 by default. The status interface is read-only by default.

→ You may also specify this option on the command line as mongod --nohttpinterface or mongos --nohttpinterface.

→ Depending on configuration and implementation, VPNs provide for certificate validation and a choice of encryption protocols, which requires a rigorous level of authentication and identification of all clients.

For best results and to minimize overall exposure, ensure that only traffic from trusted sources can reach mongod and mongos instances can only connect to trusted outputs.

Security and MongoDB API Interfaces

→ The HTTP interface is always available on the port numbered 1000 greater than the primary mongod port. By default, the HTTP interface port is 28017, but is indirectly set using the port option which allows you to configure the primary mongod port.

→ The REST API to MongoDB provides additional information and write access on top of the HTTP Status interface. While the REST API does not provide any support for insert, update, or remove operations, it does provide administrative access, and its accessibility represents a vulnerability in a secure environment.

→ The REST interface is disabled by default, and is not recommended for production use.

If you must use the REST API, please control and limit access to the REST API. The REST API does not include any support for authentication, even when running with auth enabled.

MongoDB Security Hands-on

Hands On

Integration of MongoDB with Jaspersoft

Hands On

Integration of MongoDB with Java

Hands On

Certification Project

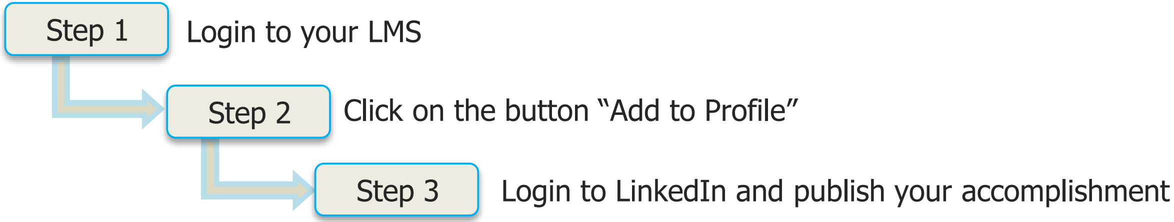
Hands On

Display edureka certification in your LinkedIn profile

edureka! and LinkedIn

→ You can now add your certification to your LinkedIn profile and enhance your career opportunities 10x times

→ The process of LinkedIn 'Add to Profile' cannot be simpler than this:



Step 1 Login to your LMS

Step 2 Click on the button "Add to Profile"

Step 3 Login to LinkedIn and publish your accomplishment

→ The in Add to profile button will get auto-enabled in your LMS post completion of your certification project

So, hurry up and complete your certification project!

Survey

Your feedback is important to us, be it a compliment, a suggestion or a complaint. It helps us to make the course better!

Please spare few seconds to take the survey after the webinar.

Thank you for being with Edureka!!

We would like to remind you that, your association with edureka does not stop here!

Remember

Lifetime Access

You have lifetime access to the courses you are registered for!

Lifetime Support

You get lifetime support for your courses

Free Additional Resources

You get free access to edureka! webinars for ALL courses

Discounts

You can get a discount on every next course you buy from edureka! For more details keep checking your LMS

Referrals

You are eligible for referral benefits. Earn when you refer anyone to edureka!

Please post all your reviews here: http://www.quora.com/Reviews-of-Edureka-online-education