mongoDB®

FOR **GIANT** IDEAS

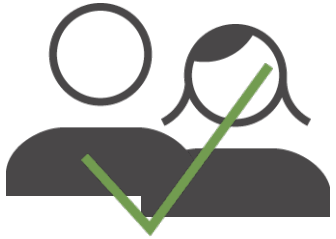
向赎金说不--MongoDB安全最佳实践

目录

- 数据库安全相关基本概念
- MongoDB安全最佳实践
- MongoDB安全资料汇总

数据库安全基本概念

验证 Authentication ：确认这个人到底谁



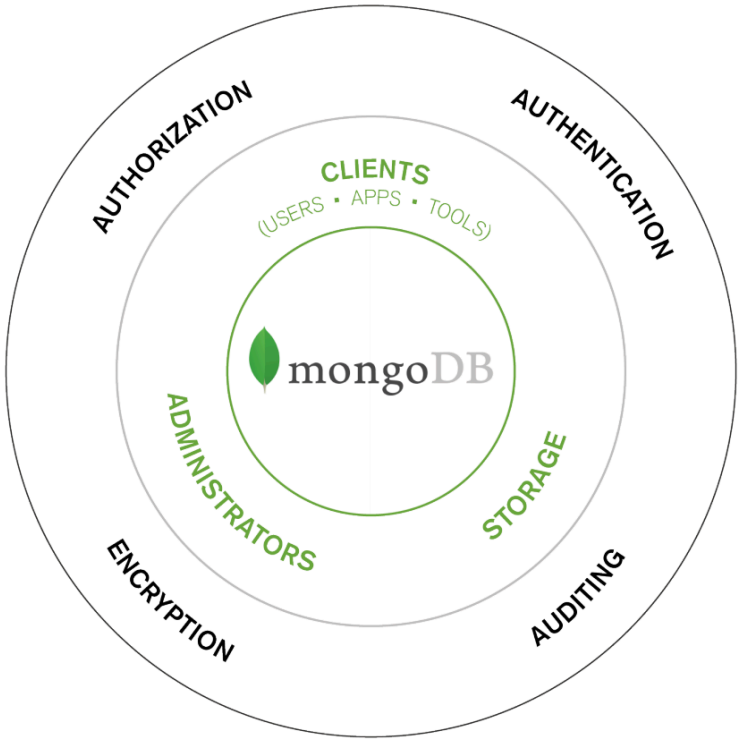
授权 Authorization ：确认这个人该干什么

数据库安全基本概念

审计 Authentication ：记录系统发生了什么

加密 Authorization ：只有授权用户才能理解

MongoDB的安全最佳实践：安全架构



认证管理：通过访问控制和授权管理，防止非授权访问

数据加密：通过数据存储和传输加密，保证数据安全

操作审计：通过操作记录，提供完整操作审计与分析

环境加固：通过操作系统和网络加固，保护数据库安全

MongoDB的认证管理：用户认证

- **MongoDB支持以下四种用户认证**
  - MongoDB自建用户认证
    - 用户名、密码认证
    - x.509证书文件认证
  - 与企业内部认证系统集成
    - LDAP（企业版支持）
    - Kerberos（企业版支持）

MongoDB的认证管理：用户基础认证

■ 户名、密码认证，配置方式

1. 启用用户认证
   - 命令行方式: mongod **--auth** --port 27017 --dbpath /data/db1
   - 配置文件方式

```
security:
 authorization: enabled
```

2. 通过本机（localhost）连接并创建“用户管理员”

```
use admin
db.createUser( {
        user: "myUserAdmin", pwd: "abc123",
         roles: [ { role: "userAdminAnyDatabase", db: "admin" } ]
         } )
```

3. 通过“用户管理员”，创建其他用户

```
mongo --port 27017 -u "myUserAdmin" -p "abc123" --authenticationDatabase "admin”
use test
db.createUser( {
        user: "myTester", pwd: "xyz123",
        roles: [ { role: "readWrite", db: "test" }, { role: "read", db: "reporting" } ] } )
         } )
```

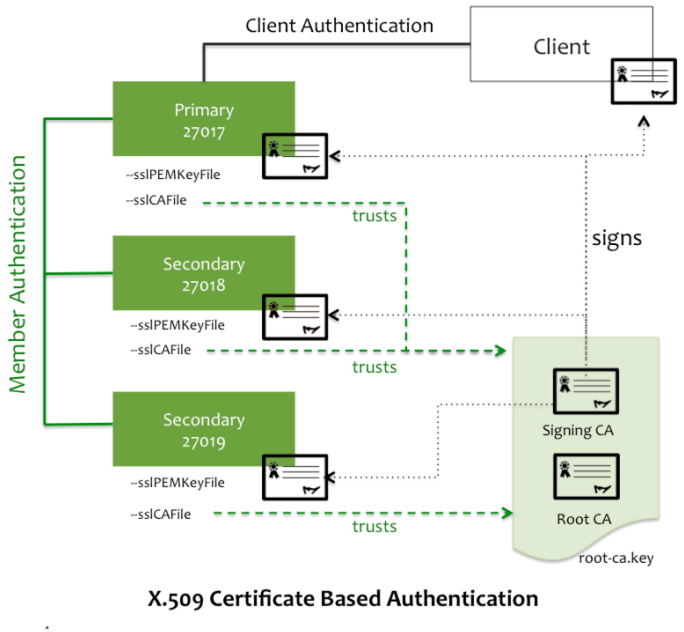
4. 使用用户口令登录

```
mongo --port 27017 -u "myTester" -p "xyz123" --authenticationDatabase "test"
```

MongoDB的认证管理：节点间认证

- x.509证书文件，配置方式

认证分为两种：客户认证和节点间认证



X.509 Certificate Based Authentication

x.509配置过程： https://www.mongodb.com/blog/post/secure-mongodb-with-x-509-authentication

MongoDB的数据加密：传输加密

- 启用TLS/SSL加密传输保证网络传输安全

1. 创建或者获得认证文件

```
openssl req -newkey rsa:2048 -new -x509 -days 365 -nodes -out mongodb-cert.crt -keyout mongodb-cert.key

cat mongodb-cert.key mongodb-cert.crt > mongodb.pem
```

2. 使用SSL参数启动mongod或者mongos

```
命令行方式：mongod --sslMode requireSSL --sslPEMKeyFile /etc/ssl/mongodb.pem
配置文件方式：net:
                    ssl:
                    mode: requireSSL
                    PEMKeyFile: /etc/ssl/mongodb.pem
```

3. 创建客户端认证文件

```
openssl req -new -x509 -days 365 -out client-cert.crt -keyout client-cert.key

cat client-cert.key client-cert.crt > client.pem
```

4. 使用客户端连接

```
mongo --ssl --sslCAFile ./mongodb.pem --sslPEMKeyFile ./client.pem --sslPEMKeyPassword yourpassword
```

MongoDB的数据加密：存储加密

- MongoDB企业版支持存储数据加密，加密需采用WT作为存储引擎

  mongod --enableEncryption --encryptionKeyFile mongodb-keyfile

- 不管是否使用数据存储加密，在操作系统上都应注意如下事项
  - 不要将数据文件放在共享文件系统上
  - 严格控制数据文件的访问权限

存储加密配置过程： https://docs.mongodb.com/manual/tutorial/configure-encryption/

MongoDB的操作审计

- MongoDB企业版支持操作审计，审计支持以下操作
  - 数据schema (DDL),
  - 部署架构
  - 用户认证与授权
  - 数据操作CRUD

```
$ mongod --dbpath data/db --auditDestination file --auditFormat JSON --auditPath
data/db/auditLog.json
```

- 可以通过“filter”指定你希望审计的操作

```
mongod --dbpath data/db --auditDestination file --auditFilter '{ atype: { $in:
[ "createCollection", "dropCollection" ] } }' --auditFormat BSON --auditPath
data/db/auditLog.bson
```

审计配置文档： https://docs.mongodb.com/manual/tutorial/configure-auditing/

审计过滤配置：https://docs.mongodb.com/manual/tutorial/configure-audit-filters/

MongoDB的安全加固

- MongoDB的服务器安全加固
  - 关闭http接口 ： net.http.enabled = False net.http.JSONPEnabled = False
  - 管理Rest API 接口： net.http.RESTInterfaceEnabled = False
  - 监听的IP地址：net.bindIp = 127.0.0.1,172.16.1.154
  - 使用普通用户，而非root运行MongoDB
- MongoDB的网络安全
  - MongoDB服务不应该直接暴露在互联网上，在云中部署，可应使用VPC
  - 修改默认监听端口：27017

审计配置文档： https://docs.mongodb.com/manual/tutorial/configure-auditing/

审计过滤配置：https://docs.mongodb.com/manual/tutorial/configure-audit-filters/

MongoDB的备份方式

- 完整备份是灾难恢复的最有效手段

备份方法	适合场景	使用限制
mongodump	适合少量数据，	不备份索引，导入时索引重建 不适合大数据量，不支持增量， 不适合分片环境
文件系统备份	使用LVM， 备份和恢复速度快， 适用复制集环境	需要确保数据无写入， 不适合分片环境， 不支持恢复到特定时间点
Ops Manager（企业版）	适用于大数量 适用于复制集环境和分片环境 支持恢复到特定时间点	对少量数据的简单环境而言，部署复杂

MongoDB安全文档汇总

- MongoDB安全白皮书：

  https://www.mongodb.com/collateral/mongodb-security-architecture

- MongoDB安全功能文档汇总

  https://docs.mongodb.com/manual/security/

- 安全检查列表：

  https://docs.mongodb.com/manual/administration/security-checklist/

- MongoDB在线安全培训：
  https://university.mongodb.com/courses/M310/about?_ga=1.242843265.269738533.1484482524

Q&A