# 钓鱼城安全基线项目

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

# MongoDB 安全基线开源版

# V1.00

# 钓鱼城安全基线项目

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

## 目　　录

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

## 修订历史

| 版本号 | 变更 | 贡献者 | 日期 |
| --- | --- | --- | --- |
| V1.00 | 初始版本V1. 00编写。 | taosec | 2019.3.18 |
| | | | |

# 钓鱼城安全基线项目

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

## 1.项目目标

对MongoDB的安全基线配置进行研究，修改出厂不安全缺省设置，消除缺省设置带来的安全隐患，有效保护数据安全和控制数据安全风险。

## 2.目标读者

MongoDB数据库管理员、安全工程师等。

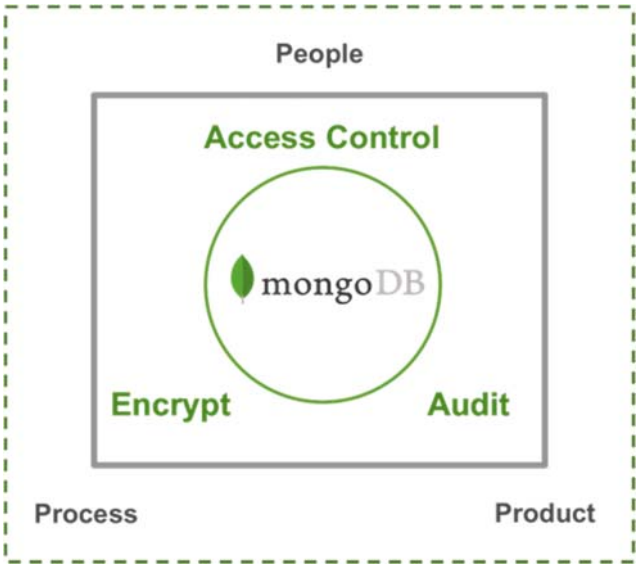
## 3.项目描述

研究开发系列安全基线，提高和加强相关系统的技术防护水平。

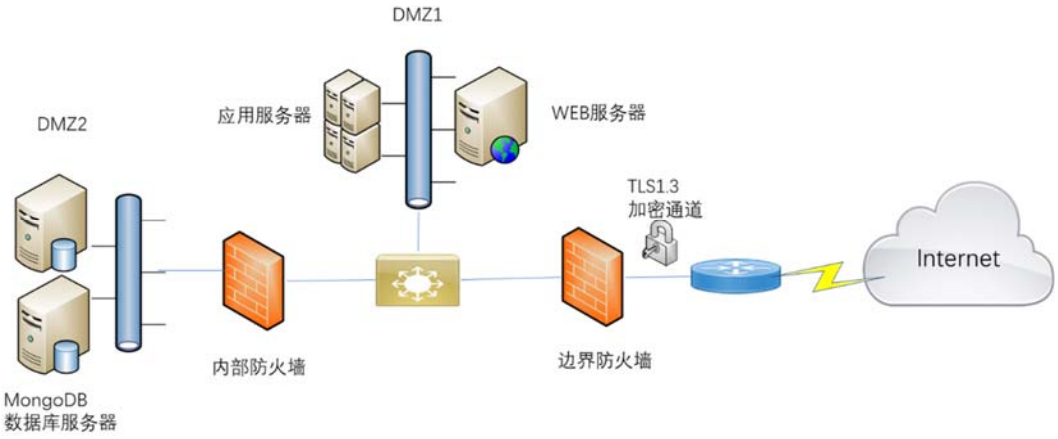
北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

## 4.端到端安全架构设计

MongoDB端到端安全架构设计如下图所示，从人员、过程和产品（技术）三个维度进行纵深安全体系防护，分别通过访问控制、加密和审计来实施。




网络安全架构部署参照下图，通过两层防火墙将WEB/应用服务器和MongoDB数据库服务器分别隔离在不同的两个DMZ类进行网络区域隔离和分层网络访问控制，数据库服务器通过防火墙访问规则控制只能由DMZ1区域内的应用服务器访问，避免了将其直接暴露给互联网的安全风险问题。



北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

## 5. 软件/补丁安装升级和运行

### 5.1. 将数据库服务器软件和安全补丁安装和升级到最新版本

版本号检查：

```
➢  db.version()
```

升级安装步骤：

1. 备份MangoDB数据库；
2. 从MangoDB官网下载最新版软件并检查下载文件数字签名无误；
3. 关闭MangoDB数据库实例；
4. 安装软件或将解包后二进制文件替换旧版本运行程序；
5. 重启MongoDB数据库实例。

### 5.2. 将数据库服务器进程以指定非特权用户的服务账号运行

当前所有数据库实例进程号和进程属主检查：

```
ps -ef | grep -E "mongos|mongod"
```

配置步骤：

1. 为运行MongoDB创建一个单独用户组和用户账号，例如mongodb:mongodb；
2. 将所有的数据库数据文件、密钥文件、SSL私钥文件设置为仅该用户可读；
3. 将日志文件设置为仅该用户可写和仅root用户可读。

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

# 6. 身份认证

## 6.1. 启用身份认证功能

身份认证功能状态检查：

```
cat /etc/mongod.conf | grep “Auth=”
```

如果身份认证功能已启用，则Auth的设置值为“True”。

激活身份认证功能步骤：

1. 启动未激活身份认证功能的MongoDB数据库实例；

```
mongod --port 27017 --dbpath /data/db1
```

2. 创建数据库系统管理员用户，并确保设置的口令符合组织口令策略的要求；

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

3. 重启已激活身份认证功能的MongoDB数据库实例。

```
mongod --auth --config /etc/mongod.conf
```

## 6.2. 禁用MongoDB通过localhost例外绕过身份认证功能

localhost例外状态检查：

```
cat /etc/mongod.conf |grep “enableLocalhostAuthBypass”
```

如果localhost例外绕过身份认证功能已经被禁用的话，
enableLocalhostAuthBypass的值应为0（false）。

禁用通过localhost例外绕过身份认证功能，将enableLocalhostAuthBypass的值设置为false。

```
  setParameter:
    enableLocalhostAuthBypass: false
```

## 7. 访问控制

### 7.1. 启用基于角色的访问控制

使用如下命令连接到MongoDB数据库实例，

```
mongo --port 27017 -u <siteUserAdmin> -p <password> --authenticationDatabase <database name>
```

```
> db.getUser()
> db.getRole()
```

识别并检查每个用户是否被适当地分配了相应的角色。

数据库用户角色设置：
（1）为MongoDB创建角色；
（2）为每个角色分配相应的权限；
（3）为每个角色分配相应的用户；
（4）移除为用户单独分配的权限。

### 7.2. 确保MongoDB数据库实例只在授权的接口上侦听网络连接

当前数据库实例网络侦听状态检查：
（1）检查MongoDB配置文件；

```
cat /etc/mongod.conf |grep –A12 “net” | grep “bindIp“
```

（2）检查相关网络访问控制设置。

```
iptables –L
```

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

当前数据库实例网络侦听配置：

配置数据库实例侦听在指定网络接口并用防火墙规则进行严格访问控制，应只允许DMZ区域里的应用服务器连接，下面以主机防火墙iptables示例配置如下。

```
iptables -A INPUT -s <ip-address> -p tcp --destination-port 27017 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -d <ip-address> -p tcp --source-port 27017 -m state --state
ESTABLISHED -j ACCEPT
```

## 8. 数据加密

### 8.1. 确保在所有的网络连接上启用了TLS协议

当前网络连接状态检查：

```
mongos --config /etc/mongos.conf
cat /etc/mongos.conf | grep –A20 'net' | grep –A10 'ssl' | grep 'mode'
```

mongod and mongos TLS证书和密钥配置：

```
net:
   ssl:
      mode: requireSSL
      PEMKeyFile: /etc/ssl/mongodb.pem
systemLog:
   destination: file
   path: "/var/log/mongodb/mongod.log"
   logAppend: true
storage:
   dbPath: "/var/lib/mongodb"
processManagement:
   fork: true
net:
   bindIp: localhost,mongodb0.example.net
port: 27017
```

### 8.2. 禁用HTTP明文协议接口

当前HTTP协议接口状态检查：

```
cat /etc/mongod.conf |grep “nohttpinterface” nohttpinterface = False
```

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

禁用HTTP协议接口：

将/etc/mongod.conf文件中的nohttpinterface选项设置为True。

# 9. 审计

## 9.1. 激活数据库审计功能

当前数据库审计功能状态检查:

```
cat /etc/mongod.conf |grep –A4 “auditLog” | grep “destination”
```

启用数据库日志审计功能并将其发送到syslog服务器:

```
mongod --dbpath data/db --auditDestination syslog
```

## 9.2. 关闭数据库日志静默模式

当前数据库日志静默模式状态检查:

```
cat /etc/mongod.conf |grep “SystemLog.quiet”
```

禁用数据库日志静默模式：

在/etc/mongod.conf 文件将SystemLog.quiet 选项设置为False来禁用日志静默模式。

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

# 10. 术语

**访问控制**

确保对资产的访问是基于业务和安全要求进行授权和限制的手段。

**证书**

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

**数字证书**

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

**加密**

通过一种密码算法产生密文的（可逆的）数据转换，即隐藏数据的信息内容。

**暴露**

特定的攻击利用数据处理系统特定的脆弱性的可能性。

**防火墙**

设置在网络环境之间的一种安全屏障。它由一台专用设备或若干组件和技术的组合组成。从一个网络环境到另一个网络环境的，以及反向的，所有通信流均通过此安全屏障，只有按照本地安全策略定义的、已授权的通信流才允许通过。

**密钥**

控制密码变换（如加密、解密、密码校验函数计算、签名生成或签名验证）运算的符号序列。

**口令**

用于实体鉴别的秘密的字、短语、数字或字符序列，是一个被默记的弱秘密。

**明文**

未加密的信息。

北京量子时空信息安全科技公司
钓鱼城安全研究中心
info@quantumsec.cn
www.quantumsec.cn

**端口**

注1：在互联网协议的语境下，端口是TCP（传输控制协议）连接或UDP（用户数据报协议）消息的逻辑信道端点。基于TCP或UDP的应用协议通常被分配默认端口号，例如，HTTP（超文本传输协议）的端口80。

**私有密钥**

一个实体的非对称密钥对中只能由该实体使用且被秘密保存的密钥。

**公开密钥/公钥**

一个实体的非对称密钥对中通常可以在不损害安全的情况下公开使用的密钥。

注1：在非对称签名系统中，公开密钥定义验证变换；在非对称加密系统中，公开密钥定义加密变换。密钥是“公开的”并不意味着任何人都可以获得。密钥可能只被某个事先确定的团体所拥有。

**安全套接层**

一种处于网络层与应用层之间，提供客户端和服务器的鉴别及保密性和完整性服务的协议。

**安全架构**

由多个安全的模块构成的一个相互协作的体系结构。

**安全审计**

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

**传输层安全协议**

一种作为安全套接层协议的后继的正式互联网协议。