【应用安全】浅谈 LINUX 系统 MONGODB 安全配置

文/EmmaDai

0x00 MongoDB 应用介绍

MongoDB 是一个基于分布式文件存储的数据库。由 C++语言编写。旨在为 WEB 应用提供可扩展的高性能数据存储解决方案。MongoDB 是一个介于关系数据库和非关系数据库之间的产品，是非关系数据库当中功能最丰富，最像关系数据库的。他支持的数据结构非常松散，是类似 json 的 bson 格式，因此可以存储比较复杂的数据类型。

0x01 为什么要做安全配置

MongoDB 数据库存在因为安全配置不合适导致的安全问题，例如，mongodb 的 REST 接口提供一个 web 界面访问，如果启用该接口，管理员可以用浏览器远程控制数据库，如果该接口被攻击者利用可直接远程控制数据库，并通过存储型 XSS 和 CSRF 的漏洞对获取更多的敏感信息。因此做好 MongoDB 的安全配置同样也十分的重要，本次主要对 MongoDB 3.0 以上版本的安全配置进行讨论。MongoDB 3.0 以上版本配置文件支持两种格式，以下加固方法将同时介绍两种方法或在启动参数上进行配置。

0x02 如何进行安全配置

1. 安装最新的安全补丁

MongoDB 应安装最新补丁进行升级，以防止漏洞被攻击者利用。MongoDB 3.0 以上版本在安全权限访问控制上和 MongoDB 2.0-2.8 版本相比，有所改进提升，因此建议使用 MongoDB 3.0 以上版本。

加固方法：
升级 MongoDB 到官方最新版。

2. 2.MongoDB 数据库启用认证

在所有人访问 MongoDB 服务器之前应该完成配置验证机制。此设置确保所有客户端，用户和服务器在被授予访问 MongoDB 数据库权限之前都需要进行身份验证。

加固方法：
a.在 mongod.conf 文件中应设置
security:
    authorization: enabled
或配置：
auth=true
b.设置启动参数--auth

3. MongoDB 仅在授权接口上监听网络连接

确保 MongoDB 在受信任的网络环境中运行包括限制网络接口上 MongoDB 实例监听传入的连接。 任何不受信任的网络连接都应该被 MongoDB 删除。

加固方法：

mongod.conf 文件中是否设置 bindIP，并且 bindIP 不为 0.0.0.0。

4. MongoDB 使用非特权专用服务帐户运行

MongoDB 服务不应该使用特权帐户运行，例如 root 权限，因为这会不必要地使操作系统面临高风险。

加固方法：
创建一个用于执行 MongoDB 数据库活动的专用用户，并使用该用户启动 MongoDB。

5. 禁止通过 HTTP 接口进行 JSONP 访问

net.http.JSONPEnabled 参数用于通过 HTTP 接口启用或禁用 JSONP 访问。 即使启用 HTTP 接口的参数设置为禁用，启用此参数也会启用 HTTP 接口。

加固方法：
mongod.conf 文件中应配置
net:
  http:
    JSONPEnabled: false
或配置：
jsonp=false

6. 禁用 REST 接口

net.http.RESTInterfaceEnabled 参数用于启用或禁用 REST API。 即使启用 HTTP 接口的参数设置为禁用，启用此参数也会启用 HTTP 接口。

加固方法：
mongod.conf 文件中应配置
net:
  http:
    RESTInterfaceEnabled: false
或配置：
rest=false

7. 禁用 HTTP 接口

net.http.enabled 参数用于启用或禁用 HTTP 接口，应禁用改接口。

加固方法：
mongod.conf 文件中应配置
net:
  http:
    enabled: false
或配置：
httpinterface=false

8. 配置正确审计过滤器

MongoDB Enterprise 支持各种操作的审计。默认情况下开启，审计工具将记录所有能够审计的操作，包含详细的事件操作，详细信息和结果。指定要记录的事件，审计的特征包括--auditFilter 选项。此检查仅适用于企业版本。

加固方法：
a.mongod.conf 文件中应配置
auditLog：
  filter：（根据企业要求进行配置）
b.设置启动参数：--auditFilter

9. 系统活动应被审计

跟踪对数据库配置和数据的访问和修改。 MongoDB Enterprise 包含一个系统审计工具，可以记录 MongoDB 实例上的系统事件（例如用户操作，连接事件）。 这些审计记录允许进行取证分析，并允许管理员验证适当的控制。

加固方法：
a.mongod.conf 文件中应配置
auditLog:
   destination: syslog\console\file
b.设置启动参数：--auditDestination

10. 禁用服务端脚本

MongoDB 支持一些服务器端操作执行 JavaScript 代码：mapReduce，group 和$ where。如果您不使用这些操作，应禁用服务器端脚本。

加固方法：
a.mongod.conf 文件中应设置为
security:
  javascriptEnabled: false
或配置：
noscripting = false。
b.设置启动参数：--noscripting

11. 将新条目追加到日志文件的末尾

当 MongoDB 实例重新启动时，默认情况下，新的日志记录将覆盖旧的记录之后重启的 mongod 或 Mongols 服务。使 systemlog.logappend 设置导致新的记录被添加到日志文件的末尾而不是重写日志的现有内容。

加固方法：
mongod.conf 文件中应配置：
systemLog:
  logAppend: true
或配置：
logappend=true

12. 设置正确的数据库文件权限

MongoDB 数据库文件需要设置文件权限进行保护。

加固方法：
MongoDB 数据库文件权限应为 660，所属用户应为 mongodb，所属组应为 mongodb。

13. MongoDB 使用非默认端口

更改 MongoDB 使用的端口使得攻击者难以找到数据库并将其定位。

加固方法：
将 MongoDB 服务器的端口更改为 27017 以外的端口。

0x03 总结

对 MongoDB 进行安全配置可以有效的防范一些常见安全问题，按照基线标准做好安全配置能够减少安全事件的发生。国内常见的基线标准有中国信息安全等级保护，美国 CIS 基线也有详细的 MongoDB 基线标准，不同的企业也可以根据自身企业业务制定符合自己企业的安全基线标准。

0x04 参考链接

- 国家信息安全等级保护制度要求

CIS_MongoDB_Benchmark_v1.0.0