Mysql优化建议

> **阅读须知**
>
> 本文档仅提供mysql的相关优化建议，请根据实际部署环境，进行参考配置或忽略。
>
> 修改mysql数据库配置文件，需要重启数据库，请谨慎操作。
>
> 所有修改操作前，建议提前备份相关文件，避免出现问题。

1、、禁用local-infile选项

详细信息：禁用local-infile选项会降低攻击者通过SQL注入漏洞读取敏感文件的能力。

处理方法：

编辑mysql配置文件<conf_path>/my.cnf，在[mysqld]段楼中配置local-infile的参数为0，并重启mysql数据库。

```
local-infile=0
```

2、禁用symbolic-links选项

详细信息：禁用符号链接以防各种安全风险。

处理方法：

编辑mysql配置文件<conf_path>/my.cnf，在mysqld段楼中配置 symbolic-link=0 ，5.6版本以上应该配置为 skip_symbolic_links=yes ，并重启mysql服务

3、避免使用熟知端口，降低初级扫描的风险

详细信息：避免使用熟知端口，降低初级扫描的风险

处理方法：编辑mysql配置文件<conf_path>/my.cnf，在mysqld段楼中设置新的端口参数，并重启mysql服务。

```
port=3506
```

4、确保用户没有使用通配符主机名

详细信息：避免在主机名中使用通配符，有助于限制连接数据库的客户端，否则服务就开放到公网上了。

处理方法：执行SQL更新语句，为每个用户指定允许连接的host范围：

①登陆数据库，执行

```
use mysql;
```

②执行语句，查看Host为通配符的用户

```
select user,Host from user where Host='%';
```

③删除用户或者修改用户HOST字段，删除语句(请谨慎执行该语句)：

```
DROP USER 'user_name'@'%';
```

更新用户语句(请谨慎执行该语句)：

```
update user set host=<New_Host> where host='%';
```

④执行语句

```
OPTIMIZE TABLE user;

flush privileges;
```