Redis 可以禁用的高危命令

作者：zeekling
原文链接：https://ld246.com/article/1672565410803
来源网站：链滴

高危命令禁用

redis一款高并发的内存K-V数据库，提供了好多命令，但是其中有部分对于生产环境来说比较危险，要禁用掉。

keys 命令

keys 命令执行的时候是需要进行全库扫描的，因为redis执行的主线程是串行的，所以会导致其他命也执行慢，从而拖垮整个redis实例。

flushdb、flushall 命令

flushdb、flushall是清空redis数据库里面数据的命令，禁用原因：

- 清空数据之后，开启RDB持久化一般无法恢复了，需要开启AOF持久化才有可能恢复数据。
- 清空数据的操作本身耗时比较长，当数据量大的时候容易扩跨整个redis实例。

config 命令

config命令可以直接修改redis加载到内存里面的配置信息，个人觉得主要是一些关键配置，比如：di 、dbfilename。这两个参数结合起来可以利用redis进行攻击，具体可以参考：https://www.freebuf.om/articles/328286.html 中webshell部分。

debug 命令

DEBUG 命令是一个内部命令。 它旨在用于开发和测试 Redis，比如下面命令，可以直接让redis停止作10

s

```
debug sleep 10
```

eval 命令

eval 命令用于执行lua脚本，建议禁止的原因是lua脚本里面信息redis没办法控制，比如，在lua脚本面构造大量循环，会导致redis主进程僵死。

script、evalsha命令

script、evalsha结合起来也可以执行lua脚本，原因同eval 命令

shutdown 命令

shutdown可以直接停止redis服务。属于危险命令的范畴。

高危命令禁用方法

在redis.conf 里面加入下面配置

```
rename-command keys ""
rename-command flushall ""
rename-command flushdb ""
rename-command debug ""
rename-command eval ""
rename-command config ""
rename-command shutdown ""
rename-command script ""
rename-command evalsha ""
```

而如果想要保留命令，但是不能轻易使用，可以重命名命令来设定。

例如：

```
rename-command FLUSHALL joYAPNXRPmcarcR4ZDgC81TbdkSmLAzRPmcarcR
rename-command FLUSHDB  qf69aZbLAX3cf3ednHM3SOlbpH71yEXLAX3cf3e
rename-command CONFIG   FRaqbC8wSA1XvpFVjCRGryWtIIZS2TRvpFVjCRG
rename-command KEYS     eIiGXix4A2DreBBsQwY6YHkidcDjoYA2DreBBsQ
```