禁止使用 root 用户启动 | 访问控制
使用 root 权限去运行网络服务是比较有风险的（nginx 和 apache 都是有独立的 work 用户，而 redis 没有)。rediscrackit 漏洞就是利用 root 用户的权限来替换或者增加 authorized_keys，来获取 root 登录权限的
（2)加固建议
使用 root 切换到 redis 用户启动服务：
useradd -s /sbin/nolog -M redis
-S<shell> 指定用户登入后所使用的 shell。
-M 不要自动建立用户的登入目录
sudo-u redis/<redis-server-path>/redis-server/<configpath>/redis.conf

禁止监听在公网 6379 端口
Redis 监听在 0.0.0.0，可能导致服务对外或内网横向移动渗透风险，极易被黑客利用入侵。
（2）加固建议
在 redis 的配置文件 redis.conf 中配置如下：bind 127.0.0.1 或者内网 IP，然后重启 redis
操作时建议做好记录或备份

打开保护模式
redis 默认开启保护模式。要是配置里没有指定 bind 和密码，开启该参数后，redis 只能本地访问，拒绝外部访问。
(2)加固建议
redis.conf 安全设置：#打开保护模式 protected-mode yes
操作时建议做好记录或备份

限制 redis 配置文件访问权限
因为 redis 密码明文存储在配置文件中，禁止不相关的用户访问改配置文件是必要的，设置 redis 配置文件权限为 600
(2）加固建议
执行以下命令修改配置文件权限：chmod 600 /<filepath>/redis.conf

最该默认端口 6379 | 服务配置
避免使用熟知的端口，降低被初级扫描的风险
（2）加固建议
编辑文件 redis 的配置文件 redis.conf，找到包含 port 的行，将默认的 6379 修改为自定义的端口号，然后重启 redis
操作时建议做好记录或备份

禁止或者重命名危险命令 | 入侵防范
Redis 中线上使用 keys*命令，也是非常危险的。因此线上的 Redis 必须考虑禁用一些危险的命令，或者尽量避免谁都可以使用这些命令，Redis 没有完整的管理系统，但是也提供了一些方案。
修改 redis.conf 文件，添加
rename-command FLUSHALL =“”
rename-command FLUSHDB =“”

rename-command CONFIG= “”
rename-command KEYS=””
rename-command SHUTDOWN=””
rename-command DEL=""
rename-command EVAL= ""
然后重启 redis。重命名为””代表禁用命令，如想保留命令，可以重命名为不可猜测的字符串，如:rename-command FLUSHALL joYAPNxRPmcarcR4ZDgC

开启 redis 认证，设置高复杂密码
redis 在 redis.conf 配置文件中，设置配置项 requirepass，开户密码认证。redis 因查询效率高，auth 这种命令每秒能处理 9w 次以上，简单的 redis 的密码极容易为攻击者暴破。
打开 redis.conf，找到 requirepass 所在的地方，修改为指定的密码，密码应符合复杂性要求：
长度 8 位以上
包含以下四类字符中的三类字符：
英文大写字母(A 到 Z)
英文小写字母到 2)
10 个基本数字(0 到 9)
非字母字符(例如!、$、%、@、^、&等，#除外)
避免使用已公开的弱密码，如：abcd.1234、admin@123 等
再去掉前面的#号注释符，然后重后 redis
操作时建议做好记录或备份
中危-版本存在安全漏洞