**Redis安全配置规范**

**1**     **概述**

**1.1**   **范围**

本规范适用于数字广东所有服务器上部署Redis程序的安全配置

**1.2**   **目的**

本规范旨在数字广东同事在安装配置Redis时进行必要的安全限制，最大化减少安全漏洞的产生，保障公司信息资产的安

**2**     **安全加固**

**2.1**   **安装**

使用最新稳定版本(当前安全且稳定版本是4.0.9)，最新版的安全性更高。下载安装命令如下：

wget http://download.redis.io/redis-stable.tar.gz

tar zxvf redis-stable.tar.gz

cd redis-stable

make && sudo make install

**2.2**   **安全启动**

1）redis配置文件里参数至少包括requirepass设置访问密码和bind只监听内网IP，以减少安全风险。更改配置命令如下：

echo "requirepass 密码" >> /etc/redis.conf

echo "bind 内网IP地址" >> /etc/redis.conf

注：密码长度至少8位，且同时包含大小写字母和数字；内网IP地址请自行修改。

2）新建普通用户redis用于降权启动服务，相关命令参考如下：

useradd redis -d /home/redis -m        #新建普通用户

chown redis:redis /etc/redis.conf        #修改配置文件属主

chmod 700 /etc/redis.conf                   #修改配置文件权限

su - redis                                               #切换至普通用户

redis-server /etc/redis.conf                  #启动服务

**2.3**   **端口限制访问**

遵循最小化原则，按需分配访问权限，以减少安全风险。Iptables命令参考如下：

iptables -A INPUT -p tcp -s 来源IP地址 --dport 6379 -j ACCEPT

iptables -A INPUT -p tcp --dport 6379 -j DROP

注：来源IP地址请自行修改；redis默认监听端口为6379(TCP)，若业务修改成其他端口，这里也要作对应修改。

**2.4**   **限制redis文件目录访问权限**

设置redis的主目录权限为700;

由于redis密码明文存储在配置文件当中，所以配置文件存放的目录权限修改为600。

命令参考如下：chmod 700 /opt/redis 、chmod 600 /opt/redis/conf

**3. 简明Checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| 阶段 | 检查点 | 检查方法 | 检查结果 |
| 下载 | 下载 | 是否从官方渠道<http://download.redis.io/redis-stable.tar.gz>, 当前最新的安全版本是4.0.9 |  |
| 校验 | 是否在下载完成后校验文件hash |  |
| 配置 | 检查配置文件 | redis配置文件里参数至少包括requirepass设置访问密码和bind只监听内网IP，以减少安全风险 |  |
| 普通用户运行redis | 新建普通用户启动redis服务 |  |
| 设置主机防火墙策略 | Iptable设置仅允许指定的应用可以访问redis数据库 7379端口，其他非业务IP禁止; |  |
| 文件目录权限配置 | 设置redis的主目录权限为700; 配置文件存放的目录权限修改为600。命令参考如下：  chmod 700 /opt/redis;  chmod 600 /opt/redis/conf |  |