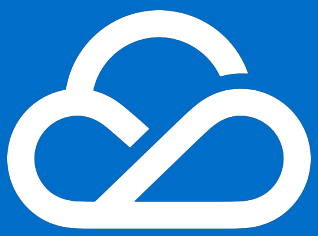
腾讯云主机安全

登录安全介绍

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

登录安全介绍

登录安全检测介绍

基于用户的常用登录地和恶意登录源两个维度，对服务□的登录日志进□分析，识别出服务器登录流水中的异地、异常登录□为，并且实时通知给用户。根据服务器的账户登录□为分析，对可疑的登录□为提供实时告警通知。

基于云服务器的流水查询功能，用户可以对比流水与自己登录□为的差异，得出是否有异常登录□为，并采取相应的安全措施。

登录审计操作说明

云镜采集了主机上的 RDP 和 SSH

登录日志，登录审计功能提供了主机上的全部登录流水展示，并对可疑的登录行为进行了标识。

说明：

- 服务器：当前被登录的服务器。
- 来源 IP：登录来源 IP，一般是公司网络出口 IP，或者使用的网络代理 IP。
- 来源地： 登录来源 IP 所在的地域。
- 登录用户名：成功登录服务器使用的登录用户名。
- 登录时间：成功登录服务器的时间（服务器上的时区时间）。
- 状态
  - 正常：云镜判断当前登录行为无异常风险，登录来源地是管理员常用的登录地。
  - 异地登录：云镜判断非常用登录地的登录行为，可能是管理密码被泄露给其他人登录，也可能是管理员在异地出差进行的登录。
- 操作
  - 误报：若认为该条登录日志属于正常的登录，你可以单击误报，这条登录日志将被置为正常登录。
  - 删除：对该记录进行删除，删除后不再显示。

弱密码检测工具

获取方法：

第一步：登录云主机，下载压缩包到云主机服务器。下载命令如下：

wget mirrors.tencentyun.com/install/sec/qcloud-checkpassword.zip

第二步：解压，unzip qcloud-checkpassword.zip

，工具由二进制程序checklocalpasswd，脚本check.sh以及弱密码库三部分组成。

使用说明：

1.check.sh主要是封装了checklocalpasswd的默认配置，直接调用脚本即可开始处理，处理时间根据机器和密码库的大小不同而不同。默认启动5个进程同时检查，每个进程占用CPU最大20%。

2.checklocalpasswd此二进制文件是实际检测弱密码程序。可以通过-h参数来查看此二进制程序的说明。主要参数见下表。

表1 参数说明表

序号	参数	说明
1	-f	样本库的文件名，没有此参数，程序只会默认检查用户名是否相同。
2	-n	启动进程数，默认启动1个进程检查，最多启动100个进程。
3	-m	导入到内存的字典数量，默认是1千万，最大支持2千万。
4	-o	输出报告文件，默认文件report.txt程序跑完后，可以在此文件中查看弱密码情况，为空则表示没有弱密码。
5	-h	参数说明

3.弱密码字典文件可以用户添加，每行一个弱密码。

演示截图如图图1，图2，图3所示：

图1 测试开始时演示图

```
root@qclount-test:~/qcloud> ./check.sh
        There is 31 users and 4 users can logon the system.
        Now compute the time,wait for seconds.
        Process need 935s.
        [PID=4003] : Now start to process.
        [PID=4004] : Now start to process.
        [PID=4005] : Now start to process.
        [PID=4006] : Now start to process.
        [PID=4007] : Now start to process.
        Now processing 5.28%.
        Now processing 6.59%.
        Now processing 7.89%.
        Now processing 9.20%.
        Now processing 11.82%.
        Now processing 13.12%.
        Now processing 14.43%.
        Now processing 15.74%.
        Now processing 18.35%.
        Now processing 19.66%.
        Now processing 20.97%.
```

图2 测试结束时演示图

```
        Now processing 88.84%.
        Now processing 89.50%.
        Now processing 90.80%.
        Now processing 91.46%.
        Now processing 92.11%.
        Now processing 92.77%.
        Now processing 93.75%.
        Now processing 94.73%.
        Now processing 95.39%.
        Now processing 96.04%.
        Now processing 96.70%.
        Now processing 98.00%.
        Now processing 98.63%.
        [PROCESS 4007] : process ok, exit
        [PROCESS 4003] : process ok, exit
        Cost time is 1175s.
        You can get detail info from report.txt.
```

图3 弱密码信息演示图

```
root@qclount-test:~/qcloud>     cat report.txt
[The password is the same as user(ddtest)]
[secu have simple passwd([redacted])
root@qclount-test:~/qcloud>
```