态势感知

最佳实践

文档版本	01
发布日期	2022-06-29

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 提升登录口令安全最佳实践

弱口令是指密码强度低，或广泛被使用，容易被攻击者破解的口令。弱口令一旦被攻击者获取，可用来直接登录系统，读取甚至修改网站代码，使用弱口令将使得系统及服务面临非常大的风险。建议您为服务器设置复杂的登录口令，并定期提升登录口令的安全性。

本文将介绍如何提升登录口令的安全性以及常见服务器登录口令的修改方法。

背景信息

- 出现弱口令的**原因**：
  - 设置的自动生成密码的方式过于简单，与弱口令检测的密码库相重合；
  - 将同一密码用于多个子账号，会被系统判定为弱密码。
- 使用弱口令可能会造成以下**危害**：
  - 对于个人用户而言，如果使用了弱口令，可能会被猜解或被破解工具破解，从而泄露个人隐私信息，甚至造成财产损失；
  - 对于系统管理员而言，如果使用了弱口令，可能会导致整个系统被攻击、数据库信息被窃取、业务系统瘫痪，造成所有用户信息的泄露和巨大的经济损失，甚至可能引发群体性的网络安全危害事件。

检测弱口令

及时检测弱口令能够有效防止系统被攻击和信息泄露，可以提高系统的安全性。

华为云态势感知**基线检查**功能，可以检查您的IAM账号/主机中是否存在高危弱口令风险。如果在您的IAM账号/主机中检测出了高危弱口令风险，建议您及时修改弱口令。具体方法请参见本文的**修改常见的服务器弱口令**、**修改常见的服务器弱口令**、**提升口令安全-IAM账号**、**提升口令安全-主机**。

提升口令安全-IAM 账号

您可以通过以下方法提升IAM账号的口令安全性：

- 提升密码复杂度。

  密码复杂度建议同时满足以下要求：
  - 密码长度至少8个字符；
  - 密码至少包含以下三种字符种类：

    - 大写字母（A~Z）
    - 小写字母（a~z）
    - 数字（0~9）
    - 特殊字符
  - 同一字符连续出现的最大次数为1次；
  - 不要重复使用最近5次（含5次）内已使用的密码。
- 不使用有一定特征和规律容易被破解的常用弱口令。
  - 生日、姓名、身份证、手机号、邮箱名、用户ID、时间年份
  - 数字或字母连排或混排，常用彩虹表中的密码、滚键盘密码
  - 短语密码
  - 公司名称、admin、root等常用词汇
- 定期修改密码。
  建议每隔90天更改一次密码。

提升口令安全-主机

您可以通过以下方法提升主机的口令安全性：

- 使用复杂度高的密码。
  建议密码复杂度至少满足如下要求：
  a. 密码长度至少8个字符。
  b. 包含如下至少三种组合：
     i. 大写字母（A~Z）
     ii. 小写字母（a~z）
     iii. 数字（0~9）
     iv. 特殊字符
  c. 密码不为用户名或用户名的倒序。
- 不使用有一定特征和规律容易被破解的常用弱口令。
  - 生日、姓名、身份证、手机号、邮箱名、用户ID、时间年份
  - 数字或字母连排或混排，常用彩虹表中的密码、滚键盘密码。
  - 短语密码
  - 公司名称、admin、root等常用词汇
- 不使用空密码或系统的缺省密码。
- 不要重复使用最近5次（含5次）内已使用的密码。
- 不同网站/账号使用不同的密码。
- 根据不同应用设置不同的账号密码，不建议多个应用使用同一套账户/密码。
- 定期修改密码，建议至少每90天更改一次密码。
- 账号管理人员初次发放或者初始化密码给用户时，如果知道密码内容，建议强制用户首次使用修改密码，若不能强制用户修改密码，则为密码设置过期的期限（用户必须及时修改密码，否则密码应被强制失效）。

- 建议为所有账户配置设置连续认证失败次数超过5次（不含5次），锁定账号策略和30分钟自动解除锁定策略。
- 建议对所有账户设置不活动时间超过10分钟自动退出或锁定策略。
- 新建系统中的账号缺省密码在首次使用前，建议强制用户更改。
- 建议开启账户登录记录日志功能，登录日志最少保存180天，登录日志中不能保存用户的密码。

修改 IAM 账号弱口令

1. 使用管理员账号登录华为云管理控制台。
2. 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

图 1-1 进入统一身份认证服务

3. 进入IAM控制台，在左侧导航栏中，选择“安全设置”页签，进入“安全设置”。
4. 进入安全设置后，选择“密码策略”页签，可以对**密码设置策略**、**密码有效期策略**、**密码最短使用时间策略**进行修改。
5. 设置完成后，在“安全设置”页面中，选择“基本信息”页签，检查IAM用户的密码强度是否为最高级别。

   如果不是，请继续根据**4**进行修改。

修改常见的服务器弱口令

系统名称	修改登录口令	说明
Windows系统	以Windows 10为例说明。 1. 登录Windows主机系统。 2. 单击左下角的  ，然后单击  ，弹出“Windows设置”窗口。 3. 在“Windows设置”窗口中，单击“账户”。 4. 在左侧导航栏中，单击登录选项。 5. 在“登录选项”页面，请根据页面提示信息修改服务器密码。	无
Linux系统	登录Linux服务器，执行以下命令，修改用户登录口令。 **passswd [<user>]**	若不输入登录用户名，则修改的是当前用户的口令。 命令执行完成后，请根据提示输入新的口令。 **说明** “user”为登录用户名。
MySQL数据库	1. 登录MySQL数据库。 2. 执行以下命令，查看数据库用户密码。 **SELECT user, host, authentication_string From user;** 部分MySQL数据库版本可能不支持以上查询命令。 若执行以上命令没有获取到用户密码信息，请执行命令。 **SELECT user, host password From user;** 3. 执行以下命令，根据查询结果及弱密码告警信息，修改具体用户的密码。 **SET PASSWORD FOR '用户名'@'主机'=PASSWORD('新密码');** 4. 执行以下命令，刷新修改的密码信息。 **flush privileges;**	无
Redis数据库	1. 打开Redis数据库的配置文件redis.conf。 2. 执行以下命令，修改弱口令。 **requirepass <password>;**	● 若已存在登录口令，则将其修改为复杂口令。 ● 若不存在登录口令，则添加为新口令。 **说明** “password”为登录口令。

系统名称	修改登录口令	说明
Tomcat	1. 打开Tomcat根目录下的配置文件“conf/tomcat-user.xml”。 2. 修改user节点的password属性值为复杂口令。	无

A 修订记录

发布日期	修改记录
2022-06-29	第一次正式发布。