**安全加固建议**

针对云上业务运营的安全性，需要腾讯云平台和您共同保障，腾讯云会负责整个云计算环境底层的物理和基础架构安全等，但数据安全(客户在云计算环境中的业务数据自身的安全管理，包括权限与加密等方面)是需要您来负责的。

具体云上安全责任共担模型可参考：https://cloud.tencent.com/developer/article/1340083。

后续防范措施建议如下:

1)服务器设置大写、小写、特殊字符、数字组成的12-16位的复杂密码 ，也可使用密码生成器自动生成复杂密码，这里给您一个链接参考：https://suijimimashengcheng.51240.com/

2)删除服务器上设置的不需要的用户

3)对于不需要登录的用户，请将用户的权限设置为禁止登录

4)修改远程登录服务的默认端口号以及禁止超级管理员用户登陆

Windows远程端口修改参考文档：https://cloud.tencent.com/developer/article/1052163

Linux远程端口修改参考文档：https://cloud.tencent.com/developer/article/1124500

5)较为安全的方法：只使用密钥登录禁止密码登陆 （针对Linux系统）

6)腾讯云平台有安全组功能，里面您只需要放行业务协议和端口，不建议放行所有协议所有端口，参考文档： <https://cloud.tencent.com/document/product/215/20398>

7)不建议向公网开放核心应用服务端口访问，例如mysql、redis等，您可修改为本地访问或禁止外网访问

8)如果您的本地外网IP固定，建议使用安全组或者系统防火墙禁止除了本地外网IP之外所有IP的登录请求

9）主机安全定期检测漏洞、定期检查安全基线，并及时修复：https://cloud.tencent.com/document/product/296/46954

10）主机安全启用暴力破解阻断功能：https://cloud.tencent.com/document/product/296/42730

需注意：做好云服务器系统的安全防护可以有效加强云服务器系统安全， 但也无法保证绝对安全， 建议定期做好云服务器系统的安全巡检及数据备份，以防突发情况导致数据丢失、或业务不可用。

在操作加固的同时，也强烈建议您通过镜像、快照、自动快照等工具备份数据保障您的数据安全：

制作系统镜像您可以参考：

https://cloud.tencent.com/document/product/213/4942

数据快照操作您可以参考：

https://cloud.tencent.com/document/product/362/5755

定期快照您可以参考：

https://cloud.tencent.com/document/product/362/8191

如数据最终无法恢复，可将当前环境创建快照备份下。然后重装系统。后续如您准备有其它方案解决加密问题。可恢复快照然后恢复数据。

重装系统参考文档：https://cloud.tencent.com/developer/article/1382388

重装会格式化系统盘，请您操作前注意备份数据。