访问管理

最佳实践

产品文档

腾讯云

最佳实践

最近更新时间：2020-06-30 17:02:58

基本指导原则

1.开启 MFA 保护

为增强账号安全性，建议您为所有账号绑定 MFA；为主账号及子账号都开启登录保护和敏感操作保护。对于支持邮箱登录或者微信登录的强烈推荐进行 MFA 二次验证。开启 MFA 后，账号登录及敏感操作需进行二次校验。相关设置请参考：为协作者设置安全保护、为子用户设置安全保护。

2.使用子账号访问腾讯云

请尽量不要使用主账号的身份凭证访问腾讯云，更不要将身份凭证共享给他人。一般情况下，应该为所有访问腾讯云的用户创建子账号，同时授权该子账号相应的管理权限。相关设置请参考：用户类型。

3.使用组给子账号分配权限

按照工作职责定义好组，并给组分配相应的管理权限。然后把用户分配到对应的组里。这样，当您修改组的权限时，组里相关用户的权限随即发生变更。另外，当组织架构发生调整时，只需要更新用户和组的关系即可。相关设置请参考：用户组。

4.最小权限原则

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限，不要授予更多无关权限。例如，一个用户仅是 CDN 服务的使用者，那么不需要将其他服务的资源访问权限（如 COS 读写权限）授予给该用户。

5.分子账号管理用户、权限和资源

建议同一个子账号不同时管理用户、权限和资源。应该让部分子账户管理用户，部分子账号管理权限，部分子账号管理其他云资源。

6.定期轮转身份凭证

建议您或 CAM 用户要定期轮换登录密码或云 API 密钥。这样可以让身份凭证泄漏情况下的影响时间受限。
主账号密码设置请参考：账号密码。
子用户密码设置请参考：子用户重置密码。

7.删除不需要的证书和权限

删除用户不需要的证书以及用户不再需要的权限。尽量减少访问凭证泄漏后带来的安全风险。

8.使用策略条件来增强安全性

尽可能的为策略定义更精细化的条件，约束策略生效的场景，强化安全性。如约束用户必须在指定的时间，指定的服务器上执行某些操作等。
相关设置请参考：元素参考 condition。