租户上云安全指南

产品文档

目录

专有云租户上云安全指南

背景

专有云租户上云安全指南旨在帮助客户在专有云环境中保护其组织数据和应用程序安全，并构建自身的云上安全体系。帮助客户了解腾讯专有云提供的多种云安全产品，指导客户配置安全的云服务，协助其上云安全。

1. 上云须知

只有通过"企业认证"，完成行业类型认证的客户，才可通过在线支持申请购买专区内的云资源（例：金融专区需完成"金融行业"类型认证）。客户可以同时管理账户下的腾讯云资源和专区内的资源，互不影响。

2. 身份与访问管理

上云之后面临企业组织结构复杂，存在多部门用户协同操作等场景，需要一套安全完善的体系来控制云资源管理访问权限，实现简单管理账号、统一分配权限、集中管控资源。

2.1 管理资产访问权限

使用访问管理（CloudAccessManagement，CAM）限制账号的访问权限： 可以在主账号里创建子账号，给子账号分配主账号下资源的管理权限，而不需要分享主账号的相关的身份凭证，针对不同的资源，授权给不同的人员不同的访问权限。

【最佳实践】正确设置COS存储桶的读配置权限，根据子账号属性赋予指定COS存储对象的写权限，其余子账号无权限访问COS存储对象，保证数据的完整性。

使用堡垒机（CBH）限制对运维人员的访问权限： 运维用户应通过CBH统一运维登录入口，创建对主机和数据库资源的运维账号访问权限，并增加高危命令阻断的策略，所有的运维账号访问将通过堡垒机转发，实现集中管理和审计。

2.2 安全配置账号权限

保护账号登录环境的安全性： 在访问管理（CAM）开启主账号、子账号、协作者三类账号的操作和登录保护，并严格保护子账号和协作者的api密钥，主账号不建议开启api 密钥。

检查并删除过期账号： 及时删除或停用无人使用的、过期的账号；保证每个用户均有独立账号，避免共享账号的存在。

通过云审计监控用户异常行为和威胁事件： 平台默认开启云审计功能，当用户的资源出现异常变更或安全问题，CloudAudit所记录的操作日志将能帮助用户找到原因。

例如：CloudAudit会记录用户的所有账号登录操作，操作时间、源 IP 地址、是否使用多因素认证登录，这些都有详细记录，通过这些记录，用户可以判断账号是否存在安全问题。

3. 互联网访问限制

3.1 划分网络区域

根据业务实际情况划分网络区域： 明确定义每个域的边界，并按照方便管理和控制的原则为各网络区域分配地址。避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

【最佳实践】使用VPC实现网络区域之间的隔离，划分“DMZ”，“计算”，“数据”等不同私有网络环境。

3.2 确保网络访问权限最小化

根据业务实际情况设置每个网络区域的访问控制列表，保证访问权限最小化： 安全组默认存在允许所有来源访问全部协议端口的规则，请按需调整安全组配置，限制各网络区域的访问，避免服务器被入侵，造成数据丢失的严重后果。

【最佳实践】

1.避免暴露多余的公网IP，不建议对公网开放高危服务端口、远程管理端口，若因业务需要必须开放，则应做好相应端口的访问控制。

2.限制VPC内流量访问策略，将安全组的ip和端口的访问控制在指定范围内。

4. 选用安全服务和产品

除了基本的身份管理和互联网访问控制，腾讯专有云还为客户提供了各类安全服务和产品，帮助用户发现并处理云上安全风险。以下表格为主要安全产品介绍和安全推荐

推荐级别：

- 必备： 强烈推荐购买，如无此产品则可能存在较大安全隐患
- 推荐： 推荐业务根据实际需求购买，如不选择则可能存在安全隐患
- 可选： 建议存在对抗场景的客户购买相关服务和产品

安全领域	专有云服务	功能介绍	推荐级别
身份与访问管理	云堡垒机	控制主机等资源访问权限，实现对云上服务器的操作运维审计	必备
网络安全	云防火墙	提供互联网边界和VPC边界防护实时入侵防御	必备
网络安全	web应用防火墙	监测网站业务流量，拦截恶意请求避免黑客恶意入侵	必备
网络安全	DDoS攻击高防服务	对来自互联网的流量攻击进行过滤清洗，防御常见的泛洪DDoS攻击，保障租户公网业务正常访问 特别注明: 专区默认提供2G流量清洗，攻击流量超过2G，会强制封禁被攻击IP（公网业务中断），保障专区整体网络带宽稳定，若需要不被2G以上泛洪攻击影响业务，必备DDoS攻击高防服务	必备
数据安全	数据安全审计	数据库的内部违规和不正当操作进行定位追责，保障数据资产安全	推荐
数据安全	KMS	符合监管和合规要求，帮助用户轻松创建和管理密钥、保护以及执行各项密钥管理策略	推荐
数据安全	云加密机（满足国密要求）	无需单独部署即可享受满足国密标准的数据加密和密钥管理功能	推荐
威胁与漏洞管理	主机安全	提供主机资产管理、漏洞管理、入侵检测、基线检查等功能	必备
威胁与漏洞管理	容器安全	提供容器从镜像生成、存储到运行时的全生命周期安全服务	推荐
云产品配置安全	XSPM（云安全态势管理）	帮助租户识别云服务配置风险，支持资产可视化识别、配置自动修复	推荐
T-Sec 安全托管服务 MSS	腾讯云渗透测试服务	腾讯专家提供人工渗透测试服务，为客户提供针对于 Web 应用、移动 APP、微信小程序的黑盒安全测试内容，可以覆盖安全漏洞全生命周期	可选
T-Sec 安全托管服务 MSS	安全攻防对抗服务	腾讯专家提供红蓝对抗演练服务，面向对安全能力有较高要求的企业用户，用户授权后通过实战模拟 APT 攻击的手法，对企业信息化资产以及可能产生危害的安全风险进行测试	可选
T-Sec 安全托管服务 MSS	安全托管服务	腾讯云应急值守团队提供全天候的安全监控和运营管理分析处置服务，快速响应主机、网络、应用、数据等安全产品的各类安全风险事件，并针对云资产进行持续风险监视和泄露监控等	推荐