消息队列 RabbitMQ 版

安全与合规

产品文档

【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默示的承诺或保证。

文档目录

安全与合规
权限管理

最近更新时间：2026-01-04 15:32:35

腾讯云消息队列 RabbitMQ 版提供完善的企业级安全防护体系，通过主子账号管理、严格的授权与鉴权机制，构建多层次、全方位的安全防护，确保消息传输的每一个环节都得到可靠保护，全面保障数据安全。

控制面权限（账号级）

通过访问管理服务（Cloud Access Management，CAM）主子账号、协作者等功能，实现主子账号之间以及企业间跨账号的授权服务，同时也可通过账号访问密钥管理实现 API 调用云资源的控制。

身份认证

通过控制台或者调用云 API 对 RabbitMQ 资源进行访问，两种方式都需要先进行身份认证，通过认证后才能访问对应的资源。

- 登录控制台：需要验证登录密码，同时提供登录保护和登录验证策略加固身份认证安全。详细介绍请参考 修改登录密码 、 设置登录保护 、 设置登录验证方式 。
- 调用云 API：需要验证访问密钥（AccessKey），访问密钥是用户访问腾讯云 API 进行身份验证时需要用到的安全凭证，由 SecretId 和 SecretKey 一起组成。详细介绍请参考 账号访问密钥管理 。

访问控制

通过访问管理服务（Cloud Access Management，CAM）可以在账号层面对 RabbitMQ 资源进行精细化的权限管理。

- 用户与权限分配：根据企业组织架构，为不同职能部门成员创建独立的用户或角色，并分配专属安全凭证（控制台登录密码、云 API 密钥等）或临时凭证，确保安全可控地访问 RabbitMQ 资源。
- 精细化权限控制：基于员工职能设置差异化的访问策略，精确控制每个用户/角色可执行的操作类型和可访问的资源范围，实现严格的权限隔离。

详细的介绍和操作方法请参考 账号权限概述 。

数据面权限（RabbitMQ 资源级）

RabbitMQ 可以通过**用户与权限管理**功能为每个生产者和消费者配置独立的用户身份，每个用户拥有独立的用户名和密码。通过为不同用户赋予不同的 Vhost 和 Vhost 下不同资源的操作权限，包括配置权限和读写权限，以达到不同用户之间权限隔离的目的。

- 配置权限：影响 Exchange、Queue 的声明和删除。
- 读写权限：影响从 Queue 里读取消息，向 Exchange 发送消息以及 Queue 和 Exchange 的绑定 (binding) 操作。

当客户端进行消息生产或消费时，系统会进行鉴权，未被授权的操作将被拒绝。

详细介绍请参考配置 Vhost 权限。

网络安全

最近更新时间：2026-01-04 15:32:35

消息队列 RabbitMQ 版支持内网访问和公网访问两种连接方式， 针对不同的网络类型 RabbitMQ 提供了多重安全保护机制，保障数据传输安全。

安全机制	机制说明	VPC 网络是否支持	公网是否支持
公网白名单	公网访问白名单支持指定哪些外部 IP 地址或者 IP 范围可以访问 RabbitMQ 服务，其他所有未明确允许的 IP 地址将被自动拒绝，有效保障公网通信安全。	×	✓
TLS 加密	SSL 是一种数据传输安全协议，通过加密技术确保数据在传输过程中不被窃取或篡改，有效提升通信安全性。 RabbitMQ 支持绑定自定义 SSL 证书，用于保护客户端与服务器之间的通信安全，同时支持单向认证和双向认证，验证通过则允许客户端连接服务端。 • 单向认证：由**客户端认证服务端**，客户端对服务端的认证通过服务端证书完成，服务端会使用您选择的证书和客户端建立连接。 • 双向认证：**客户端与服务端之间相互认证**，通过服务端证书和客户端 CA 证书完成服务端和客户端的认证，以保证客户端和服务端通信链路的安全及可靠。	✓	×

更多详细的介绍请参考 网络连接要求 。

删除保护

最近更新时间：2026-01-04 15:32:35

消息队列 RabbitMQ 版提供了多维度的集群删除保护机制，有效防止集群通过控制台或者 API 被误删除，保障业务数据安全。

操作环节	保护机制	机制说明	参考文档
删除前保护	销毁保护开关	• 开启集群销毁保护开关后，集群将无法通过控制台或者 API 被删除，如需销毁集群，您需要先手动关闭销毁保护开关，才能执行集群的销毁操作。建议对关键业务长期开启此保护开关。 • 集群销毁保护对系统层级的销毁不生效，如按小时计费集群因欠费导致释放，包年包月集群因到期隔离后释放。	配置销毁保护
删除时验证	MFA 认证	• MFA（Multi-Factor Authentication）即多因子认证，是一种简单有效的安全认证方法。它可以在用户名和密码之外，再增加一层保护。 • RabbitMQ 已默认为删除集群操作开启了 MFA 认证，删除集群时，需要先完成身份验证（微信扫码验证、手机验证码校验），以确保是本人操作。	MFA 操作保护
删除后缓冲	隔离期保留	集群销毁后，集群仍然为您保留7天（状态为隔离中），隔离期间您可以手动彻底删除集群，也可以手动恢复集群。7天后集群会自动彻底删除。彻底销毁后该集群的所有资源和元数据将被清除且不可恢复，请提前备份数据。 隔离期间集群的消息读写将被禁止，并且会限制控制台的操作和云 API 的调用。集群内已保存和未消费的消息将不会保留，因此请提前备份数据。	销毁集群

变更记录

最近更新时间：2026-01-04 15:32:35

变更记录将 TDMQ RabbitMQ 版所生成的变更事件数据进行集中的管理、存储、分析和可视化展示，便于日后查询、审计和回溯。您可以在变更记录模块内查看变更记录详情。
详情请参考 查看变更记录 。

云 API 审计

最近更新时间：2026-01-04 15:32:35

操作审计（CloudAudit，CA） 是一项支持对您的腾讯云账号进行监管、合规性检查、操作审核和风险审核的服务。借助 CloudAudit，您可以记录日志、持续监控并保留与整个腾讯云基础设施中操作相关的账号活动。
CloudAudit 提供腾讯云账号活动的事件历史记录，这些活动包括通过腾讯云管理控制台、API 服务、命令行工具和其他腾讯云服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。

- CloudAudit 的详细介绍和开通配置方法请参考 CloudAudit 快速入门 。
- CloudAudit 支持记录的 RabbitMQ 操作事件列表请参考 操作审计支持的 RabbitMQ 操作列表 。