云市场

商品接入

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
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。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

商品接入
接入类型概览

最近更新时间：2020-09-03 16:23:28

镜像服务

镜像服务商品 指将服务商制作的镜像作为商品，用户可以基于镜像来创建实例，从而获得与镜像一致的系统环境。这类商品在操作系统上整合了具体的软件环境和功能，通过将应用软件与云资源结合，实现用户对云服务器即开即用。

SaaS 服务

SaaS 服务商品 指服务商提供的在线应用软件作为商品。用户使用时无需购买独立的云资源，只需购买后登录到指定的网站后即可使用。

人工服务

人工服务商品 指服务商为用户提供的人工服务作为商品，不交付具体的软件或云资源。

API 服务

API 服务商品 指算法或者数据的集成，开发者选购 API 服务后，可以通过服务的调用地址来获取相关的服务（算法或数据）。为保证腾讯云用户正常使用 API 服务，服务商需要在腾讯云网关上部署相关 API 服务。

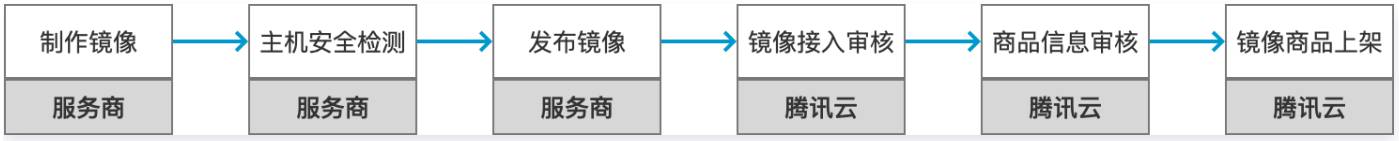
镜像服务

最近更新时间：2024-10-10 14:33:21

简介

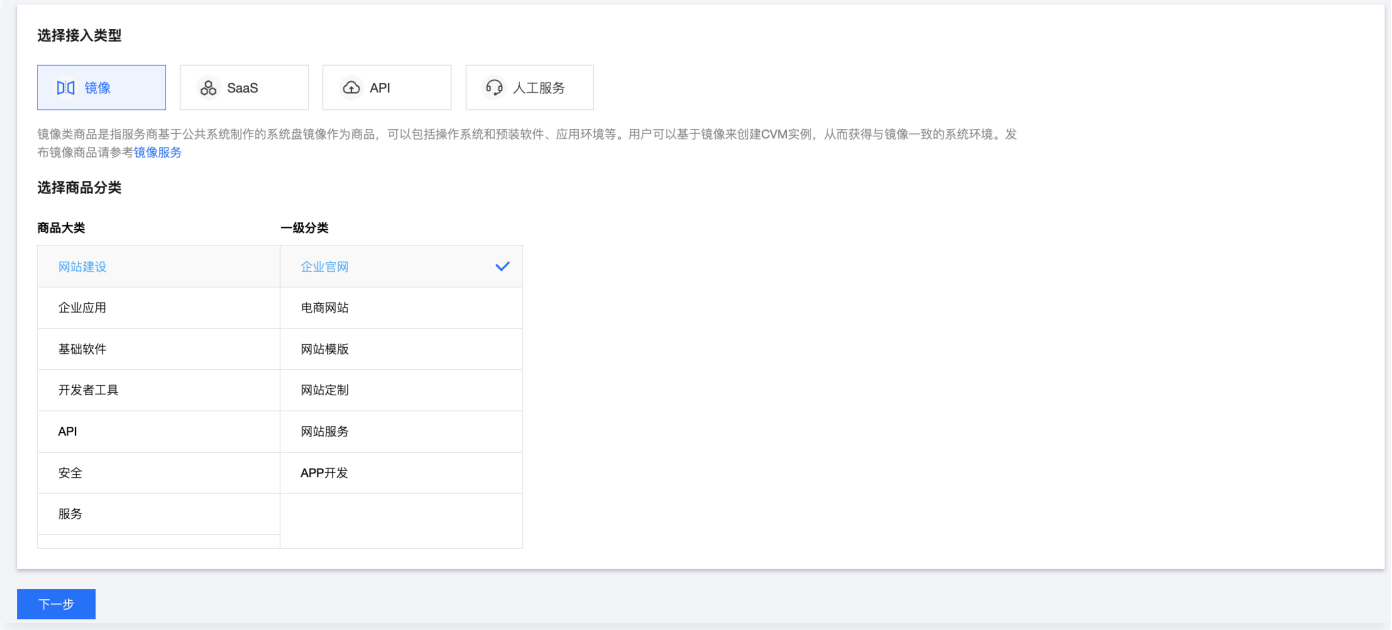
服务商提供的镜像可以是基础的操作系统，或整合具体软件与环境。镜像商品接入云市场后，需要与腾讯云云服务器强绑定。腾讯云用户在选购云市场镜像时，会同时选购腾讯云云服务器，并在云服务器上自动安装与运行镜像。
为保障腾讯云用户正常使用镜像服务，服务商需要在腾讯云云服务器环境上部署环境与应用，并制作镜像。具体请参考《云市场镜像制作》文档。

上架流程



操作步骤

1. 登录 云市场服务商管理控制台，选择左侧菜单栏**商品管理 > 商品列表**。
2. 进入商品列表页面，单击**新建商品**。
3. 选择商品的接入类型“镜像”。
4. 根据商品的功能及使用场景，选择正确的商品分类。



5. 填写镜像商品的接入信息、基本信息、业务信息、销售信息。

接入信息

信息	填写说明
商品名称	必填，输入商品名称，80字内。
版本名称	必填，推荐采用如 v1.2.1，v2.0命名风格的版本号，长度不超过20个字符。
接入镜像	必填，请选择账号下的自定义镜像，您可以前往 商品审核规范 管理和新增镜像，新增完后可点此刷新。制作镜像请参考 云市场镜像制作 。
主机安全检测报告	根据镜像安全要求，上架的市场镜像需要完成 主机安全（专业版）检测，检测通过后才支持镜像上架，主机安全检测有漏洞的镜像务必先修复后再发布市场镜像；对镜像进行主机安全检测需要开通 CVM + 主机安全（专业版），费用需要服务商自付，建议开通按量付费的 CVM + 主机安全（专业版），检测完成后可及时释放 CVM + 主机安全（专业版）。

基本信息

信息	填写说明
商品图片	必填，至少上传1张商品配图，图片大小用于展示在列表页、详情页头部的展示，商品配图需符合 商品审核规范，图片大小不得超过2M，尺寸：390 x 260px，分辨率72dpi。
商品视频	选填，商品视频用于商品详情页展示，会增加曝光的机会；视频支持 mp4 格式，分辨率 1280*720 px，大小不超过 100MB，第一帧不能出现全黑或全白。
商品亮点	必填，介绍产品的亮点，后续商品若上架资源位，将在资源位介绍栏目呈现，文字长度请控制在 8个 – 16 个字符内。
商品简介	必填，简要描述您的商品优势和价值，140字以内。
商品功能特性	选填，介绍产品核心功能和服务商，区别于同类商品的特性，500字以内。
商品详情	必填，详细描述服务内容，包括但不限于：服务介绍、服务流程、使用方法、交付物、帮助文档、过往案例、客户评价。支持图文展示，不支持添加外链。
使用指南	必填，支持本地文档上传，文档格式：PDF、Word、PPT、ZIP、RAR，大小：不超过2M。（镜像服务商品必须包含商品文档，且可下载使用。）
售后服务说明	必填，请按照实际服务内容填写支持的服务范围、时间范围、业务范围、费用范围等信息，500字以内。
商品资质	选填，请上传产品取得的相关资质信息，如：软件著作权证书、开源软件声明或其他资质证书。用以在详情页展示给用户查阅。
客户案例	选填，商品以往服务客户的案例信息，支持图文展示，不支持添加外链。

- **业务信息**

信息	填写说明
商品分类	必填，选择商品上架后的展示栏目。
系统集成软件	必填，填写一至五个标签以说明镜像文件中包含的软件清单，为避免用户纠纷请如实填写。
商品标签	必填，选择一至五个标签以描述商品的属性，回车即可添加新标签。
适用规模	必填，选择产品服务规模。
适用行业	必填，选择一至五个产品主要服务行业，回车即可添加。
适用场景	必填，选择一至五个适用场景，回车即可添加。
商品服务协议	必填，勾选相应协议或者新增协议。《商品服务协议》的内容请参考 云市场《商品服务协议》上线的通知 。
应用开通信息	选填，设置此项后客户在下单时需要填写客户信息才可提交订单。

- **销售信息**

信息	填写说明
是否公开销售	必填，选择“是”，商品上架后可在云市场及 CVM 镜像市场公开展示和搜索；选择“否”商品信息将无法搜索，仅支持链接进入商品详情页。
售卖方式	必填，选择镜像的计费方式：按量计费及按周期计费。 • 按量计费：采用后付费方式结算，用户购买镜像时不收费，使用时按照小时收费，目前按量计费的镜像仅支持0元的规格售卖。 • 按包周期计费：按月定价或者按年定价。

6. 商品信息填写过程中，您可随时单击页面最下方的**保存草稿**随时保存商品信息。
7. 单击**上一步**可返回上个界面修改信息。
8. 单击**提交审核**可将商品提交审核，提交后商品为“审核中”状态，云市场运营人员会在**7个工作日**左右完成审核。
9. 商品提交审核后，在商品管理列表页中，可单击商品名称进入商品预览页，如商品仍需修改，单击**撤销审核**，重新编辑商品信息后，提交审核即可。

相关文档

如需了解更多商品管理信息，请参见 商品管理 文档。

镜像商品制作说明

最近更新时间：2024-09-14 15:23:01

为保障发布到云市场镜像能够顺利在腾讯云服务器上运行，服务商需要先购买腾讯云云服务器。服务商可以考虑按量购买服务器。云服务器购买指南请参见 快速配置 Linux 云服务器 、快速配置 Windows 云服务器 。镜像制作完毕后，可关闭服务器以避免产生新费用。

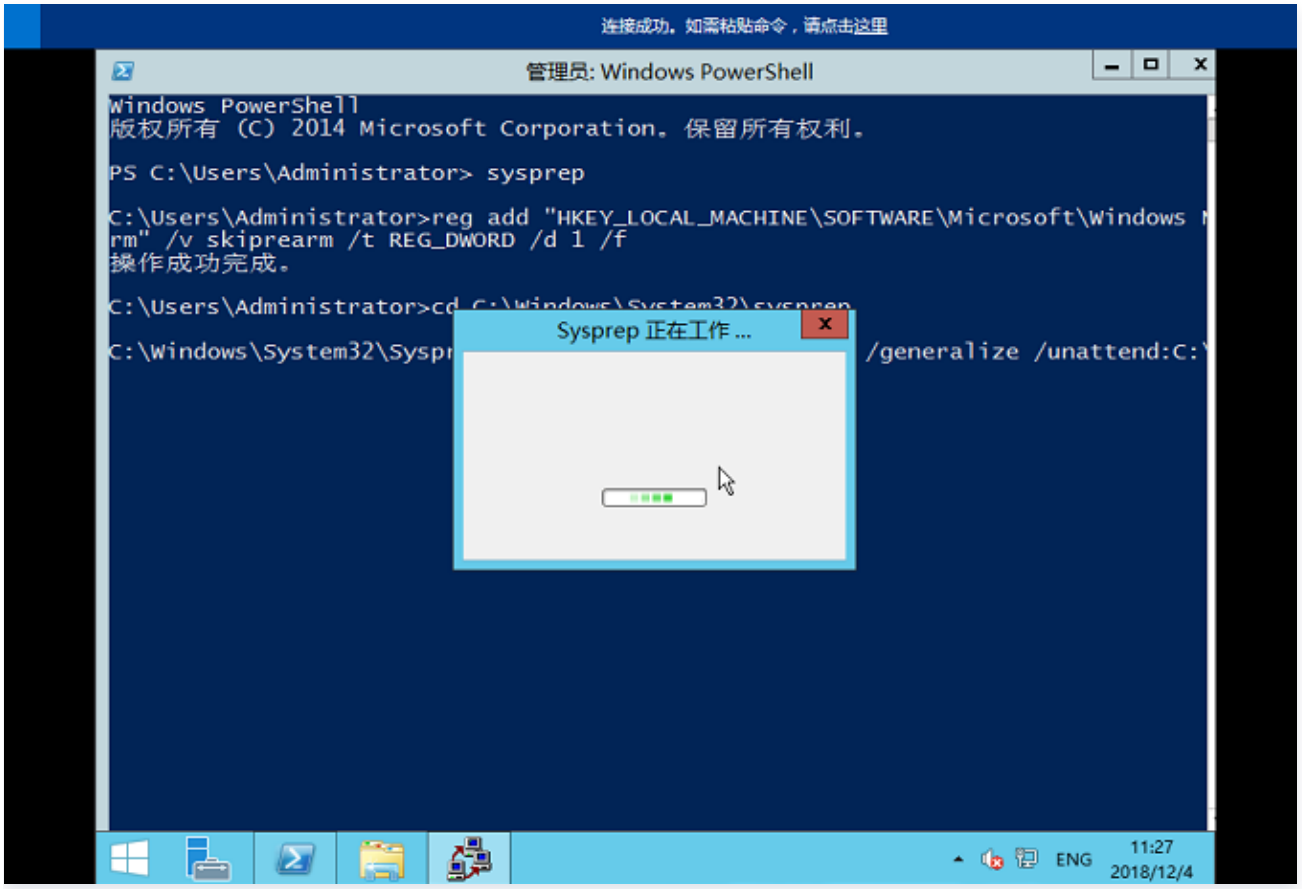
镜像制作步骤

步骤一：查找目标主机

登录 云服务器控制台， 查找已购买的目标云服务器。

步骤二：安装所需软件

在实例正常运行的情况下，您可以通过 SSH 或者带外控制登录到云服务器，安装所需软件以及配置网络与环境。



注意：

- 若为 Windows 镜像制作，请勿在此环节执行 sysprep，否则将不会通过审核。执行 sysprep 制作镜像会有如下影响：
  - 需要云服务器已启用 administrator 账户。
  - 基于 Windows2008 制作的镜像中无法保存 administrator 账户的用户配置。

- 若为 Windows 镜像制作，请务必确认 cloudbase-init 服务已设置为自动启动，否则制作的镜像将不可用。
- 若为 Windows 镜像制作，请勿在桌面上放置任何使用文档或者生成密码文件。对于使用指引请以单独的文档提供，我们将在商品详情页面给与展示；对于密码文件等，请统一放置在确定的目录下， 并在商品详情中，指引用户在该目录下寻找必要的文件。

步骤三：清理日志和缓存文件

当安装好必要的软件后，建议您在制作镜像前对系统进行一次清理操作。将镜像制作过程中产生的日志进行清理，给最终用户呈现一个纯净的环境。以下为 Windows 系统下清理日志和缓存文件的指引：

1. 系统更新缓存：目录在 `Windows/SoftwareDistribution/Download` ，底下有没加分隔符的 uuid 目录(此类目录为更新缓存目录)都可以删除。
2. Windows 系统日志：占用可以用日志事件管理器去清理，在“管理工具”中打开“事件查看器” ，其中 Windows 下：
   - 应用程序（用户态变更日志，例如手动安装的应用程序）：排查 WindowsServer 故障时的关键日志，**建议保留14天**。
   - 安全（本地/远程登入登出记录、修改鉴权记录日志）：产生的日志量较大，**建议保留7天**。
   - 设置（Setup 日志，记录系统更新、应用程序安装卸载日志）：**建议保留3天**，关键的更新在 WindowsUpdate.log 中会体现，可适当保留时间短一些。
   - 系统（系统态变更日志。例如电源、磁盘变更等）：排查 WindowsServer 故障时的关键日志，**建议保留14天**；可以在对应日志属性中设置最大日志文件大小，并选择“按需要覆盖时间（旧事件优先）” ，则设置将在日志文件到达设置大小时，自动覆盖掉倒序旧日志。

步骤四：生成自定义镜像

1. 选定目标主机，并将其关机。主机只有在关机的条件下，才能制作为镜像。
2. 单击目标主机**更多**选项，选择**制作镜像**，在弹出框中填写镜像名称和镜像描述后，单击**确定**，镜像开始制作。
3. 制作完成后，可在自定义镜像中查看该镜像。

镜像制作安全规范

- 为保障用户使用镜像的质量和云服务器安全性，服务商上架镜像形态商品前，需充分自测以保障服务质量，并达到 镜像安全审核标准 后，方可通过腾讯云审核。
- 不得修改操作系统内核，如的确有需要，请提前联系腾讯云工作人员。
- 不得删除系统镜像的安全加固组件和其他关键配置，如下表所示。
- 不得放置任何后门、木马等恶意程序，一经发现将立即挂起该服务商所有镜像商品。
- 镜像需保证云服务器的基础能力完全正常，包括“开机，关机，重启，登录，重置密码， 制作镜像，密钥绑定，解绑（限定 Linux 系统）、云监控”。
- 镜像的实际功能，需要与对应商品的文字描述完全一致。

模块	类型	安装路径	进程名	配置项	描述
洋葱	软件	/usr/local/sa	Secu-tcs-agent	/	安全组件
网管	软件	/usr/local/agenttools	agent	/	虚拟机运行监控模块
DNS	配置	/	/	广州： nameserver 10.138.224.65 nameserver 10.182.20.206 nameserver 10.182.24.12 上海： Nameserver 10.236.158.106 nameserver 10.237.148.54 nameserver 10.237.148.60 在虚拟机内部执行一下命令确保能进行正常的域名解析， `http://nslookupopenapi.tencentyun.com/`	从虚拟机访问腾讯云服务，外部服务的 dns 解析服务器
NTP	配置	/	/	在 crontab 中有配置 ntp 服务	腾讯云提供的时间 服务器配置
洋葱	软件	/	WinAgent	/	安全组件
网管	软件	C:/win-agent	win-agent	/	虚拟机运行监控模块

镜像上架流程

进行主机安全检测

根据镜像安全要求，上架的市场镜像需要完成 主机安全（专业版）检测，检测通过后才支持镜像上架，主机安全检测有漏洞的镜像务必先修复后再发布市场镜像；对镜像进行主机安全检测需要开通 CVM + 主机安全（专业版），费用需要服务商自付，建议开通按量付费的 CVM + 主机安全（专业版），检测完成后可及时释放 CVM + 主机安全（专业版）。

申请镜像商品上架

镜像制作完成后，登录服务商管理后台，发布镜像商品至云市场。详情请参见 镜像服务 。

镜像审核和镜像上架

1. **审核说明：**腾讯云工作人员，会对服务商申请的镜像的安全、功能等进行扫描检查，以及对商品内容进行审核。
   - 审核通过后将由腾讯云工作人员审核上架该商品。
   - 若未审核通过，将联系服务商进行修改。
2. **上架说明：**商品上架后，建议服务商主动检查该商品的正确性，如有任何问题，欢迎随时联系腾讯云。

镜像安全审核标准

最近更新时间：2025-07-08 10:15:24

定义

本文档主要适用于对腾讯云云市场中镜像服务类产品进行安全审核。
镜像的安全审核要求主要分为两类：

- **必备要求项**：为审核前必须满足的基本条件，如有不符将在安全审核中不予通过。
- **优化建议项**：为在满足“必备要求”的基础上提供额外的加固指导和建议，为可选项，建议镜像服务商结合自身业务情况进行强化加固，以提升服务镜像的安全性和可用性。

适用范围

腾讯云云市场 镜像服务类商品的安全审核。

系统组件安全

系统组件加固主要针对系统基础支撑组件进行加固，这部分组件为系统的各类服务支持，可以保证系统底层的安全性，防止黑客入侵。

必备要求

- 禁止镜像存在公开可利用的且已公布修复方案的高危安全漏洞。
- 禁止使用官方已停止维护的发行版本进行镜像，例如 Debian6、CentOS4、Win2003。
- 镜像制作时必须安装所有官方安全更新，具体请参见下文 安装系统安全更新 。
- 禁止镜像默认安装任何病毒、木马、后门、挖矿以及挂机等恶意程序。
- 禁止使用任何盗版或者破解版程序。

> **注意：**
> 已上架镜像会被定期扫描，若发现服务镜像不满足上述条件存在安全漏洞或违规行为，腾讯云将有权对厂商镜像做下架处理。

优化建议

安装系统安全更新

- Windows 系列镜像：建议开启 Windows Update 自动更新，保证最新更新已安装。
- 红帽系列镜像：包括 RHEL、CentOS、OpenSUSE 等，请使用 yum update 命令进行 重要安全组件 更新。
- Debian 系：包括 Debian、Ubuntu 等 Linux 发行版，在配置好正确的 APT 镜像源地址的情况下，可使用 apt update &&apt upgrade 命令进行更新。
- 其他发行版包括 BSD 衍生版，请使用相应的命令进行更新。

更新常用核心组件

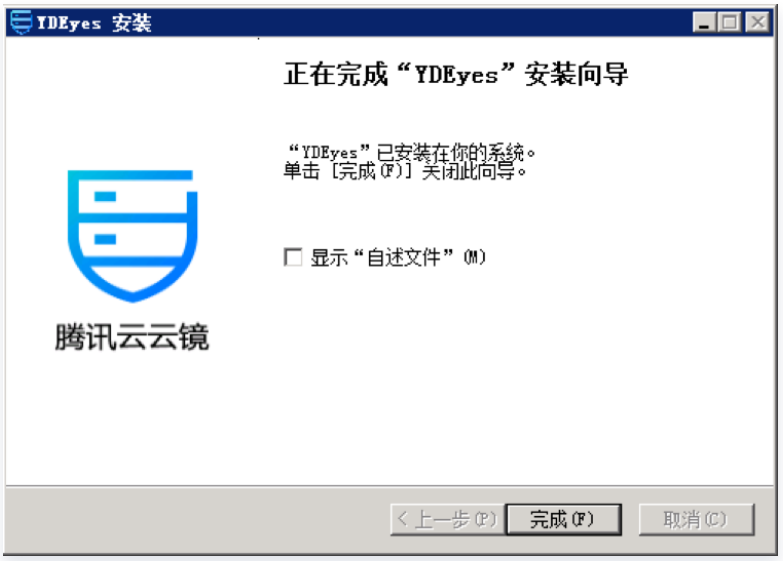
需确保如下组件已更新且无漏洞，更新方法可参照系统安全更新所提命令：

类型	组件名称
内核及引导	grub、kernel、initramfs、sysvinit、systemd、efistub 等。
常用依赖库	libc6、glibc、libssl（openssl）、libgnutls、OpenJDK、SunJDK、libtomcat、libxml、libgd、libpng、zlib、libpython、libnet、libkrb、libcup、libfuse、libdbus 等。
常见应用	包含但不限于 wget、rsync、curl、tar、apt、dpkg、rpm、yum 、sshfs、shell（bash、zsh、csh、dash…）、openssh、ftp、gzip、sudo、su、ppp、exim 等。

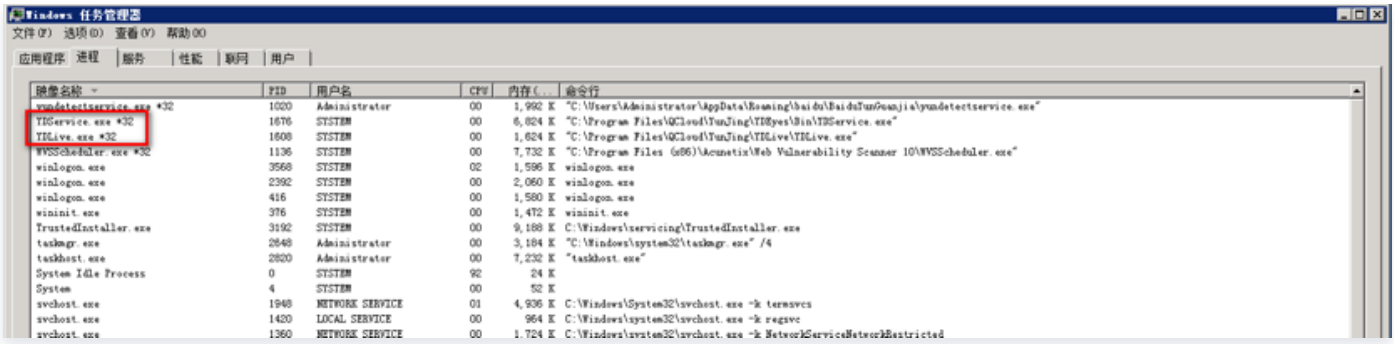
安装主机安全组件

Windows 安全 Agent 安装指引

1. 登录腾讯云控制台，根据镜像版本下载相应的主机安全控件：主机安全（云镜）。
2. 安装主机安全控件，如下图：



3. 检查是否安装完成。通过“任务管理器”查看是否存在 YDService 和 YDLive 两个进程，若存在，则表示已安装成功，至此，主机安全客户端组件完成安装。



Linux 安全 Agent 安装指引

1. 登录腾讯云控制台，根据镜像版本下载相应的主机安全控件：安全概览 。
2. 登录主机，执行安装脚本：

```
[root@VM_99_227_centos ~]# wget http://u.yd.qcloud.com/ydeyesinst_linux64.tar.gz && tar -zxvf ydeyesinst_linux64.tar.gz && sh self_cloud_install_linux64.sh
--2018-09-06 17:18:44--  http://u.yd.qcloud.com/ydeyesinst_linux64.tar.gz
Resolving u.yd.qcloud.com (u.yd.qcloud.com)... 10.142.35.74, 10.142.21.34, 10.142.21.35, ...
Connecting to u.yd.qcloud.com (u.yd.qcloud.com)|10.142.35.74|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2384834 (2.3M) [application/octet-stream]
Saving to: 'ydeyesinst_linux64.tar.gz'

100%[======================================================================================================================>] 2,384,834   --.-K/s   in 0.1s

2018-09-06 17:18:45 (21.4 MB/s) - 'ydeyesinst_linux64.tar.gz' saved [2384834/2384834]

self_cloud_install_linux64.sh
ydeyesinst_linux64.md5
ydeyesinst_linux64.tar.gz
ydeyes.xml
checking the md5 file...
check package success
```

3. 返回如下结果则说明安全组件安装成功：

```
checking the md5 file...
check package success
install package success
```

系统配置安全

除系统自身漏洞以及引入的第三方组件漏洞外，另一方面的威胁来自于安全配置失误导致的安全问题，通过对系统及重点组件进行加固，可以大大降低人为配置失误或弱配置导致的入侵风险。

必备要求

- 禁止系统及应用高危端口默认对外网开放，常见高危端口列表见附表。
- 合理配置系统关键目录的权限，例如 /etc、/bin、~/.ssh 等。
- 除了 /tmp 目录，其他目录不允许出现 777 权限。
- 默认日志服务保证正常运行，如 dmesg、syslog、wtmp、btmp、sudo 等。
- 设置合理的防火墙或安全组策略，屏蔽不安全的端口（如137、139、445等，详见如下表格），仅开放需要的端口；建议使用 iptables 默认屏蔽所有端口，单独开放需要的端口，例如 HTTP80、SSH22、RDP3389、HTTPS443 等。

附表：

服务名称	默认服务端口	常见漏洞
Rlogin	513	Rlogin 空密码登录。
MySQL	3306	MySQL 弱口令及高危漏洞。
SQL Server	1433、1434	SQL Server 弱口令及高危漏洞。

Windows	SMB 137、139、445	永恒之蓝漏洞，SMB 漏洞。
Rsync	873	Rsync 未授权访问漏洞。
Docker	2375	Docker Remote API 未授权访问漏洞。
CouchDB	5984	CouchDB 未授权访问漏洞导致系统命令执行。
Redis	6379	Redis 未授权漏洞。
Tomcat	8080	Tomcat/WDCP 主机管理系统，默认弱口令。
Elasticsearch	9200	ElasticSearch 命令执行漏洞。
Memcached	11211	Memcached 未授权访问。
Mongodb	27017、27018	MongoDB 未授权访问。
Hadoop	50070、50030	Hadoop 默认端口未授权访问。

优化建议（Linux）

Linux 软件更新配置

腾讯云官方常见软件源供自定义的镜像使用：

CentOS 系列镜像

镜像版本	Yum 源地址
CentOS	`https://mirrors.cloud.tencent.com/help/centos.html` `https://mirrors.cloud.tencent.com/help/epel.html`

> ⚠ **注意：**
> **建议修改前提前做好备份，备份操作方法如下：**
> `cp /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.bak` 。

Ubuntu 系列镜像

镜像版本	APT 源地址
Ubuntu	`https://mirrors.cloud.tencent.com/help/ubuntu.html`

> ⚠ **注意：**

建议修改前提前做好备份，备份操作方法如下：
`cp /etc/apt/sources.list /etc/apt/sources.list.bak` 。

Debian 系列镜像

镜像版本	APT 源地址
Debian	`https://mirrors.cloud.tencent.com/help/debian.html` `https://mirrors.cloud.tencent.com/help/debian-security.html`

注意：
建议修改前提前做好备份，备份操作方法如下：
`cp /etc/apt/sources.list /etc/apt/sources.list.bak` 。

Linux 口令策略加固

操作目的	加强口令的复杂度等，降低被猜解的可能性
检查方法	使用命令 `cat /etc/login.defs/grep PASS` 和 `cat /etc/pam.d/system-auth` 查看密码策略设置。

加固方法	1. 使用命令 `vi /etc/login.defs` 修改配置文件。
	`PASSMAX_DAYS 90 #新建用户的密码最长使用天数`
	`PASS_MIN_DAYS 0 #新建用户的密码最短使用天数`
	`PASS_WARN_AGE 7 #新建用户的密码到期提前提醒天数`
	使用 chage 命令修改用户设置，例如：
	`chage -m 0 -M 30 -E 2000-01-01 -W 7 <用户名>`
	表示：将此用户的密码最长使用天数设为30，最短使用天数设为0，密码2000年01月01日过期，过期前 7 天里警告用户。
	2. 设置连续输错 10 次密码，账号锁定 5 分钟。
	使用命令 `vi /etc/pam.d/system-auth` 修改配置文件，添加
	`auth required pam_tally.so onerr=fail deny=10 unlock_time=300`
	注：解锁用户 faillog -u <用户名> -r

回退方法	`vi /etc/login.defs` 和 `vi /etc/pam.d/ system-auth` ，将配置改回加固前配置。
备注	锁定用户功能谨慎使用，密码策略对 root 不生效。

操作目的	应设置口令最小长度
检查方法	对于采用静态口令认证技术的设备，应配置用户口令最小长度不小于8位。
加固方法	参考配置操作

	在文件 `/etc/login.defs` 中设置 `PASS_MIN_LEN` 不小于标准值8。
检测方法	1. 判定条件 密码长度小于8位修改密码不成功。 2. 检测操作 用要修改密码的用户先登录系统，然后用 passwd 命令修改密码，当长度小于8位提示错误： `BAD PASSWORD: it is too short`
回退方法	修改 `/etc/login.defs` ， `PASS_MIN_LEN` 密码长度改回为0。
备注	无

操作目的	建议重要服务器采用密钥登录
检查方法	`cat /root/.ssh/authorized_keys` ，检查是否有登录账户密钥。
加固方法	1. 通过 ssh-keygen 生成待登录机器的密钥； 2. 将 `/root/.ssh/id_rsa.pub` 内容填入待登录机器密钥文件中 `/root/.ssh/authorized_keys` 。
检测方法	判定条件 抽取测试机， `cat .ssh/authorized_keys` ，检查是否存在。

Linux SSH 服务加固

修改默认端口和监听地址

操作方法
1. `Vi /etc/ssh/sshd_config` 2. 注释#Port 22，添加 Port XXXX，改为其他非默认端口。 3. 添加 ListenAddress <本地监听地址>，如 ListenAddress 10.104.233.1。

配置会话登录超时退出

操作方法
1. `Vi /etc/ssh/sshd_config` 2. 取消注释#ClientAliveInterval 0，改为 ClientAliveInterval 600 或 900，10分钟或者15分钟自动退出。 3. 添加 ListenAddress <本地监听地址>，如 ListenAddress 10.104.233.1。

配置防火墙限制指定源 IP 或者网段才能登录

操作方法

1. `Iptables -A INPUT -s 192.168.0.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT`
2. 这里192.168.0.0/24 可以改为自身已知网段地址。

禁止空密码账户登录

操作方法

1. `Vi /etc/ssh/sshd_config`
2. 找到 PermitEmptyPasswords 项，将其改为 no，即不允许空密码存在。

Linux 高危端口加固

相应服务开启后，查看是否还有高危端口开放

操作方法

1. `netstat -anltp`
2. 若存在非业务端口对外网开放（监听0.0.0.0:XXX），可关闭相应服务或端口所对应进程。

Linux 敏感文件加固

操作方法

1. 具有 suid 和 sgid 的文件具有相当的危险性。简单说就是普通用户使用这些命令时可以具有超级用户的权限，检查特殊权限位文件命令：
   ```
   find /usr/bin/chage /usr/bin/gpasswd /usr/bin/wall /usr/bin/chfn /usr/bin/chsh /usr/bin/newgrp /usr/bin/write /usr/sbin/usernetctl /usr/sbin/traceroute /bin/mount /bin/umount /bin/ping /sbin/netreport -type f -perm +6000 2>/dev/null
   ```
2. 如果存在输出结果，则使用 chmod 755 文件名命令修改文件的权限。例如：`chmod a-s /usr/bin/chage` 。

优化建议（Windows）

修改远程桌面默认端口

基线名称	应修改远程桌面服务(RDP)的默认端口
基线说明	不能使用默认的端口3389。
操作指南	1. **参考配置操作** 打开命令提示符，运行命令 `regedit` 打开注册表编辑器，浏览到路径 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`

	，修改名称为 “PortNumber” 的数值的数据，使其不等于默认值3389。 2. **补充操作说明** 需要重启系统才能生效。
检测方法	1. **判定条件** 在其它的 Windows 上，不能仅使用 IP 通过远程桌面连接程序连接被检查计算机。 2. **检测操作** 打开命令提示符，运行命令 `regedit` 打开注册表编辑器，浏览到路径 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp` ，查看 “PortNumber” 的数值的数据是否等于默认值3389。

配置 Windows 密码策略

操作目的	应启用并正确配置密码策略
检查方法	在组策略中找到密码策略选项，根据自身要求进行配置
加固方法	1. **参考配置操作** 打开命令提示符，运行命令 `gpedit.msc` 打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\ Windows 设置\安全设置\账户策略\密码策略”，配置“密码最长存留期(使用期限)”、“密码最短存留期(使用期限)”、“密码长度最小值”、“强制密码历史”为指定值，并启用“密码复杂性要求”。 2. **推荐设置如下：** 2.1 **账户策略 > 密码策略** ○ 密码必须符合复杂性要求：启用 ○ 密码长度最小值：8个字符 ○ 密码最短使用期限：0天 ○ 密码最长使用期限：90天 ○ 强制密码历史：1个记住密码 ○ 用可还原的加密来存储密码：已禁用 2.2. 账**户策略 > 账户锁定策略** ○ 账户锁定时间：30分钟 ○ 账户锁定阈值：10次无效登录 ○ 重置账户锁定计数器：30分钟 2.3. **本地策略 > 安全选项** 交互式登录：不显示最后的用户名：启用
检测方法	**判定条件** 设置新密码时有以下限制： • 不能设置不符合复杂性要求的密码。 • 不能设置太短的密码。 • 不可在最短留存期内修改密码。 • 必须在最长留存期后修改密码。

	• 不能循环使用指定次数之内的密码。

删除 Windows 无关账户

操作目的	应删除或锁定高危、无关账户。
检查方法	在组策略中找到安全选项，禁用来宾账户或系统其他无关账户。
加固方法	**参考配置操作** 1. 打开命令提示符，运行命令 `gpedit.msc` 打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\ Windows 设置\安全设置\本地策略\安全选项”。 2. 删除或锁定无关账户，操作如下： ○ 使用 “net user 账户名 /del” 删除无关账户。 ○ 使用 “net user 账户名 /active:no” 锁定无关账户。
检测方法	**判定条件** 已禁用来宾账户，或者已删除或锁定其它与实际需求无关的账户。

配置 Windows 事件审核

操作目的	记录 Windows 账户各类操作事件，方便事后追溯。
检查方法	在组策略中找到安全选项， 修改审核策略配置
加固方法	**参考配置操作** 1. 打开命令提示符，运行命令 `gpedit.msc` 打开组策略编辑器。 2. 找到“本地计算机策略\计算机配置\ Windows 设置\安全设置\本地策略\安全选项”。 3. 推荐设置如下： ○ 审核策略更改：成功 ○ 审核登录事件：成功，失败。 ○ 审核对象访问：成功 ○ 审核进程跟踪：成功，失败。 ○ 审核目录服务访问：成功，失败。 ○ 审核系统事件：成功，失败。 ○ 审核账户登录事件：成功，失败。 ○ 审核账户管理：成功，失败。
检测方法	**判定条件** • 已禁用来宾账户。 • 已删除或锁定其它与实际需求无关的账户。
备注	为避免日志空间不足，可提升日志存储空间，通过路径**开始 > 运行 > eventvwr.msc > windows 日志 > 查看**“应用程序”、“安全”、“系统”的属性进行配置，推荐设置为 20480KB 或更高。

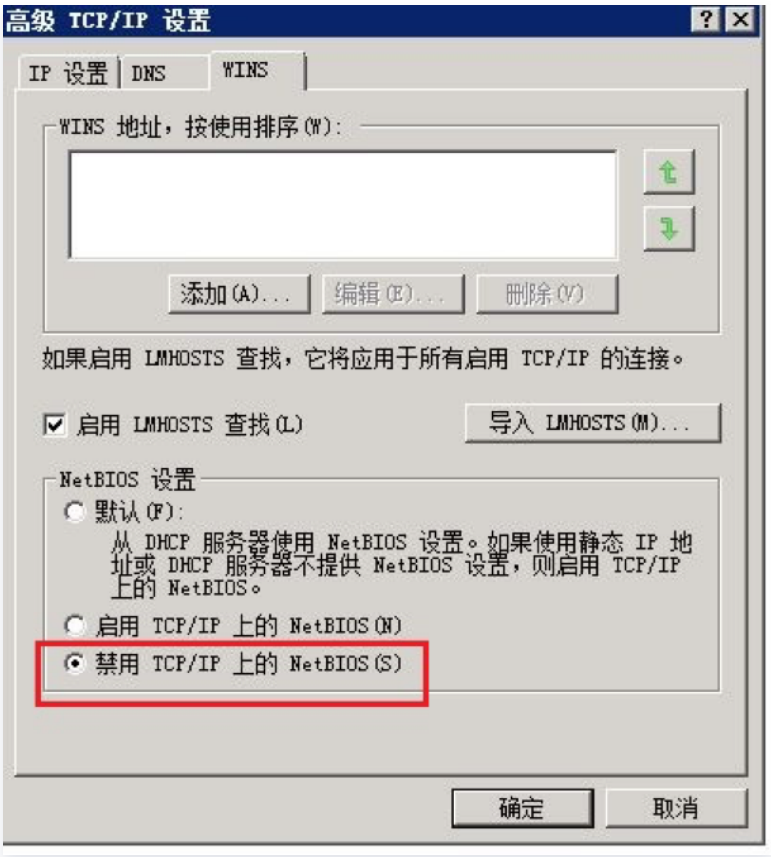
优化 Windows 启动服务

操作目的	应提高系统服务安全，优化系统资源，减少受攻击面。
检查方法	打开“控制面板”，打开“管理工具”中的“服务”，**以不影响业务为前提，禁用以下服务**： • Alerter 服务 • Clipbook 服务 • Computer Browser • Messenger • Remote Registry Service • Routing and Remote Access • Simple Mail Trasfer Protocol(SMTP)（可选） • Simple Network Management Protocol(SNMP) Service（可选） • Simple Network Management Protocol(SNMP) Trap（可选） • Telnet • World Wide Web Publishing Service（可选） • Print Spooler • Terminal Service

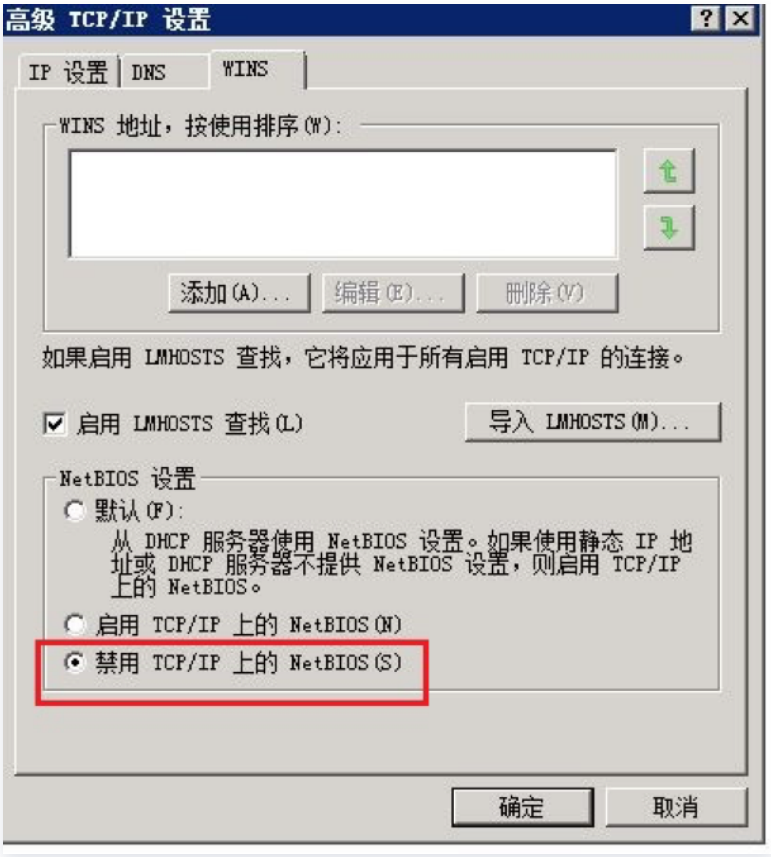
强化网络访问控制权限

操作目的	关闭高危网络端口及默认共享，启用网络访问限制。
检查方法	1. **启动网络访问控制** ○ 操作方法如下： **开始 > 运行 >** `secpol.msc` **> 安全设置 > 本地策略 > 安全选项** ○ 推荐配置如下： ○ 网络访问：不允许 SAM 账户的匿名枚举：已启用。 ○ 网络访问： 不允许 SAM 账户和共享的匿名枚举：已启用。 ○ 网络访问：将 Everyone 权限应用于匿名用户：已禁用。 ○ 账户： 使用空密码的本地账户只允许进行控制台登录：已启用。 ○ 关闭共享服务端口（135、137、139、445 等）。 若未用到 SMB、RPC 等服务，建议用户关闭相应服务端口。方法如下： ○ 135 端口关闭方法： 1.1.1 单击**开始 > 运行**，输入“dcomcnfg”，单击**确定**，打开组件服务。 1.1.2 在弹出的“组件服务”对话框中，选择“计算机”选项。 1.1.3 在“计算机”选项右边，右键单击**我的电脑**，选择“属性”。 1.1.4 在出现的“我的电脑属性”对话框“默认属性”选项卡中，去掉“在此计算机上启用分布式 COM”前的勾。 1.1.5 选择“默认协议”选项卡，选中“面向连接的 TCP/IP”，单击**删除**按钮。 1.1.6 单击**确定**按钮，设置完成，重新启动后即可关闭 135 端口。 ○ 137、138、139等 Netbios 服务端口关闭方法：

通过路径“控制面板 > 网络与共享中心 > 本地连接”右键单击**属性**，选择“TCP/IPv4协议”属性，在“常规”选项卡下选择“高级”，选择“WINS”选项卡，选中“禁用 TCP/IP 上的 NetBIOS”，这样即关闭了 139 端口。



具体操作可参考这里。



2. **关闭默认共享**
   - 查看共享：**开始 > 运行 > cmd.exe > net share**
   - 关闭默认共享操作：

     开始 > 运行 > regedit，找到

     ```
     HKEYLOCALMACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
     ```

     选项，新建 AutoShareServer（REGDWORD），键值设置为0即可。

第三方组件安全

第三方组件为各类 Web 类应用服务提供丰富的支撑环境，如果爆发漏洞，会给操作系统本身以及用户的业务带来极大的风险和隐患，对第三方的组件进行加固，可以保服务组件整体的安全性，以及保障服务自身安全及用户信息安全。

必备要求

- 禁止镜像第三方组件存在公开可利用的且已公布修复方案的安全漏洞。
- 禁止使用已停止维护的软件版本，如 PHP 5.3. 与 5.4. 版本、PHPMyadmin 4.0.0 以下版本，MySQL 5.1. 版本等。
- 镜像制作中需从第三方组件官方提供的下载页面下载最新稳定版本进行安装，禁止通过非官方站点下载部署。
- 禁止使用任何非授权或破解版商业程序提供商业服务。
- 涉及到镜像内置的软件功能（包括但不限于数据库，FTP，商业软件）的密码，均不能使用“默认方式”内置到镜像文件内，而是通过“启动脚本”的方式（shell，cloud-init 等方案）在镜像创建云服务器的过程随机生成密码文

件，客户在拿到云服务器的访问权限后，可通过 SSH 或者远程桌面等自行去云服务器上查找密码文件以获得密码；生成密码文件的脚本必须使用随机算法，保证每次云机创建后获得的都是唯一的密码。

优化建议

Web 服务组件

常用 Web 组件/CMS	当前稳定版本推荐	官方下载链接
PHP	>=5.6. >=7.0. >=7.1.	http://php.net/
MySQL	>=5.5. >=5.6. >=5.7.	http://dev.mysql.com/downloads/mysql/
Apache	>=2.2. >=2.4.	https://httpd.apache.org/
Nginx	>=1.10. >=1.11. >=1.12.	http://nginx.org/en/download.html
Tomcat	>=9.0. >=8.5.	https://httpd.apache.org/
Redis	>=4.0.*	https://redis.io/download
memcached	>=1.5.10	https://memcached.org/
Squid	3.5 系列最新版本 4.2 系列最新版本	http://www.squid-cache.org/Versions/
Nodejs	>=8.0	https://nodejs.org/en/download
Jetty	>=9.2.*	https://jetty.org/download.html
ProFTPD	1.3.6* 1.3.5*	http://www.proftpd.org/
Drupal	>=7	https://www.drupal.org/

注意：
如上推荐版本为截止2018年08月底最新稳定版，具体可参考官方链接进行下载安装。

Web 应用系统

- 使用的开源 CMS、BBS 等系统以及插件需为截止镜像发布前的最新版本。
- Web 应用系统禁止存在高危安全漏洞，如 SQL 注入、命令注入、文件上传等漏洞。
- Web 应用系统管理后台及数据库密码首次安装使用时需强制用户进行密码修改，禁止服务初始化后使用默认密码提供服务。

Web 环境安全

Web 环境安全包含常见易出现安全问题的 Web 支撑服务组件，典型的如 PHP、Apache、Tomcat、Nginx、IIS、MySQL 、Redis、JBoss、Jetty、vsFTPd。

必备要求

- 建议从官方下载稳定版组件进行部署安装，注意不要下载和使用 beta 版本。
- Web 服务组件必须以普通账户权限运行。
- 禁止 HTTP 目录索引，外部用户可直接访问 Index/ 等目录。
- 不允许使用弱密码，需使用随机字符串作为初始默认密码。
- 合理配置目录访问权限，禁止未授权的目录访问行为，如 .git/.svn 等目录 。
- 默认关闭组件或程序调试模式，避免敏感信息泄露。

优化建议

PHP 安全优化建议

控制脚本访问权限

PHP 默认配置允许 PHP 脚本程序访问服务器上的任意文件，为避免 PHP 脚本访问不该访问的文件，从一定程度上限制了 PHP 木马的危害，需设置 PHP 只能访问网站目录或者其他必须可访问的目录。
`/usr/local/apache2/web/` 为网站根目录，打开 `php.ini` ，安全加固配置方式如下：

```
open_basedir = /usr/local/apache2/web/
```

需要多个目录时，以冒号隔开如：

```
open_basedir = /usr/local/apache2/web/:/tmp/:/data/adc/
```

隐藏 PHP 版本信息

攻击者在信息收集时候无法判断程序版本，增加防御系数。打开 `php.ini` 安全加固配置方式如下，隐藏版本设置：

```
expose_php =off
```

开启安全模式

修改 PHP 配置文件 `php.ini` ，添加如下配置：

```
safe_mode = on
safe_mode_gid = off
```

关闭全局变量

关闭全局变量，配置如下：

```
register_globals =  off
```

禁用 PHP 危险函数

Web 木马程序通常利用 PHP 的特殊函数执行系统命令，查询任意目录文件，增加修改删除文件等。PHP 木马程序常使用的函数为：dl, eval, assert, exec, popen, system, passthru, shell_exec 等。
修改 PHP 配置文件 `php.ini` ，添加如下配置：

```
disable_functions=
dl,eval,assert,exec,passthru,popen,proc_open,shell_exec,system,phpinfo,assert
```

可酌情调整函数内容。

开启 magic_quotes_gpc：

magicquotesgpc 会把引用的数据中包含单引号（ ' ）和双引号（ " ）以及反斜线（ \ ）自动加上反斜线，自动转译符号，确保数据操作的正确运行，magicquotesgpc 的设定值将会影响通过 Get/Post/Cookies 获得的数据，可以有效的防止 SQL 注入漏洞。
打开 `php.ini` ，安全加固配置方式如下，打开 magicquotesgpc 设置：
`magicquotesgpc = On` *

其他参考配置

- 开启 magic_quotes_runtime，对文件或者数据库中取出的数据过滤，能很好地解决二次注入漏洞。
  `magic_quotes_runtime = On`
- 关闭错误信息提示：
  `display_errors = off`
  `display_startup_errors = off`
- 开启错误日志记录，关闭 display_errors 后能够把错误信息记录下来，便于查找服务器运行的原因，同时也要设置错误日志存放的目录，建议跟 webserver 的日志放在一起。
  `log_errors = On`
  `error_log = /usr/local/apache2/logs/php_error.log`
- 不允许调用 dl：
  `enable_dl = off`
- 关闭远程文件，允许访问 URL 远程资源使得 PHP 应用程序的漏洞变得更加容易被利用，PHP 脚本若存在远程文件包含漏洞可以让攻击者直接获取网站权限及上传 Web 木马，一般会在 PHP 配置文件中关闭该功能，若需要访问远程服务器建议采用其他方式，如 libcurl 库：
  `allow_url_fopen = off` `allow_url_include = off`
- 开启 http only：
  `session.cookie_httponly = 1`
  `cookie domain`
- 开启 https secure：
  `session.cookie_secure = 1`
- 适当的 PHP redirects：
  `cgi.force_redirect = 0`
- SQL 的安全模式：
  `sql.safe_mode = on`

Apache 安全优化建议

Apache 软件下载

应该从 Apache 官方提供的下载页面。

删除默认页面

Apache 安装好后，存在默认的示例页面：需要删除两个目录：`icons`、`manual`，并且注释或删除 Apache 配置文件中的以下两行内容：`Alias /icons/ "/usr/share/apache2/icons/"`

```
AliasMatch ^/manual(?:/(?:de|en|es|fr|ja|ko|ru))?(/.*)?$ "/usr/share/apache2/manual$1"
```

目录权限配置

如果 Apache 以 daemon 普通用户启动，则黑客通过网站漏洞入侵服务器后，将获得 Apache 的 daemon 权限，因此需要确认网站 Web 目录和文件的属主与 Apache 启动用户不同，防止网站被黑客恶意篡改和删除。网站 Web 目录和文件的属主可以设置为 root 等（非 Apache 启动用户）。Web 目录权限统一设置为755，Web 文件权限统一设置为644（ cgi 文件若需执行权限可设置为 755），只有上传目录等需要可读可写权限的目录可以设置为777。假设网站目录为：`/usr/local/apache2/htdocs/`，上传目录为：`/usr/local/apache2/htdocs/upload/`

```
chown -R root:root /usr/local/apache2/htdocs/
chmod 755 /usr/local/apache2/htdocs/
find /usr/local/apache2/htdocs/ -type d -exec chmod 755 {} \;
find /usr/local/apache2/htdocs/ -type f -exec chmod 644 {} \;
chmod -R 777 /usr/local/apache2/htdocs/upload/
```

为了防止黑客在777权限目录中上传或者写入 Web 木马，因此需要设置 777 权限的目录不能执行或访问脚本。禁止执行或访问脚本的安全配置如下：

```
<Directory "/usr/local/apache2/htdocs/yourpath">
        Options None
        AllowOverride None
        Order deny,allow
        deny from all
        <FilesMatch "\.(jpg|jpeg|gif|png)$">
                Order deny,allow
                allow from all
        </FilesMatch>
</Directory>
```

消除目录浏览漏洞

Apache 默认允许目录浏览，如果目录下没有索引文件则会出现目录浏览漏洞。
需要把 Apache 配置文件中的全部 “Indexes” 删除或者改为 “-Indexes”。

开启访问日志

开启日志有助于发生安全事件后方便进行入侵回溯，分析原因及定位攻击者：

`CustomLog /www/logs/access_log common`

默认情况下，Apache 已开启访问日志记录，请在 Apache 配置文件中确认已开启访问日志。

其他参考配置

- `FollowSymLinks` 此指令为默认启用，因此在创建符号链接到网页服务器的文档 root 目录时，请慎重行事。例如，请勿为“/”提供符号链接。
- `ServerTokens ProductOnly`
  `serversignature Off`
  Apache 默认输出的 banner 会泄露关键信息，如服务器 OS 类型、Apache 版本、安装的应用程序类型及版本。暴露过多的信息只会给黑客带来便利。
  在 Apache 配置文件中，修改 ServerToken、ServerSignature 设置（如果没有这两行配置，请自行添加）。
- `UserDir` 此指令可确认系统中用户账户是否存在，所以要默认禁用 `UserDir` 指令。
  要在服务器上启用用户名目录浏览，则须使用以下指令：
  `UserDir enabled`
  `UserDir disabled root`
  这些指令用于 `/root/` 之外的所有用户目录，可激活其用户目录浏览这一功能。在禁用账户列表中添加用户，要在 `UserDir disabled` 命令行添加以空格分隔的用户列表。

Tomcat 安全优化建议

Apache 软件下载

应该从 Tomcat 官方提供的下载页面进行安装部署。

Tomcat 日志记录

编辑 `server.xml` 配置文件，确保在 HOST 标签中有记录日志功能，配置如下：

```
<valve cassname="org.apache.catalina.valves.AccessLogValve"
Directory="logs" prefix="localhost_access_log."
 Suffix=".txt"
 Pattern="common" resloveHosts="false"/>
```

> **注意**
> 默认 Tomcat 已经开启日志记录功能。

启动安全模式

为了限制脚本的访问权限，防范 webshell 木马，建议启动时增加安全参数启动，如采用如下方式启动 Tomcat：

`Tomcat/bin/startup.sh -security`

删除 Tomcat 默认页面

删除 `tomcat/webapps/` 目录下的所有文件及目录，已知 `webapps` 目录包含：

`Tomcat/webapps/docs/`
`Tomcat/webapps/examples/`

`Tomcat/webapps/host-manager/Tomcat/webapps/manager/`
`Tomcat/webapps/ROOT/`
删除 Tomcat 的 admin 控制台软件：删除 `{Tomcat安装目录}\webapps` 下 `admin.xml` 文件。
删除 Tomcat 的 Manager 控制台软件：删除 `{Tomcat安装目录}\webapps` 下 `manager.xml` 文件。

删除 jspx 文件解析

Tomcat 默认是可以解析 jspx 文件格式的后缀，解析 jspx 给服务器带来了极大的安全风险，若不需要使用 jspx 文件，建议删除对 jspx 的解析，具体操作为修改 conf/web.xml 文件，将如下代码注释掉：

```
<url-pattern>*.jspx</url-pattern>
```

禁止显示错误信息

Tomcat 在程序执行失败时会有错误信息提示，可能泄露服务器的敏感信息，需要关闭错误提示信息。可以通过指定错误页面的方式不将错误信息显示给用户，修改 `tomcat/conf/web.xml` ,增加如下配置项：

```
<error-page>
<error-code>500</error-code>
<location>/500.jsp</location>
</error-page>
```

> **注意**
> 可以根据需要自行增加相应的错误码，常见的如500，404等，location 选项为指定跳转的页面，该 jsp 文件需要自己生成。

Nginx 安全优化建议

Nginx 软件的下载

应该从 Nginx 官方提供的下载页面下载进行部署安装，需要下载最新稳定版本。注意不要下载 beta 版本， Nginx 官网下载地址为： `http://nginx.org/en/download.html` 。

消除目录浏览漏洞

```
cat/etc/nginx/nginx.conf
```

Nginx 默认不允许目录浏览，请检查目录浏览的相关配置，确保没有目录浏览漏洞。确保 autoindex 的配置为 off ，即 autoindex off 或者没有配置 autoindex。

关开启访问日志

开启日志有助于发生安全事件后回溯分析整个事件的原因及定位攻击者。
默认情况下，Nginx 已开启访问日志记录，请在 Nginx 配置文件中确认已开启访问日志

```
access_log /backup/nginx_logs/access.log combined;
```

关闭服务器标记

```
cat/etc/nginx/nginx.conf
```

添加这行配置：`server_tokens off`

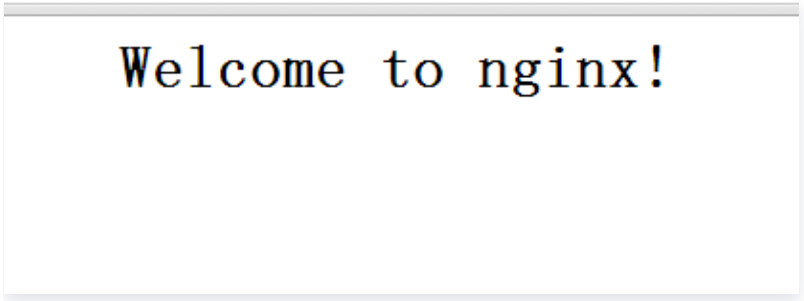
删除默认页面

删除 Nginx 默认首页 index.html，业务可以自行创建默认首页代替之。
删除如下配置信息：

```
location /doc {
                root /usr/share;
                autoindex on;
                allow 127.0.0.1;
                deny all;
        }

        location /images {
                root /usr/share;
                autoindex off;
        }
```

删除首页 index.html 后，新建其他首页内容不允许出现如下首页内容：



其他配置

- 隐藏 Nginx 版本信息，打开配置文件 隐藏版本设置：
  `Server_tokens off;`
  攻击者在信息收集时候无法判断程序版本，增加防御系数。
- 禁用非必要的请求方法：
  `if ($request_method !~ ^(GET|HEAD|POST)$ ) { return 444; }`
  trace 请求用于网络诊断，会暴露信息，只允许 GET、HEAD、POST 请求，其他请求直接返回444状态码（444是 Nginx 定义的响应状态码，会立即断开连接，没有响应正文，TRACE 请求 Nginx 内置405拒绝。）

IIS 安全优化建议

IIS 软件的安装

业务应基于 IIS7.0 或以上版本搭建。

删除 IIS 默认站点、无关页面，关闭不需要的服务

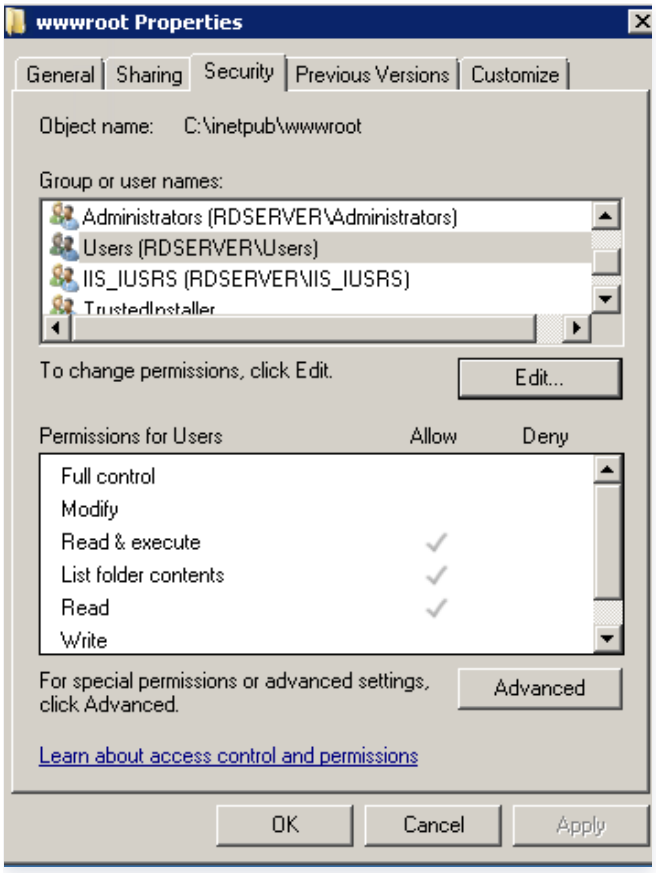
1. 删除 `c:\Inetpub` 以及其他默认站点目录。
2. 应删除 Defaul.htm、Default.asp、index.htm、index.html、iisstart.htm 等默认文档。
3. 关闭站点不需要的服务如 SMTP、FTP。

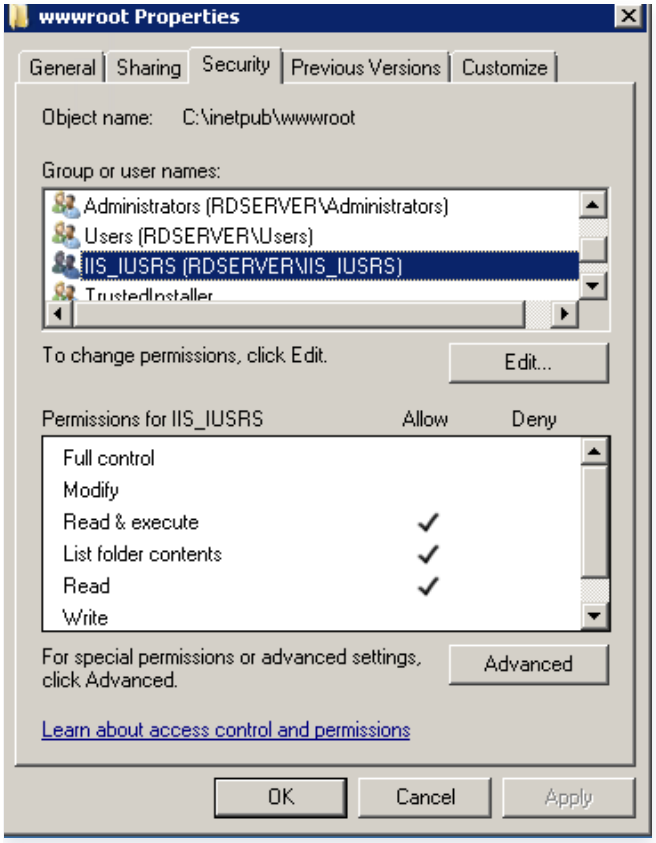
删除无关账号

IIS 站点部署后系统会自动生成 IIS 用户账号 IUSRS，在不影响站点正常访问和系统运行维护的前提下删除其他不必要的账号。如 ASPNET 账号、Guest 账号、User 账号等；系统管理员组仅允许管理员账号 administrator 加入。

关闭 Web 目录的写权限

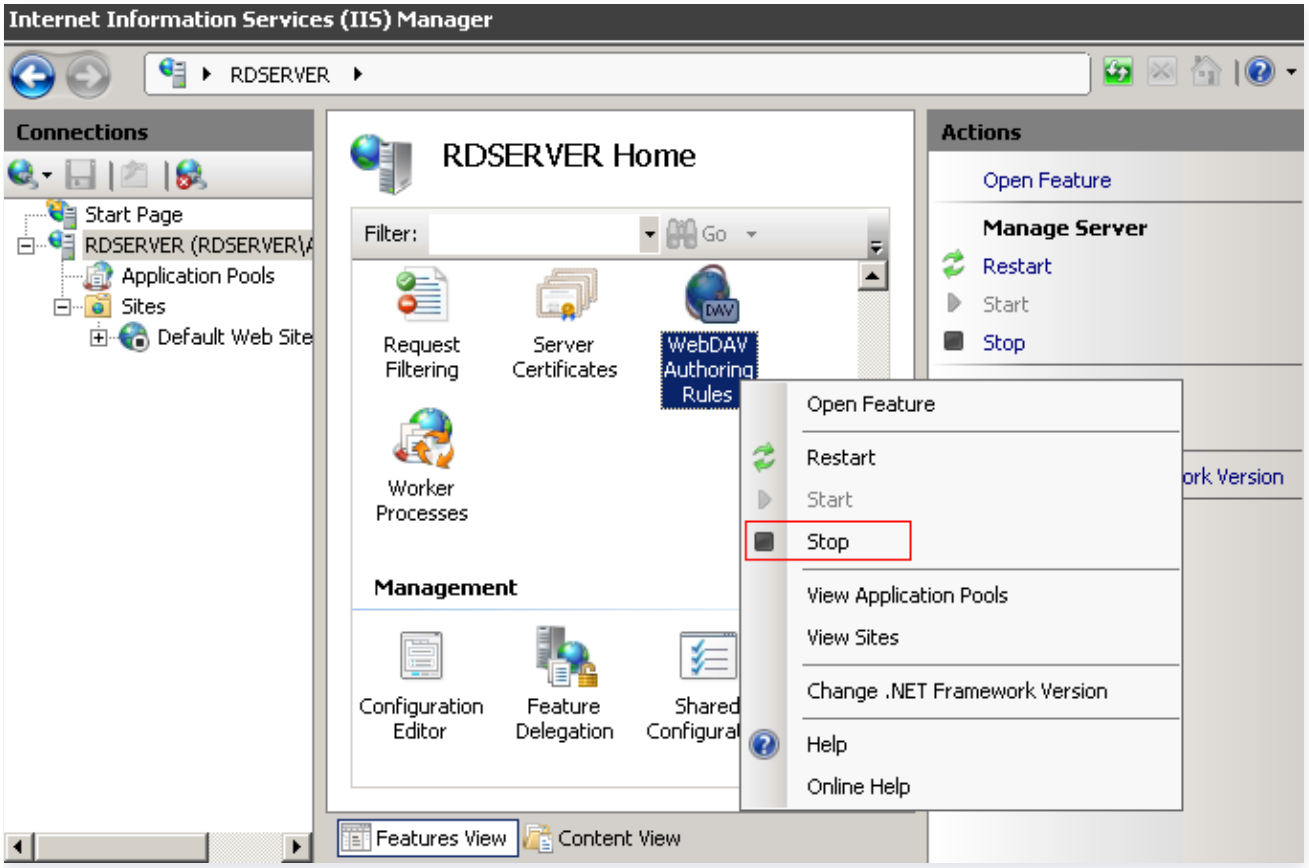
为确保 Web 目录的文件不被非法篡改和删除，应禁止用户对 Web 目录的写权限。



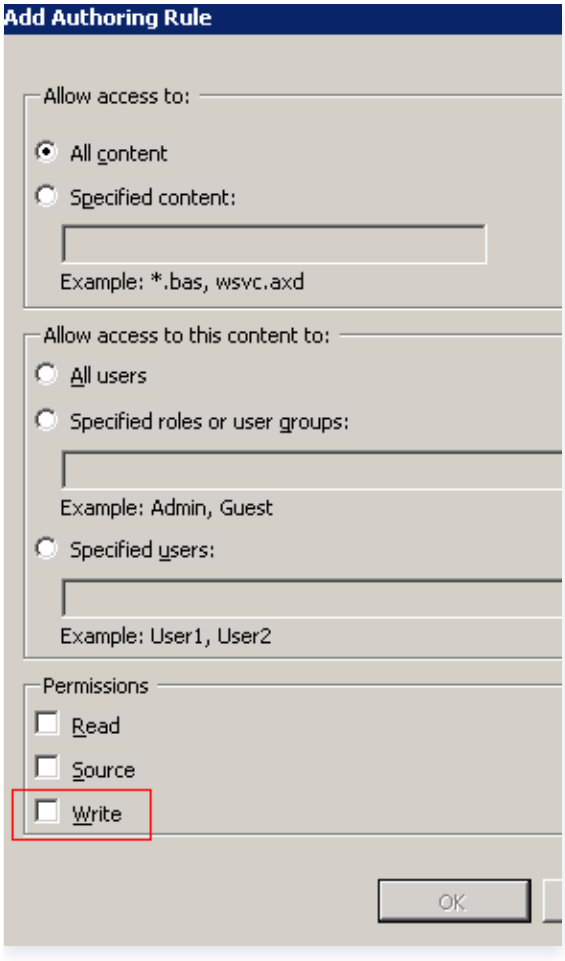


关闭 WebDav

站点若无用户文件操作、文档在线编辑等功能，建议关闭 WebDav 功能。
关闭方法如下图所示：



若必须开启 WebDav，建议禁止 WebDav 目录的“Write”权限：



IIS 访问权限配置

1. 如果 IIS 中有多个网站，建议为每个网站配置不同的匿名访问账户。
2. 新建一个账号，加入Guests 组。
3. “网站属性” > “目录安全性” > “身份验证和访问控制”，将“启用匿名访问”处，用刚新建的账户代替默认账户。

禁用不必要的 Web 服务扩展

打开 IIS 管理器，检查是否有不必要的“ Web 服务扩展”，如果有则禁用掉。

不显示详细的 ASP 错误信息

“ IIS 管理器” > “属性” > “主目录” > “配置” > “调试”，选择“向客户端发送下列文本错误消息”项，自定义出错时返回的错误信息。

修改默认错误页面

“ IIS 管理器” > “属性” > “自定义错误”，用自定义的错误页面替换默认的默认页面。

MySQL 安全优化建议

修改 MySQL 网络监听地址

MySQL 默认配置为绑定所有的 IP，服务器有外网可以被外网访问。为安全起见必须绑定内网 IP，不允许外网访问，可编辑配置文件 my.cnf，在 mysqld 选项中增加一项：`bind_address = 172.16.x.x`，后面的 IP 地址代表需要绑定的内网 IP 地址。

修改 MySQL 默认端口

更改默认端口（默认3306），可以从一定程度上防止端口扫描工具的扫描。
编辑 `/etc/my.cnf` 文件，增加端口参数，并且设定端口，注意该端口未被使用，保存退出。例如：

```
[mysqld]
port=3806
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
```

非 Root 账户运行 MySQL

首先必须要使用独立的受限账户启动 MySQL，一般是系统中用户名和用户组均为 MySQL 的账户，同时把配置文件拷贝到 `/etc` 目录。使用 MySQL 来启动 MySQL 服务：
`/usr/local/mysql/bin/mysqld_safe -user=mysql &` 。

MySQL Root 账户设置密码

5.6 中，rpm 包安装完 MySQL 后，会随机生成一个 root 密码，保存在 `/root/.mysql_secret` 。
5.5 以前，rpm 包安装完 MySQL 后，缺省管理员账户的密码为空，需要对该账户设置密码，可以采用如下办法设置管理员密码：

```
mysql> use mysql;
mysql> update user set password=password('upassword') where user='root';
mysql> flush privileges;
```

删除默认数据库及用户

MySQL 初始化后会自动生成空用户和 test 库，会对数据库安全构成威胁，需要全部删除。可采用如下方法：

```
mysql>drop database test;mysql>use mysql;
mysql>delete from db;
mysql>delete from user where not(host="localhost" and user="root");
mysql>flush privileges;
```

控制远程连接

由于 MySQL 是可以远程连接的，需要控制远程连接的范围，如仅内网访问或不允许网络访问，禁止任意远程账户连接。 可以采用如下方式或者通过防火墙来限制 MySQL 的远程访问。

```
mysql> show grants for username;   //显示账户权限
mysql> grant all on dbname.*  to 'username'@'ip地址' identified by '密码';
```

控制数据库的权限

对于使用 Web 脚本进行交互的数据库，建议建立一个用户只针对某个库有 update、select、delete、insert、drop table、 create table 等权限，减小数据库的用户名和密码被黑客窃取后的影响和损失。控制数据库的权限可参考如下：

```
Mysql> grant select,insert,update,delete,create,drop privileges on dbname.*  To
user1@localhost identified by '密码';
```

数据库名，账户及密码需要根据实际情况填写。

文件读写权限控制

在 Mysql 中，提供对本地文件的读取，使用的是 `load data local infile` 命令，默认在5.0版本中，该选项是默认打开的，该操作令会利用 MySQL 把本地文件读到数据库中，然后用户就可以非法获取敏感信息了，假如您不需要读取本地文件，请务必关闭。
网络上流传的一些攻击方法中就有用它 `LOAD DATA LOCAL INFILE` 的，同时它也是很多新发现的 SQL Injection 攻击利用的手段！黑客还能通过使用 `LOAD DATALOCAL INFILE` 装载 `"/etc/passwd"` 进一个数据库表，然后能用 SELECT 显示它，这个操作对服务器的安全来说，是致命的。
在 my.cnf 中添加：
`local-infile=0` 或者加参数 `local-infile=0` 启动 MySQL。

Redis 安全优化建议

安装下载

使用最新稳定版本，最新版的安全性更高。下载安装命令如下：

```
wget http://download.redis.io/redis-stable.tar.gz
tar zxvf redis-stable.tar.gz
cd redis-stable
make && sudo make install
```

安全启动

- Redis 配置文件里参数至少包括 requirepass 设置访问密码和 bind 只监听内网 IP，以减少安全风险。更改配置命令如下：
  echo "requirepass 密码" >> /etc/redis.conf
  echo "bind 内网IP地址" >> /etc/redis.conf

> **注意**
> 密码长度至少8位，且同时包含大小写字母和数字；内网 IP 地址请自行修改。

- 新建普通用户 Redis 用于降权启动服务，相关命令参考如下：

```
useradd redis -d /home/redis -m          #新建普通用户
chown redis:redis /etc/redis.conf          #修改配置文件属主
chmod 700 /etc/redis.conf                #修改配置文件权限
su - redis                                 #切换至普通用户
redis-server /etc/redis.conf               #启动服务
```

修改默认端口

修改 Redis 默认端口6379为其他端口，打开配置文件 `redis.conf`，如：`vim /etc/redis.conf`，将 port 6379修改为 port xxxx。

端口限制访问

遵循最小化原则，按需分配访问权限，以减少安全风险。Iptables 命令参考如下：

```
iptables -A INPUT -p tcp -s 来源IP地址 --dport 6379 -j ACCEPT
iptables -A INPUT -p tcp --dport 6379 -j DROP
```

> **注意**
> 来源 IP 地址请自行修改；Redis 默认监听端口为6379（TCP），若业务修改成其他端口，这里也要做对应修改。

限制 Redis 文件目录访问权限：

设置 Redis 的主目录权限为700，因为 Redis 密码明文存储在配置文件当中，所以配置文件存放的目录权限修改为600。命令参考如下：`chmod 700 /opt/redis` 、`chmod 600 /opt/redis/conf`

MongoDB 安全优化建议

安装下载：

使用最新稳定版本，最新版的安全性更高。最新版下载地址：`http://www.mongodb.org/downloads` 。

安全配置方案

1. 创建 mongodb 数据库文件夹：
   `mkdir /mongodb/db`
2. 创建 mongodb 日志文件：
   `touch /mongodb/log/mongodb.log`
3. 启动 mongodb 时需要添加— auth 参数，并立即在 admin 数据库创建一个用户（默认情况下 MongoDB 是无需验证的，所以这是至关重要的一步。）
   ```
   ./mongod --dbpath /mongodb/data --logpath /mongodb/log/mongodb.log --nohttpinterface --auth
   ```
4. 启动的时候需要加上 -- nohttpinterface 参数，取消默认 Web 管理页面。
5. 非 root 权限启动 mongodb，在机器上登录非 root 账户，给予 mongodb 程序和数据库文件夹，日志文件的该账户读写执行权限。

端口限制访问

```
iptables -A INPUT -p tcp -s 来源IP地址 --dport 27017 -j ACCEPT
iptables -A INPUT -p tcp --dport 27017 -j DROP
```

> **说明**
> 来源 IP 地址请自行修改；mongodb 默认监听端口为27017，若业务修改成其他端口，请做对应修改。且 monggodb 端口禁止对外网访问。

文件目录限制

- 配置文件只允许属主读取和修改、属组读取。
- `chmod 640/usr/local/mongodb/mongodb.conf`
- 数据目录只允许属主读取和修改。
- `chmod 700 /usr/local/mongodb/data/`
- 日志文件目录只允许属主读取和修改、属组读取。
- `chmod 740 /usr/local/mongodb/log/`

Jboss 安全优化建议

设置目录权限

修改 `deploy\jbossdomain\deploy\jbossweb-tomcat55.sar\conf\` 下面的 web.xml 文件中的如下内容：

```
<init-param>
<param-name>listings</param-name>
```

```
<param-value>false</param-value>
</init-param>
```

将 “param-value” 默认值 true 改为 false。

删除危险服务：

Jboss 中存在较多容易出现安全漏洞的组件，需要把 jmx-console 和 web-console 控制台删除，建议直接删除避免引入安全漏洞风险：

- **删除 Jboss 的 /web-console 控制台：**
  删除 `JBOSS_HOME/server/default/deploy/jbossweb-tomcat55.sar` 目录下的 `root.war` 。
  删除 `JBOSS_HOME/server/default/deploy/management/console-mgr.sar/web-console.war` 。
- **删除 Jboss 的 /jmx-console 控制台：**
  删除 `JBOSS_HOME/server/default/deploy/jmx-console.war` 以及其他目录下的 `jmx-console.war` 文件。
  删除 `JBOSS_HOME/server/default/deploy/jbossws.sar/jbossws-context.war` 以及其他目录下的 `jbossws-context.war` 文件。
  删除 `JBOSS_HOME/server/default/deploy/jboss-web.deployer/context.xml`
- **删除 Jboss 的 http-invoker：**
  删除 `JBOSS_HOME/server/default/deploy/http-invoker.sar` 目录。
  测试一下：
  `<http://XXXX/jmx-console/>`
  `<http://XXXX/web-console>`

> **注意**
> 端口使用实际的，访问不到页面就成功了。

限制危险服务：

设置 Jboss 的 Bootstrap JNP、RMI naming service 服务只允许本地访问。
修改 server/default/conf 下的 jboss-service.xml 文件内容以及其他目录下的 jboss-service.xml 文件。
修改 Bootstrap JNP（端口1099）和 RMI naming service(1098)只允许本地访问。

```
<mbean code="org.jboss.naming.NamingService"
name="jboss:service=Naming"
xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
<attribute name="CallByValue">false</attribute>
<attribute name="Port">1099</attribute>
<attribute name="BindAddress">127.0.0.1</attribute>
<attribute name="RmiPort">1098</attribute>
<attribute name="RmiBindAddress">127.0.0.1</attribute>
<depends optional-attribute-name="LookupPool"
proxy-type="attribute">jboss.system:service=ThreadPool</depends>
```

```
<depends optional-attribute-name="Naming"
proxy-type="attribute">jboss:service=NamingBeanImpl</depends>
</mbean>
```

vsFTPd 安全优化建议

安装部署：

在 `<http://vsftpd.beasts.org/#download>` 下载最新版 vsftp 源码包，编译安装。

关闭匿名访问功能：

如业务无必要，可关闭匿名访问功能，修改 VSFTP 配置文件 vsftpd.conf，修改以下配置，关闭匿名访问：
`anonymous_enable=NO`

禁止 VSFTP 显示 Banner，防止泄露版本信息：

1. 登录 FTP 服务器，查看是否显示 Banner：

```
C:\>ftp 192.168.10.1
Connected to 192.168.10.1
220 (vsftpd 2.0.5)
User (192.168.10.1:(none)):
```

2. 修改 VSFTP 配置文件 vsftpd.conf，修改以下语句：

```
ftpd_banner=Welcome
```

3. 重新启动 VSFTP 后，查看 Banner：

```
C:\>ftp 192.168.10.1
Connected to 192.168.10.1
220 Welcome
User (192.168.10.1:(none)):
```

如允许匿名用户上传文件，建议配置只写目录：

找到 `/ var/ftp/pub` 目录，通过如下命令创建只写目录：
`mkdir /var/ftp/pub/upload_files`

限制 FTP 匿名用户访问上传文件目录：

`chmod 730 /var/ftp/pub/upload_files`

开启日志记录：

修改 VSFTP 配置文件 vsftpd.conf，修改以下行，启用日志记录：

```
xferlog_enable=YES
xferlog_file=/var/log/xferlog
dual_log_enable=YES
vsftpd_log_file=/var/log/vsftpd.log
use_localtime=YES
```

SFTP 默认只有上下传记录，没有用户登录等信息的记录。按照上述加固方法，可以在 `/var/log/vsftpd.log` 查看用户登录记录，创建目录删除目录等信息。

Jetty 安全优化建议

禁止目录浏览

修改 etc/webdefault.xml：

```
<init-param>
<param-name>dirAllowed</param-name>
<param-value>false</param-value>
</init-param>
```

限定文件解析类型

修改 etc/webdefault.xml，只保留 jsp 相关解析：

```
<servlet-mapping>
<servlet-name>jsp</servlet-name>
<url-pattern>*.jsp</url-pattern>
<url-pattern>*.JSP</url-pattern>
</servlet-mapping>
```

控制文件权限

```
chmod 755 jetty/etc/*
```

禁止 CGI

删除 `contexts/test.d` 这个和下面那个不删也行，启动会报错，但是不影响使用。
删除 `contexts/test.xml`
删除 `webapps/` 目录下的 `test.war` 文件。

隐藏服务器版本信息

修改 `etc/jetty.xml` ,此处默认是 true，修改为 false：

```
<Set name="sendServerVersion">false</Set>
```

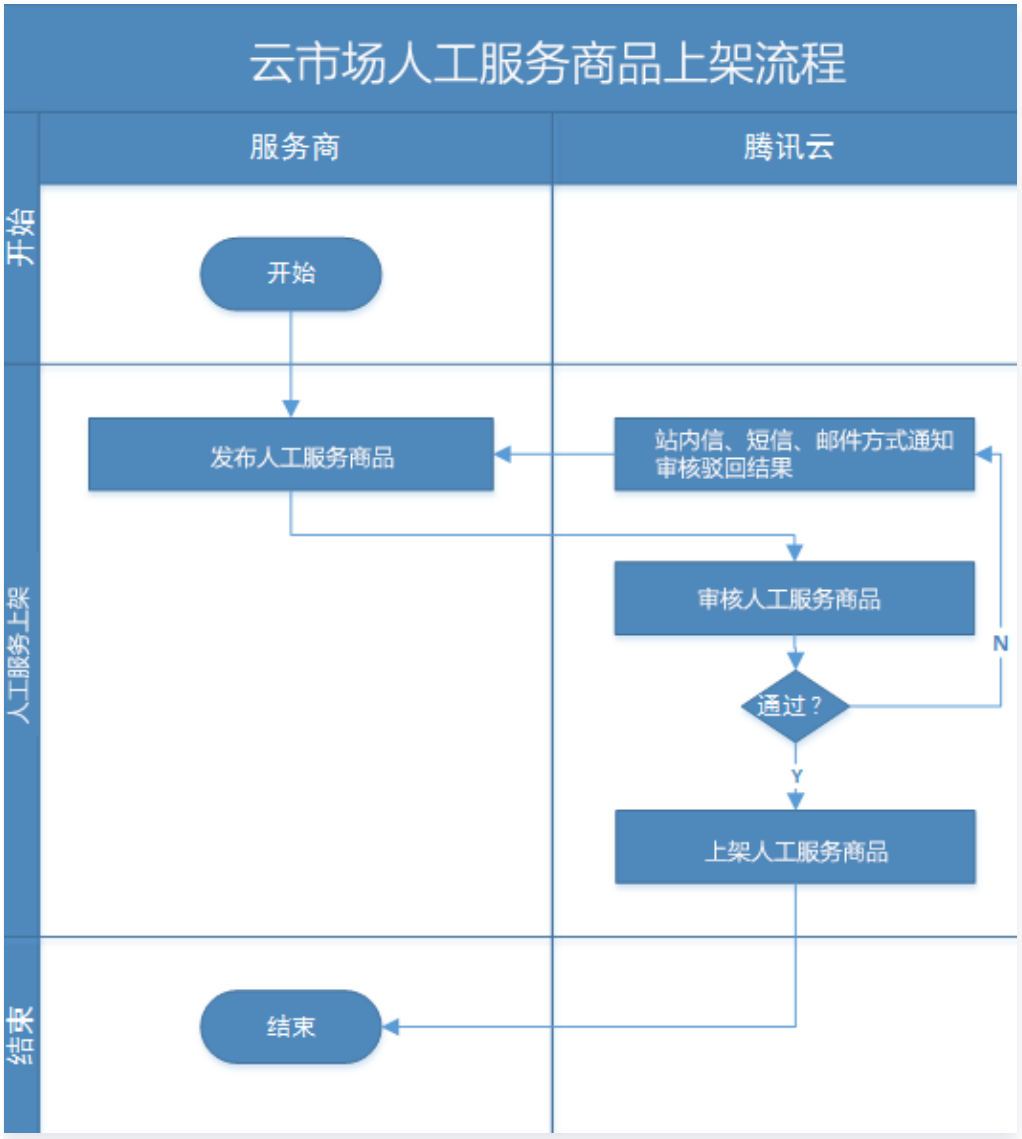
人工服务

最近更新时间：2024-10-10 14:33:21

简介

人工交付服务商品，是由服务商为腾讯云用户提供人工服务，不交付具体的软件或云资源，如服务器运维、数据迁移、授权软件安装服务等。人工交付适用于技术运维服务市场、定制服务市场、应用授权市场、安全市场、企业管家市场。为避免人工服务出现的交易纠纷，云市场为用户与服务商提供服务过程的监管功能。
本文主要引导您完成人工交付类商品上架和订单实施。

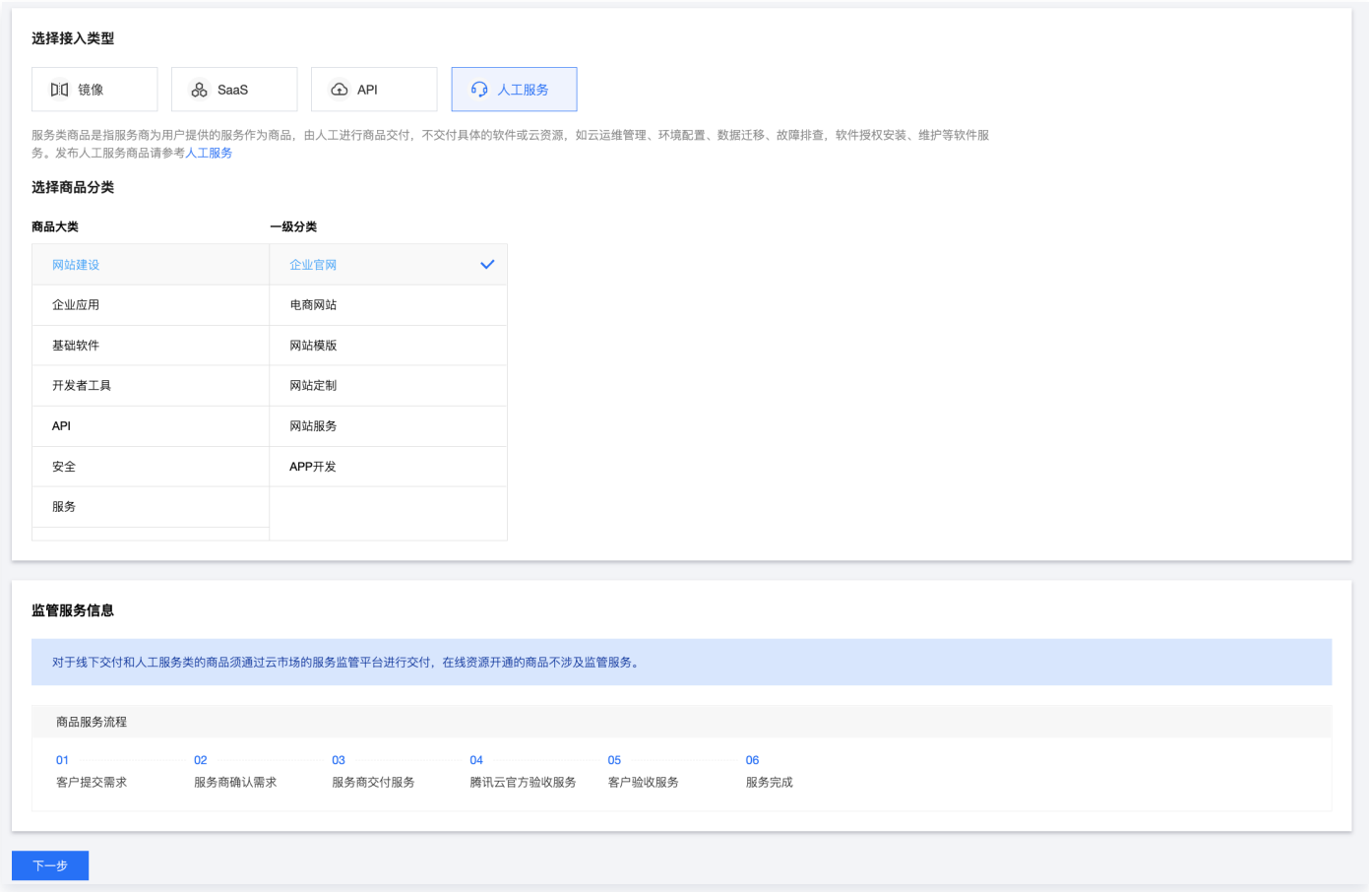
商品上架流程



上架操作步骤

1. 登录 云市场服务商管理控制台，选择左侧菜单栏**商品管理 > 商品列表**。
2. 进入商品列表页面，单击**新建商品**。

3. 选择商品的接入类型“人工服务”。
4. 根据商品的功能及使用场景，选择正确的商品分类。



5. 填写人工服务商品的接入信息、基本信息、业务信息、销售信息。

- **接入信息**

信息	填写说明
商品名称	必填，输入商品名称，80字内。
计费计入方式	第三方商品默认云市场定价，非自研商品云计费定价。
交付时长	必填，商品订单约定最长交付时间。
商品服务流程	人工服务商品默认接受平台监管，人工服务商品订单交付流程及监管流程详细可查看 交付中心 文档介绍。
需求模板	选填，商品下单后，需要用户下单后提交的需求内容。

- **基本信息**

信息	填写说明
商品图片	必填，至少上传1张商品配图，图片大小用于展示在列表页、详情页头部的展示，商品配图需符合 商品审核规范，图片大小不得超过2M，尺寸：390 x 260px，分辨率72dpi。
商品视频	选填，商品视频用于商品详情页展示，会增加曝光的机会；视频支持 mp4 格式，分辨率 1280*720 px，大小不超过 100MB，第一帧不能出现全黑或全白。
商品亮点	必填，介绍产品的亮点，后续商品若上架资源位，将在资源位介绍栏目呈现，文字长度请控制在 8 – 16 个字符内。
商品简介	必填，简要描述您的商品优势和价值，140字以内。
商品功能特性	选填，介绍产品核心功能和服务商，区别于同类商品的特性，500字以内。
商品详情	必填，详细描述服务内容，包括不限于：服务介绍、服务流程、使用方法、交付物、帮助文档、过往案例、客户评价。支持图文展示，不支持添加外链。
使用指南	必填，支持本地文档上传，文档格式：PDF、Word、PPT、ZIP、RAR，大小：不超过2M。
售后服务说明	必填，请按照实际服务内容填写支持的服务范围、时间范围、业务范围、费用范围等信息，500 字以内。
商品资质	选填，请上传产品取得的相关资质信息，如：软件著作权证书、开源软件声明或其他资质证书。用以在详情页展示给用户查阅。
客户案例	选填，商品以往服务客户的案例信息，支持图文展示，不支持添加外链。

- **业务信息**

信息	填写说明
商品分类	必填，选择商品上架后的展示栏目。
商品标签	必填，选择一至五个标签以描述商品的属性，回车即可添加新标签。
适用规模	必填，选择产品服务规模。
适用行业	必填，选择一至五个产品主要服务行业，回车即可添加。
适用场景	必填，选择一至五个适用场景，回车即可添加。
商品服务协议	必填，勾选相应协议或者新增协议。《商品服务协议》的内容请参考 云市场《商品服务协议》上线的通知 。
应用开通信息	选填，设置此项后客户在下单时需要填写客户信息才可提交订单。

- **销售信息**

信息	填写说明
是否公开销售	必填，选择“是”，商品上架后可在云市场公开展示和搜索；选择否商品信息将无法搜索，仅支持链接进入商品详情页售卖。
售卖方式	必填，选择商品的计费方式及规格周期设置，详细指引可查看文档 关于 SaaS 和人工交付类商品规格周期设置的说明 。

6. 商品信息填写过程中，您可随时单击页面最下方的保存草稿随时保存商品信息。
7. 单击**上一步**可返回上个界面修改信息。
8. 单击提交审核可将商品提交审核，提交后商品为“审核中”状态，云市场运营人员会在**7个工作日**左右完成审核。
9. 商品提交审核后，在商品管理列表页中，可单击商品名称进入商品预览页，如商品仍需修改，单击**撤销审核**，重新编辑商品信息后，提交审核即可。

相关文档

如需了解更多商品管理信息，请参见 商品管理 。

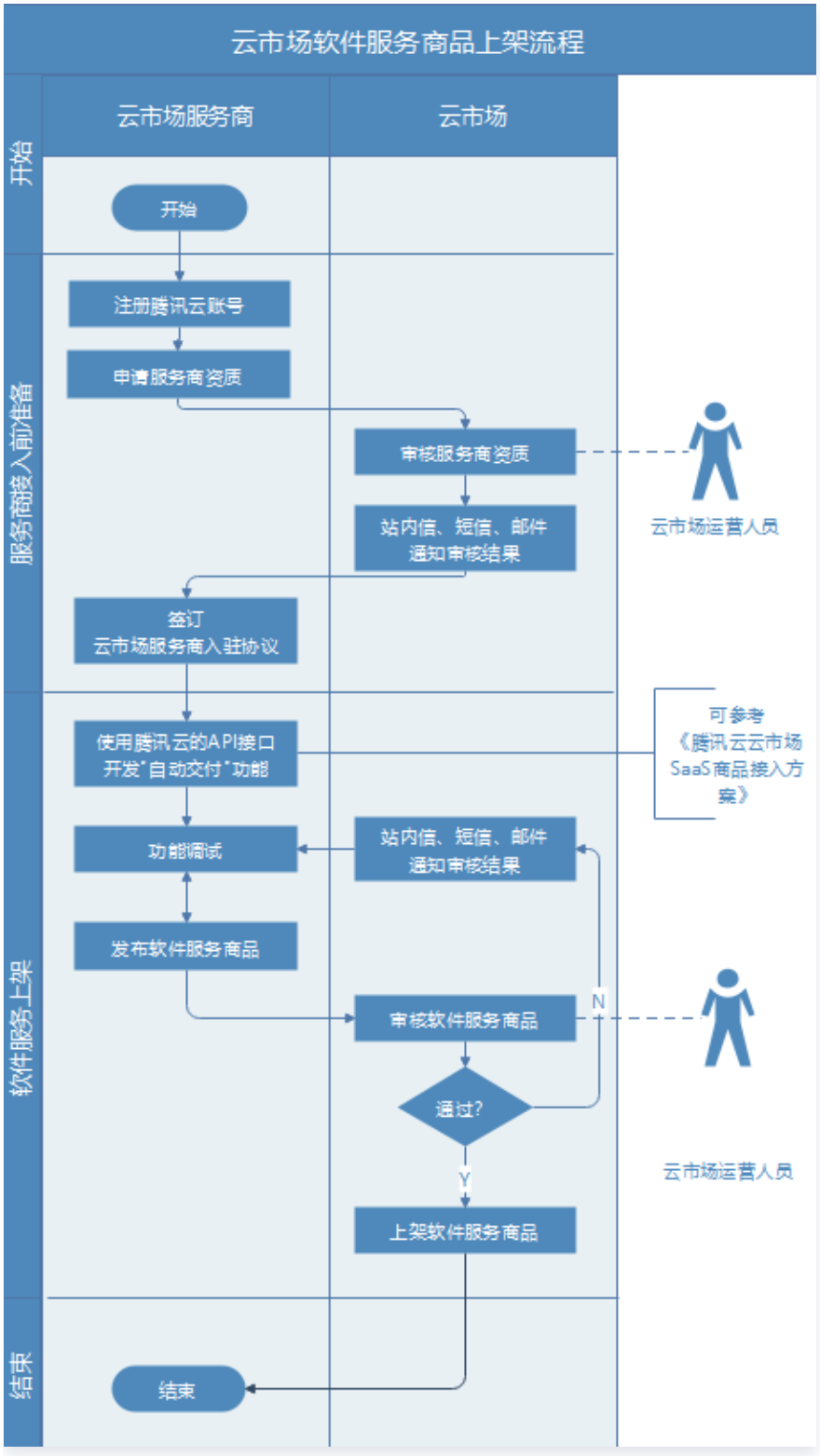
SaaS 服务

最近更新时间：2024-10-10 14:33:21

简介

云市场 SaaS 服务提供“自动交付”的接入方式：相较于传统的兑换码换商品方式，自动交付可以给用户更佳的用户体验，从而获得腾讯云更多的流量推荐。该方式下，用户购买后会接收应用访问 URL 地址，通过服务商提供的账号密码访问或免登 URL 访问应用，直接使用服务。同时，支持版本升级、续费等特性。

上架流程

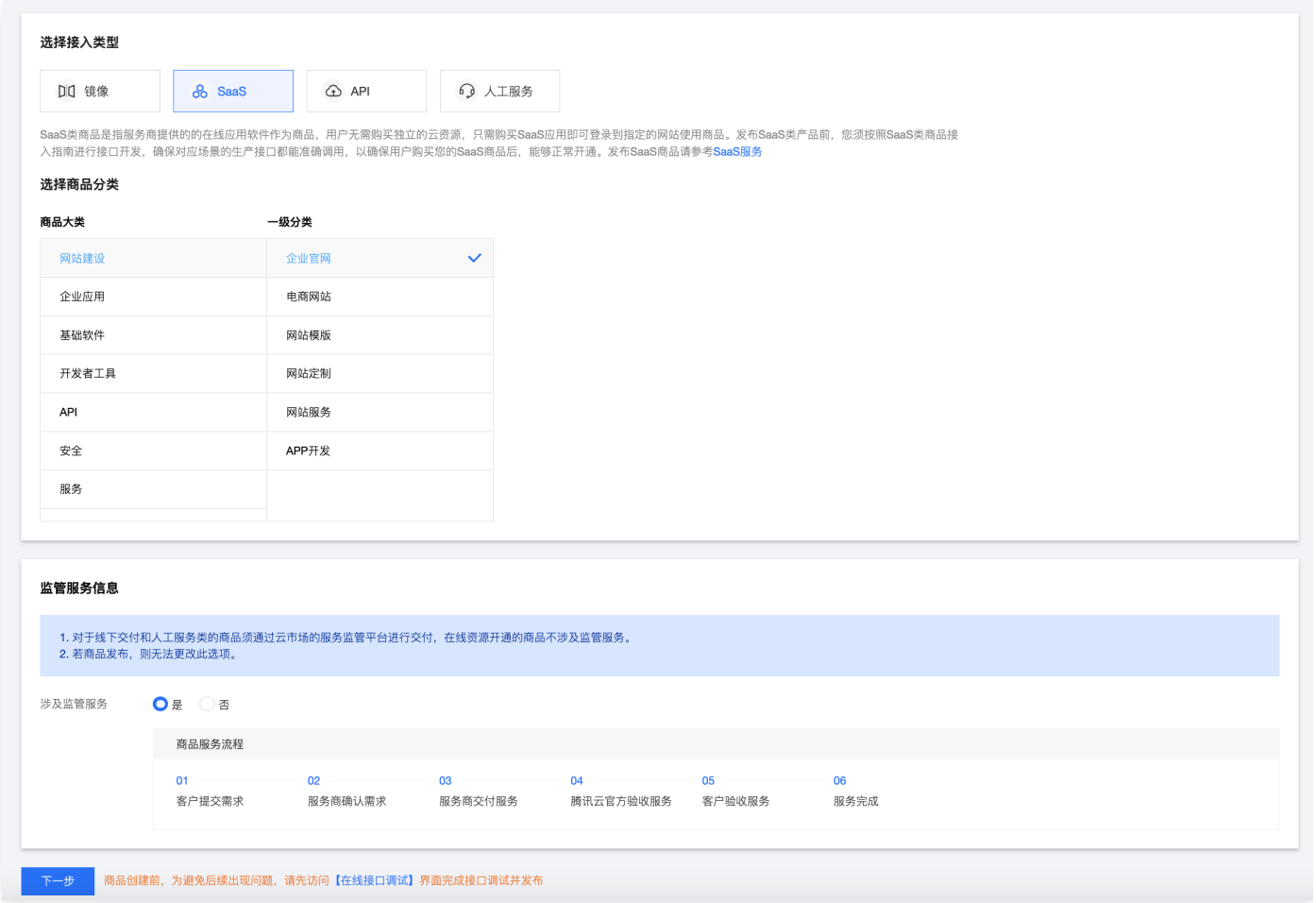


操作步骤

为了保证服务商可自动接收到客户在云市场发生的购买、续费、退款等一系列行为的消息通知，云市场提供了发货接口的 API 文档，需服务商参考 自动交付接入方案 进行 API 接口开发，以实现相关消息通知功能，主要包括创建实例、续费通知、配置变更通知、退款通知等。

完成 API 开发后，登录 云市场服务商管理控制台，选择左侧菜单栏**开发配置 > 在线接口调试**，填写测试地址，调试相关接口。完成 API 的开发和测试后，服务商方可进行 SaaS 商品创建，具体操作如下：

1. 登录 云市场服务商管理控制台，选择左侧菜单栏**商品管理 > 商品列表**。
2. 进入商品列表页面，单击**新建商品**。
3. 选择商品的接入类型“SaaS”。
4. 根据商品的功能及使用场景，选择正确的商品分类。
5. 如果发布的 SaaS 商品需要通过线下人工实施服务，勾选**是**，涉及监管服务。如果发布的 SaaS 商品属于在线资源开通的商品，勾选**否**，不涉及监管服务。



6. 填写 SaaS 服务商品的接入信息、基本信息、业务信息、销售信息。

- **接入信息**

信息	填写说明
商品名称	必填，输入商品名称，80字内。
计费计入方式	第三方商品默认云市场定价，非自研商品云计费定价。
生产系统接口地址	必填，服务商按照 自动交付接入方案 接入完成后将会有相应接口地址可选。

涉及监管	SaaS服务商品默认不选择平台监管，选择后将按照人工交付流程管理订单，不支持自动交付，需要服务商手动交付，订单支持续费；若商品发布，则无法更改此选项。

- **基本信息**

信息	填写说明
商品图片	必填，至少上传1张商品配图，图片大小用于展示在列表页、详情页头部的展示，商品配图需符合 商品审核规范，图片大小不得超过2M，尺寸：390 × 260px，分辨率72dpi。
商品视频	选填，商品视频用于商品详情页展示，会增加曝光的机会；视频支持 MP4 格式，分辨率 1280 × 720px，大小不超过 100MB，第一帧不能出现全黑或全白。
商品亮点	必填，介绍产品的亮点，后续商品若上架资源位，将在资源位介绍栏目呈现，文字长度请控制在8个 – 16个字符内。
商品简介	必填，简要描述您的商品优势和价值，140字以内。
商品功能特性	选填，介绍产品核心功能和服务商，区别于同类商品的特性，500字以内。
商品详情	必填，详细描述服务内容，包括不限于：服务介绍、服务流程、使用方法、交付物、帮助文档、过往案例、客户评价。支持图文展示，不支持添加外链。
使用指南	必填，支持本地文档上传，文档格式：PDF、Word、PPT、ZIP、RAR，大小：不超过2M。
售后服务说明	必填，请按照实际服务内容填写支持的服务范围、时间范围、业务范围、费用范围等信息，500字以内。
商品资质	选填，请上传产品取得的相关资质信息，如：软件著作权证书、开源软件声明或其他资质证书。用以在详情页展示给用户查阅。
客户案例	选填，商品以往服务客户的案例信息，支持图文展示，不支持添加外链。

- **业务信息**

信息	填写说明
商品分类	必填，选择商品上架后的展示栏目。
商品标签	必填，选择一至五个标签以描述商品的属性，回车即可添加新标签。
适用规模	必填，选择产品服务规模。
适用行业	必填，选择一至五个产品主要服务行业，回车即可添加。
适用场景	必填，选择一至五个适用场景，回车即可添加。

商品服务协议	必填，勾选相应协议或者新增协议。《商品服务协议》的内容请参考 云市场《商品服务协议》上线的通知 。
应用开通信息	选填，设置此项后客户在下单时需要填写客户信息才可提交订单。

- **销售信息**

信息	填写说明
是否公开销售	必填，选择“是”，商品上架后可在云市场公开展示和搜索；选择否商品信息将无法搜索，仅支持链接进入商品详情页售卖。
售卖方式	必填，选择商品的计费方式及规格周期设置，详细指引可查看文档 关于 SaaS 和人工交付类商品规格周期设置的说明 。

7. 商品信息填写过程中，您可随时单击页面最下方的保存草稿随时保存商品信息。
8. 单击**上一步**可返回上个界面修改信息。
9. 单击提交审核可将商品提交审核，提交后商品为“审核中”状态，云市场运营人员会在**7个工作日**左右完成审核。
10. 商品提交审核后，在商品管理列表页中，可单击商品名称进入商品预览页，如商品仍需修改，单击**撤销审核**，重新编辑商品信息后，提交审核即可。

相关文档

如需了解更多商品管理信息，请参见 商品管理 。

API 服务

最近更新时间：2024-10-10 14:33:21

简介

服务商提供的 API 服务可以是算法或者数据的集成，开发者选购 API 服务后，可以通过服务的调用地址来获取相关的服务（算法或数据）。为保证腾讯云用户正常使用 API 服务，服务商需要在腾讯云网关上部署相关 API 服务，如何部署接入API请查看 云市场 API 网关操作说明 。

上架流程

1. 服务商发布 API 服务至发布环境，操作详情可参见 云市场 API 网关操作说明 。
2. 服务商上架 API 服务商品，并申请审核。
3. 腾讯云审核商品信息。

操作步骤

1. 登录 云市场服务商管理控制台 ，选择左侧菜单栏**商品管理 > 商品列表**。
2. 进入商品列表页面，单击**发布商品>集市商品**。
3. 选择商品的接入类型“API”，填写 API 服务商品的接入信息、基本信息、业务信息、销售信息。

- **接入信息**

信息	填写说明
商品名称	必填，输入商品名称，长度不超过50个字符，名称与商品内容相符，禁止出现重复词汇。
接入API	必填，服务商需要在云市场API网关上部署相关 API 服务，鉴权方式选择“密钥对”鉴权。创建完成后可选择对应服务资源上架，创建流程具体请参考 云市场 API 网关操作说明 。

- **基本信息**

信息	填写说明

商品图片	必填，至少上传1张商品配图，图片大小用于展示在列表页、详情页头部的展示，商品配图需符合 商品审核规范，图片大小不得超过2M，尺寸：390 x 260px，分辨率72dpi。
商品视频	选填，商品视频用于商品详情页展示，会增加曝光的机会；视频支持 MP4 格式，分辨率1280 x 720px，大小不超过100MB，第一帧不能出现全黑或全白。
商品亮点	必填，介绍产品的亮点，后续商品若上架资源位，将在资源位介绍栏目呈现，文字长度请控制在8个 - 16个字符内。
商品简介	必填，简要描述您的商品优势和价值，140字以内。
商品功能特性	选填，介绍产品核心功能和服务商，区别于同类商品的特性，500字以内。
商品详情	必填，详细描述服务内容，包括不限于：服务介绍、服务流程、使用方法、交付物、帮助文档、过往案例、客户评价。支持图文展示，不支持添加外链。
使用指南	必填，支持本地文档上传，文档格式：PDF、Word、PPT、ZIP、RAR，大小：不超过2M。
售后服务说明	必填，请按照实际服务内容填写支持的服务范围、时间范围、业务范围、费用范围等信息，500字以内。
商品资质	选填，请上传产品取得的相关资质信息，如：软件著作权证书、开源软件声明或其他资质证书。用以在详情页展示给用户查阅。
客户案例	选填，商品以往服务客户的案例信息，支持图文展示，不支持添加外链。

- **业务信息**

信息	填写说明
商品分类	必填，选择商品上架后的展示栏目。
商品标签	选填，选择一至五个标签以描述商品的属性，回车即可添加新标签。
适用规模	选填，选择产品服务规模。
适用行业	选填，选择一至五个产品主要服务行业，回车即可添加。
适用场景	选填，选择一至五个适用场景，回车即可添加。
商品服务协议	必填，勾选相应协议或者新增协议。《商品服务协议》的内容请参考 云市场《商品服务协议》上线的通知 。

- **销售信息**

信息	填写说明

是否公开销售	必填，选择“是”，商品上架后可在云市场公开展示和搜索；选择否商品信息将无法搜索，仅支持链接进入商品详情页售卖。
售卖方式	必填，API 售卖方式为按次计费，服务商自行制定调用次数所需费用规格；API 规格上线后将不支持删除，API 商品上架要求所有规格都必须上线。
授权折扣	必填，授权给腾讯云可对最终客户销售的最低折扣，用于腾讯云销售的拓客。
商品规格	必填，根据售卖意愿填写规格内容、规格定价、规格配额和购买限制。

4. 商品信息填写过程中，您可随时单击页面最下方的保存草稿随时保存商品信息。
5. 单击**上一步**可返回上个界面修改信息。
6. 单击提交审核可将商品提交审核，提交后商品为“审核中”状态，云市场运营人员会在**7个工作日**左右完成审核。
7. 商品提交审核后，在商品管理列表页中，可单击商品名称进入商品预览页，如商品仍需修改，单击**撤销修改**，重新编辑商品信息后，提交审核即可。

相关文档

如需了解更多商品管理信息，请参见 商品管理 文档。

云市场 API 网关操作说明

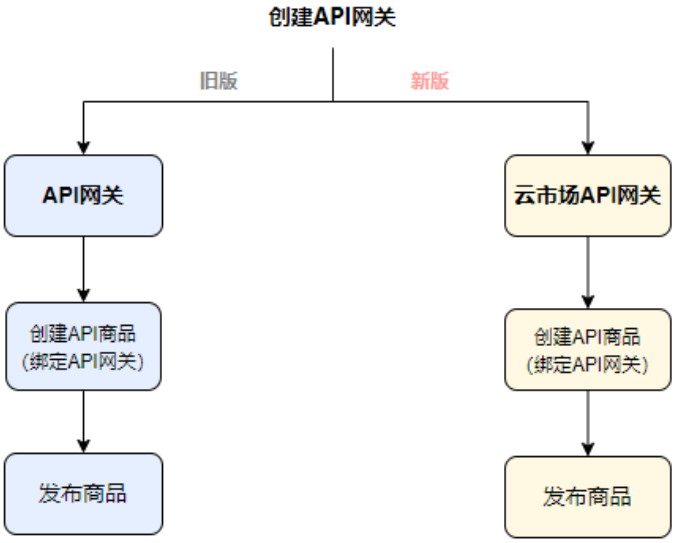
最近更新时间：2025-04-18 17:48:21

背景

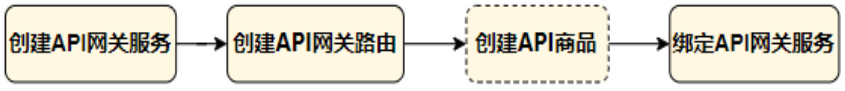
由于腾讯云产品业务调整，API 网关产品将做如下调整：2024年07月01日00:00，产品停止售卖，范围是新、老用户无法再购买或创建资源，包含实例、服务、资源包。新用户指从未创建过 API 网关资源的用户。老用户已在使用中的服务暂不受影响。API 停售公告详情查看：【重要】API 网关产品停止售卖公告 。
2024年07月01日之前通过 API 网关**已经创建的 API 服务可以继续选择“API网关”**发布云市场 API 商品；2024年07月01日后**新增 API 服务请使用云市场 API 网关**创建 API 服务，并且发布商品时需要选择"云市场API网关”中的 API 服务。

基本介绍

腾讯云产品业务调整后，发布 API 商品时，API 的创建动作由从 API 网关侧转移到云市场侧，本文主要引导您完成云市场 API 网关服务的创建和调试。



操作流程



1. 登录 API网关服务，选择“**新建服务**”。

2. **创建 API 服务**。在创建过程中，需要填写名称、选择服务所属的地域、同意服务条款。API 网关服务创建成功后，**在未绑定商品前，可对该服务进行编辑、删除和新建 API 的操作**。
3. **创建 API** 。单击对应网关操作栏的“**新建API**”，在此网关服务基础上创建一个 API。在创建 API 时，分为三个步骤，前端路由、后端服务、响应参数。当外部请求到达 API 网关时，它会根据路由规则转发到相应的后端服务进行处理。**创建后可在 API 网关服务 > API 列表**处单击 ID 名称查看路由详情。

4. **绑定 API 商品**。在创建 API 商品的过程中，需要选择绑定之前创建的 API 网关服务，让 API 商品继承 API 网关服务的相关配置，包括路由规则、后端服务地址等在完成 API 商品的创建及发布后供外部用户调用。

配置参数

创建 API 产品需要配置服务参数及API 参数。

服务参数

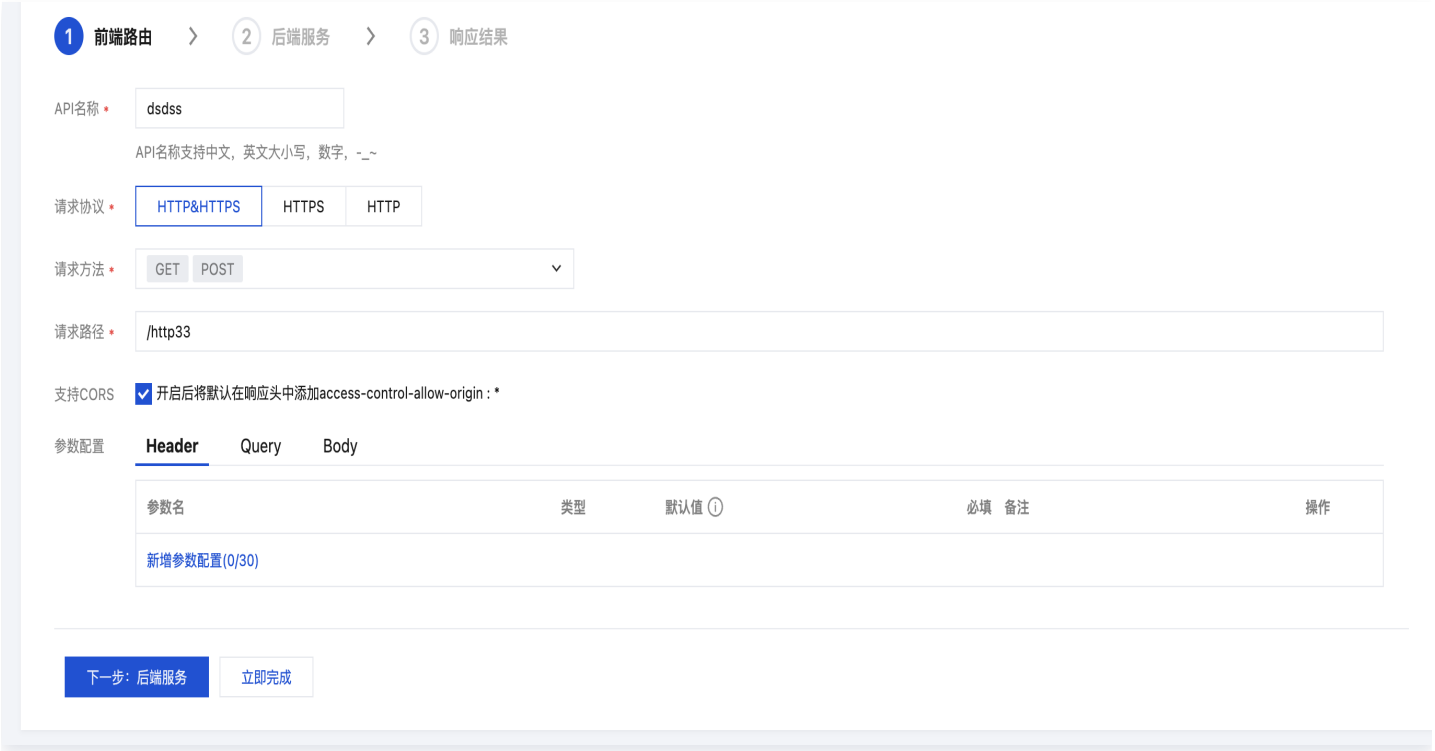
字段配置	说明
服务名称	在单个地域内，服务名称必须是唯一的，且长度不得超过50个字符。

所属地域	不同地域的对外接口地址会有所不同，如果一个服务选择一个地域，后续不可更改。例如，如果选择了广州地域，网关最终部署在广州，对应的域名将为：ap-guangzhou.cloudmarket-apigw.com。 支持的地域列表： • 上海：ap-shanghai.cloudmarket-apigw.com • 广州：ap-guangzhou.cloudmarket-apigw.com • 北京：ap-beijing.cloudmarket-apigw.com

API 参数

创建 API 分为三个部分，如下文描述。

前端路由



字段配置	说明
API 名称	在单服务内，API 名称必须是唯一的，不能与其他 API 名称重复。API 名称长度需在50个字符以内。
请求方法	指对外进行 API 调用时所使用的 HTTP 方法，如 GET、POST、PUT 等，支持多选。
请求路径	用户需要自定义一个对外暴露的路径，该路径将追加到对外请求地址的末尾。当请求转发到服务商后端服务时，此路径不会包含在内。例如，若请求路径设置为 /index，对外

	请求域名为 example.market.tencent.com，则完整的对外请求路径将是 example.market.tencent.com/index。
参数配置（ 参数配置用于生成接口文档供用户使用 ）	• Query：查询参数将会拼接到 URL 路径的末尾，以问号（?）分隔。例如，若 URL 路径为 /search，查询参数为keyword=test，则完整的请求 URL 将是 /search?keyword=test； • Body：请求体参数适用于需要发送大量数据的场景，支持配置 JSON 结构。该部分数据会填充到 HTTP 请求的 body 消息体中； • Header：头部参数将会设置到 HTTP 请求头中，用于传递额外信息或进行身份验证等操作。常见的头部参数包括 Content-Type、Request-ID 等。
支持 CORS	当选择 CORS 复选框，开启后将默认在响应头中添加 access-control-allow-origin:*

后端服务

字段配置	说明
服务地址	后端服务域名或者 IP 地址。
服务端口	一般 http 默认端口为80，https 默认端口为443，也可以选择自定义的端口。

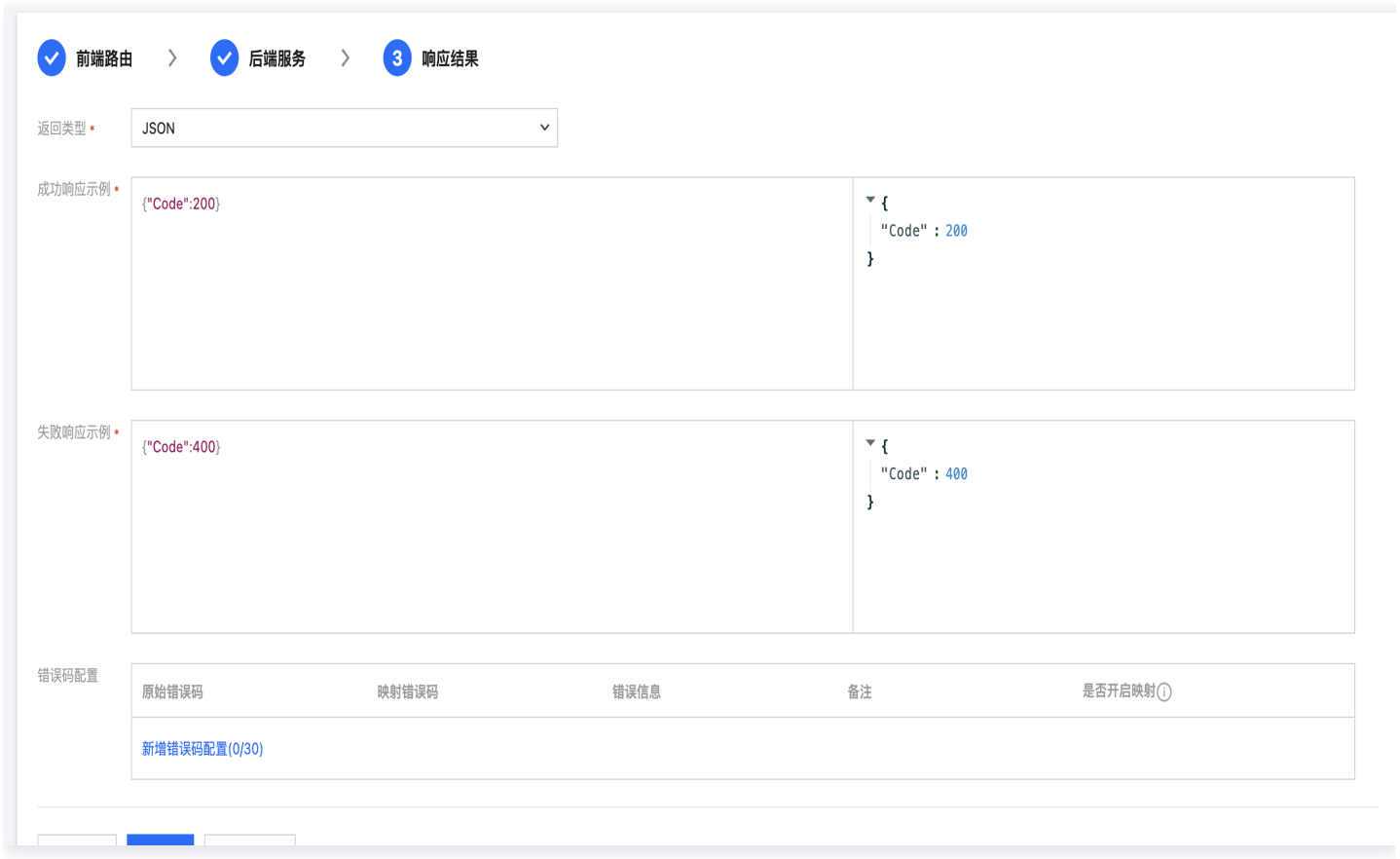
服务协议	选择使用 HTTP 或 HTTPS 协议。请注意，当您选择 HTTPS 协议时，服务端口必须选择 HTTPS 配置的端口。
服务路径	必须以“/”开头。
超时时间	用户请求经过网关后，和后台连接持续时间，超过这个时间会自动连接，默认 3000ms，不超过 10s。
重试次数	如果一次请求服务不通过，会进行≤ **重试次数**的请求，在网络条件不好的时候，建议重试次数较高。
API 鉴权参数	针对服务商的一些需求，服务商以一些固定的参数配置在网关。在用户发起请求后，固定的参数通过 path 或者 header 中传递给服务商，具体内容参考 请求及返回 。 **添加鉴权参数：**单击网关操作栏的“API 鉴权参数”。 支持鉴权参数类型： • Header：这个类型的参数会以 json 形式填写在 Header 中的 X-Auth-Config-Header 中。 • Query：将配置好的查询参数添加到 url 的query参数中。 • HeaderOrg: 将配置的参数填写在请求头中。注意名称不能含有 “_”。 • Body：将配置参数写入到 Body 中，不过仅支持 application/x-www-form-urlencoded 类型，其他类型自动忽略这个参数。

示例

假设服务商后端接口路径是：https://example.market.tencent.com/testadd，则各项值如下：

- 服务地址：example.market.tencent.com
- 服务端口：443
- 服务路径：/testadd

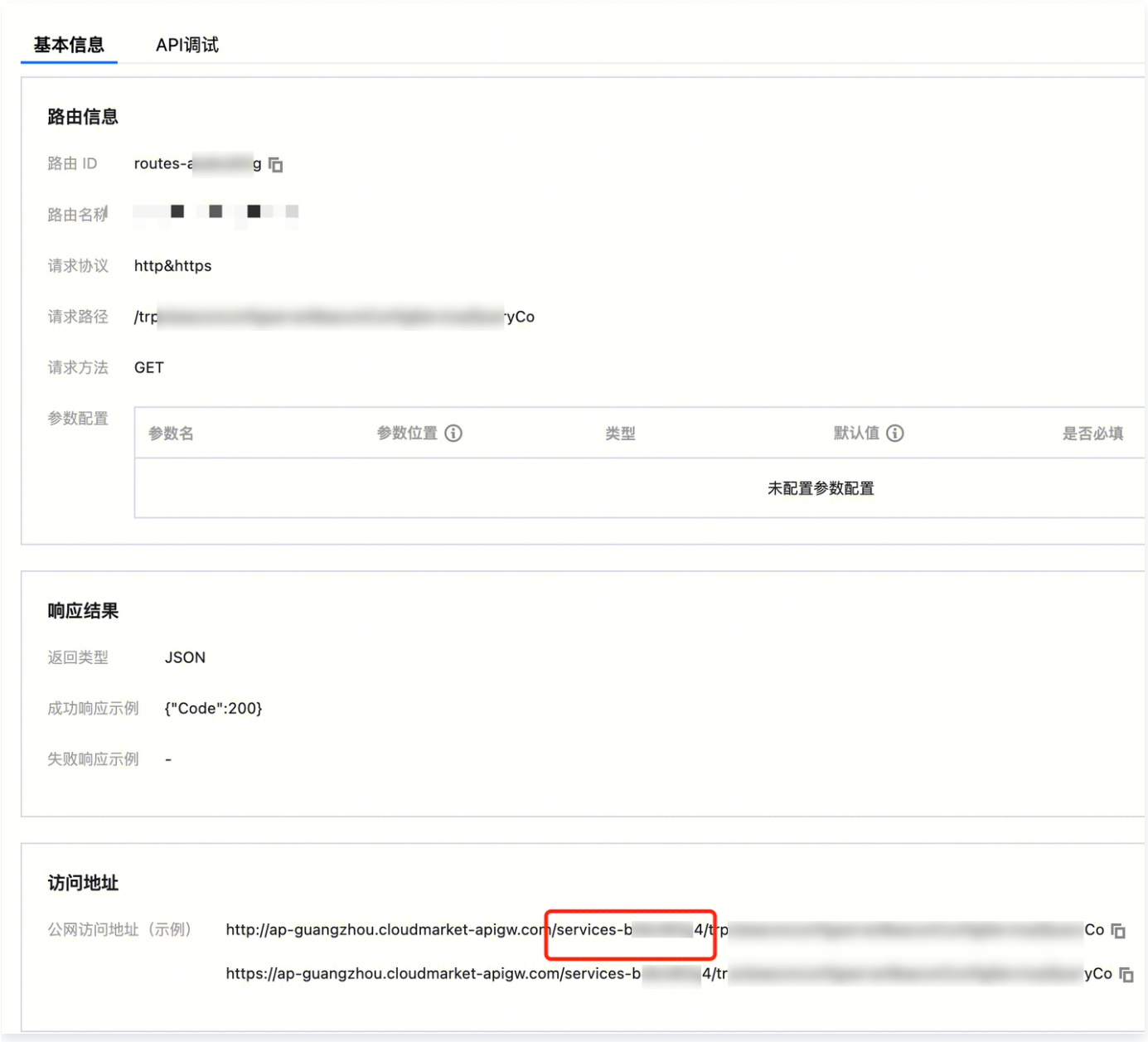
响应结果



字段配置	说明
返回结构（用于生成接口文档供用户使用）	支持 JSON/HTML/TEXT/BINARY/XML 形式。
成功/成功响应示例（用于生成接口文档供用户使用）	如果为 JSON 结构，自动检测结构类型。
错误码配置（用于生成接口文档供用户使用）	服务商配置一些返回码和注释，生成文档后，供用户查看。

访问地址

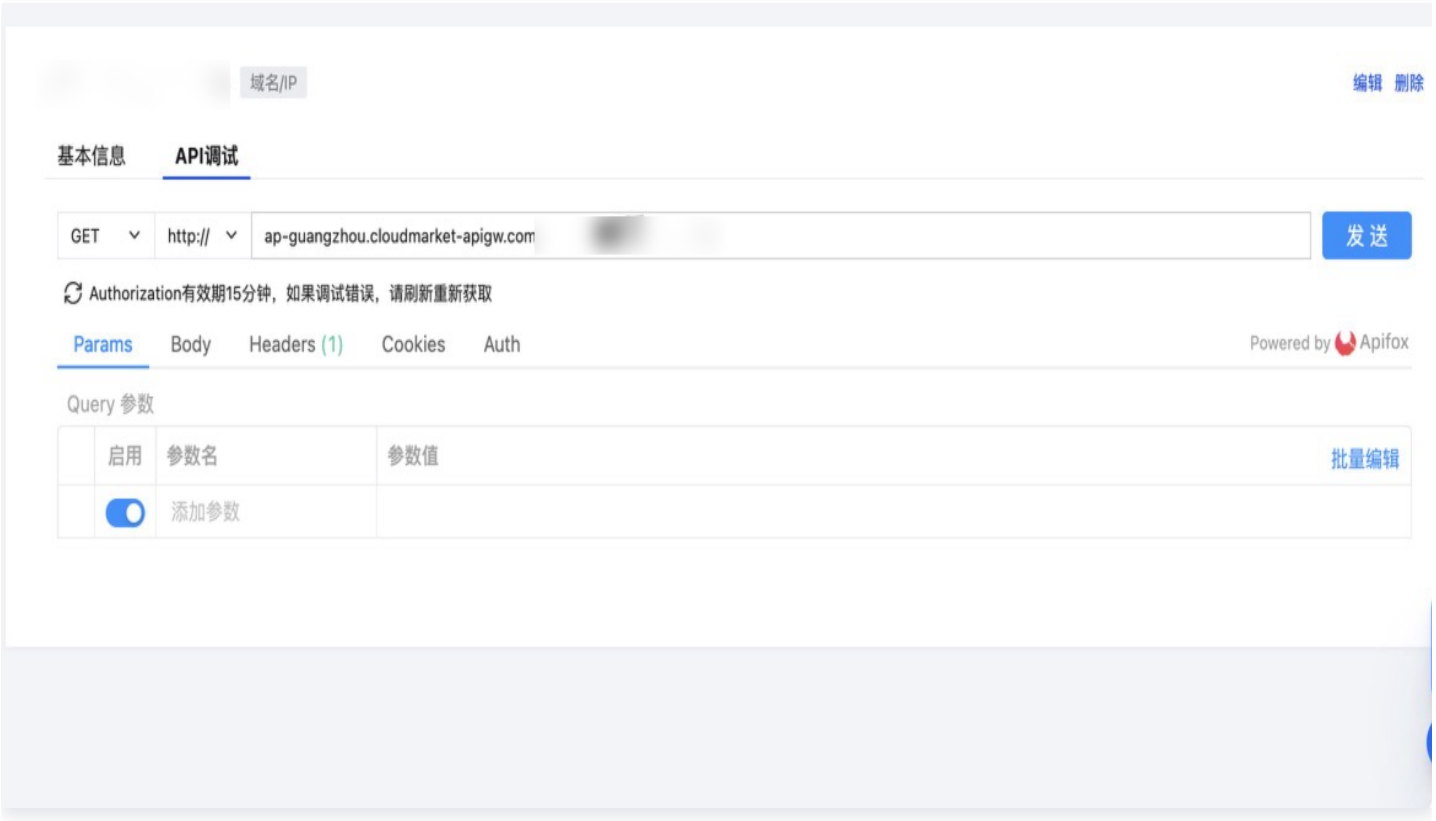
配置完成后 API 详情中可以查看访问地址。访问地址生成规则：http|https://{region}.cloudmarket-apigw.com/{service-id}/{RoutePath}。



API 网关调试

调试接口用来测试服务商服务是否成功接入到云市场 API 网关中，需进入到 API 详情页面进行调试。

> **注意：**
> 不要在调试页面更改地址栏中的地址，会导致调试失败。



请求及返回

针对不同的服务商的配置，API 网关会添加值到 Header 中。

服务端

Key	Value
X-TCloudMarket-Custom-AuthConfig	服务商在 API 鉴权参数中 配置的值。例如：{"test_json":1233,"test_parmar":"testvalue"}
X-TCloudMarket-Trace-Consumer	标记此请求来源的用户的 ID。例如：MQarpkSIP2mpNbMZwIV5ng==
Request-Id	当用户发起请求时，可以在请求的头部（header）中添加一个名为 "request-id" 的字段来标记该请求。如果用户没有提供该字段，网关会自动生成一个 "request-id" 字段，用于记录和跟踪该请求。
X-TCloudMarket-Request-Info	这次请求返回的是使用计划 ID、使用量和配额。例如：{"used":16994,"total":88888,"useplanid":"planId-0"}。**需要注意的是，使用量仅供参考。如果请求通过了网关鉴权，但服务端返回的状态码≥300，该请求将不会计入使用量中，使用量的（used）异步减少。**

Authorization	用户请求的鉴权参数，包含请求的 sid，请求时间：{"id": "AKIDXXX", "x-date": "Date:Mon, 19 Mar 2018 12:08:40 GMT"}'

用户端

Key	Value
Request-Id	网关会将用户在请求头部填写的 "request-id" 字段返回给用户。如果用户没有填写该字段，网关会生成一个 "request-id" 并将其返回给用户端和服务端。
X-TCloudMarket-Request-Info	返回这次请求的使用计划 ID，使用量和总和量，用户可以根据返回值判断当前使用计划的剩余量，例如：{"used":16994,"total":88888,"useplanid":"planId-0"} **需要注意的是，使用量仅供参考。如果请求通过了网关鉴权，但服务端返回的状态码≥300，该请求将不会计入使用量中，使用量的（used）异步减少。**

网关错误返回

如果用户的请求在网关被拦截，http 返回 status≥300，返回错误的具体样式如下：

```
{
    "requestid" :  "1728995097970162775",
    "message" :  "签名校验信息不对"
}
```

常见的网关返回错误如下表：

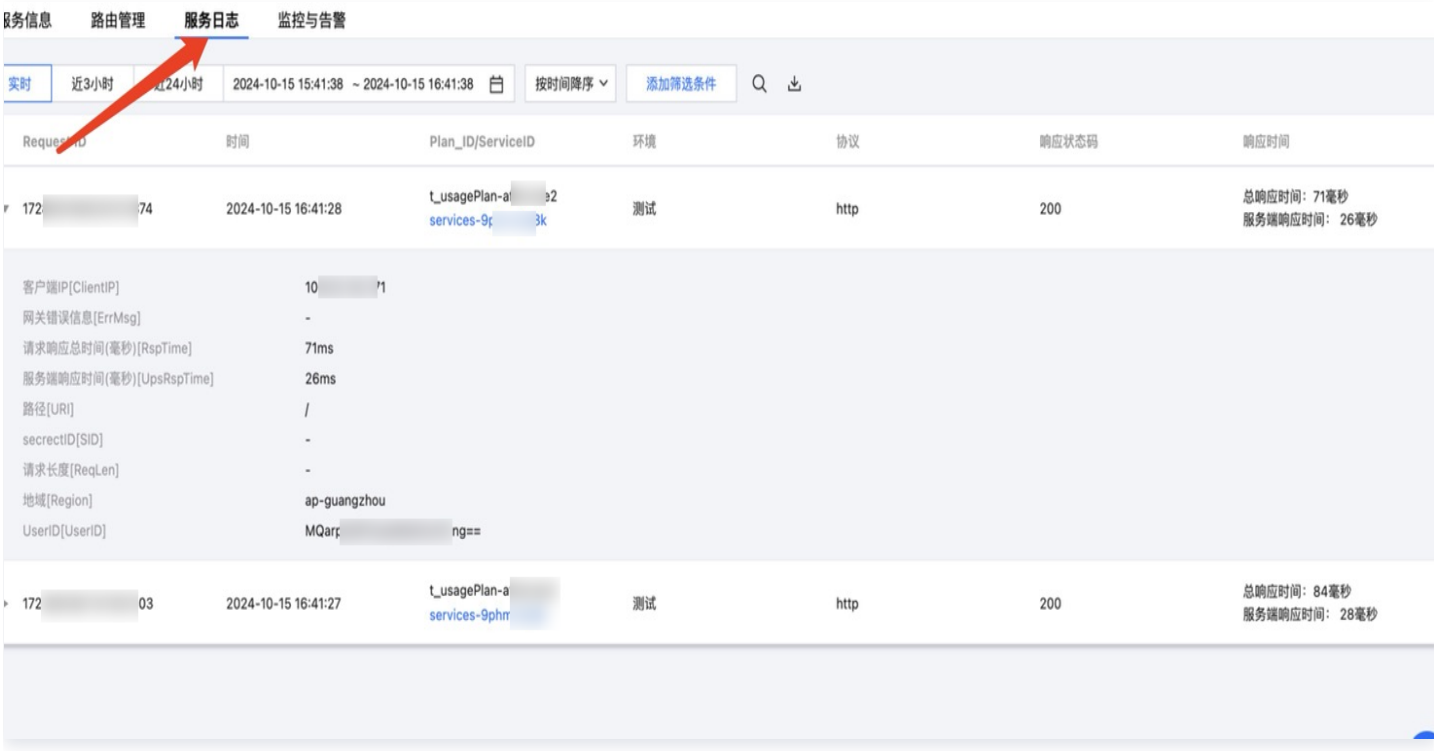
status	message
401	当前使用计划已经耗尽。
402	签名信息未校验通过。
403	签名时间超时，请重新生成签名。
404	密钥已经失效。
405	服务商已经停用该使用计划。
411	鉴权信息未在 header 中找到。
412	签名或者密钥格式不正确。
413	签名日期格式不对。
414	传递鉴权信息格式不对。

415	域名禁止访问，DNS 配置 IP 有问题。
427	密钥和服务信息不匹配，请确认您的 secretID 和您购买的 API 是对应的。
420<code<430	这类错误为内部错误，检查您的 SecretID 是否为在云市场购买的 API 产品提供的 ID。
500	其他类型错误。
⩾500	检查后端服务的具体配置。

服务日志

日志查看

您可以单击对应网关操作栏中的"**服务日志**"，来查看当前服务的最近访问日志。



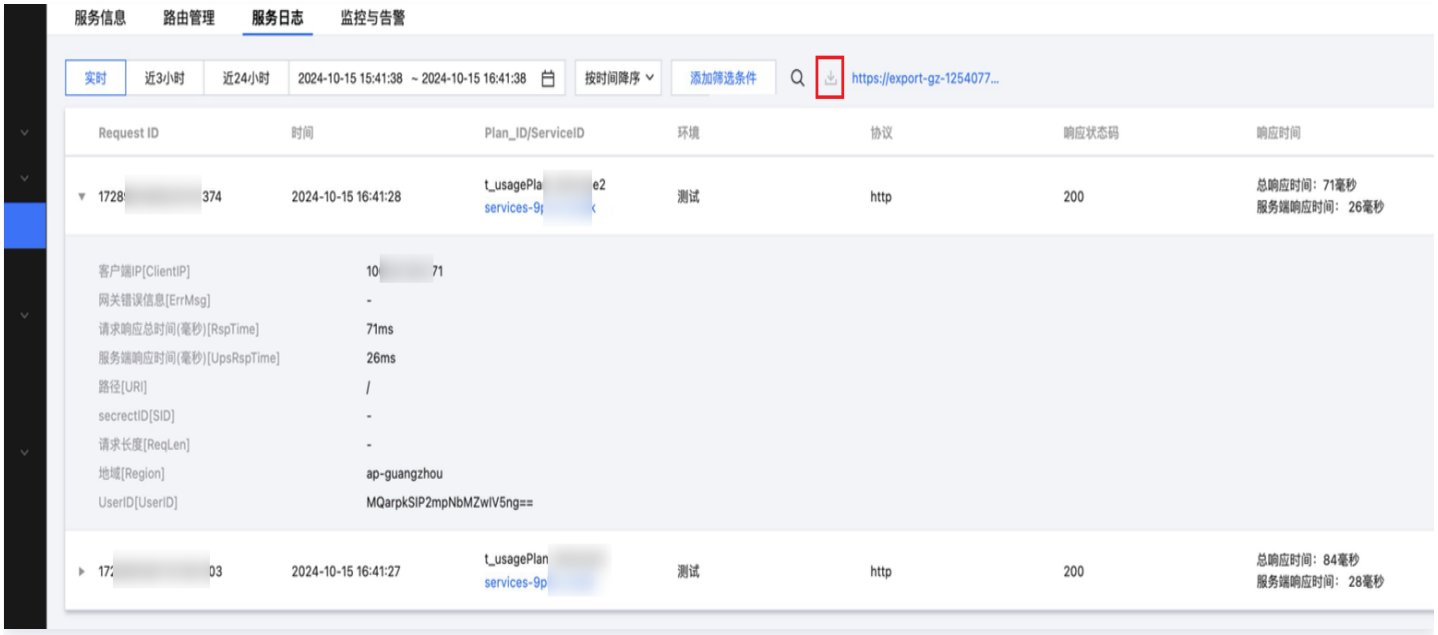
日志下载

您可以按照以下步骤下载当前查询条件下的服务日志：

1. 单击对应网关操作栏中的"**服务日志**"。
2. 在服务日志页面，找到并单击下载图标。
3. 将触发下载操作，您能够下载当前查询条件下的日志。

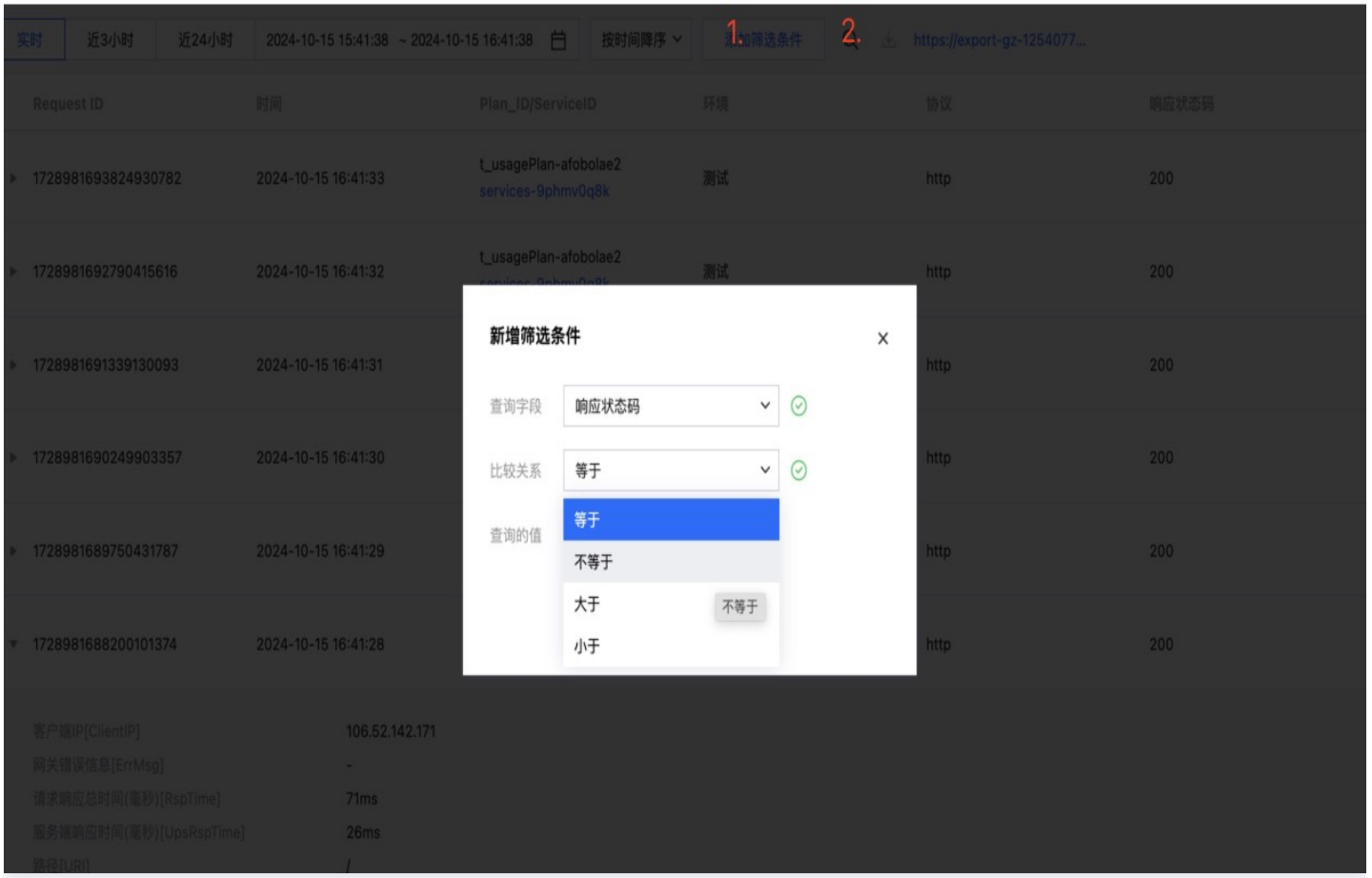
> ⚠ **注意：**

> 最多只能下载1万条日志。



日志查询

1. 单击**添加筛选条件**，选择所需的筛选条件，
2. 单击查询图标，查看查询结果。



监控与告警

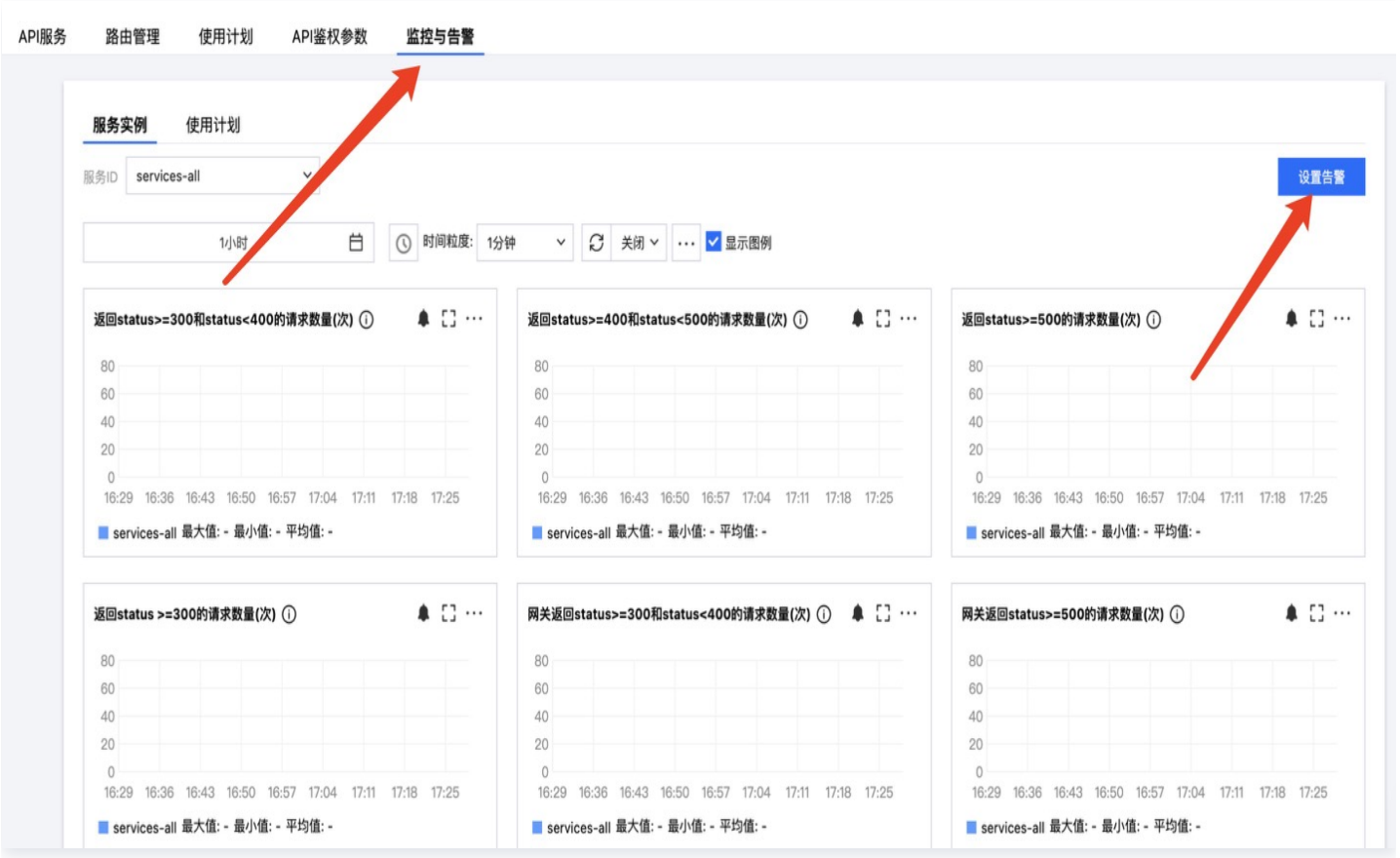
监控

当您单击对应网关操作栏的"**监控与告警**"时，您可以查看当前用户的所有服务实例的使用情况，包括服务实例和使用计划。

- 服务实例：您可以通过下拉框选择不同的服务实例，并查看该服务实例的请求数量。
- 使用计划：您可以查看已售出的所有订单对应的使用计划。

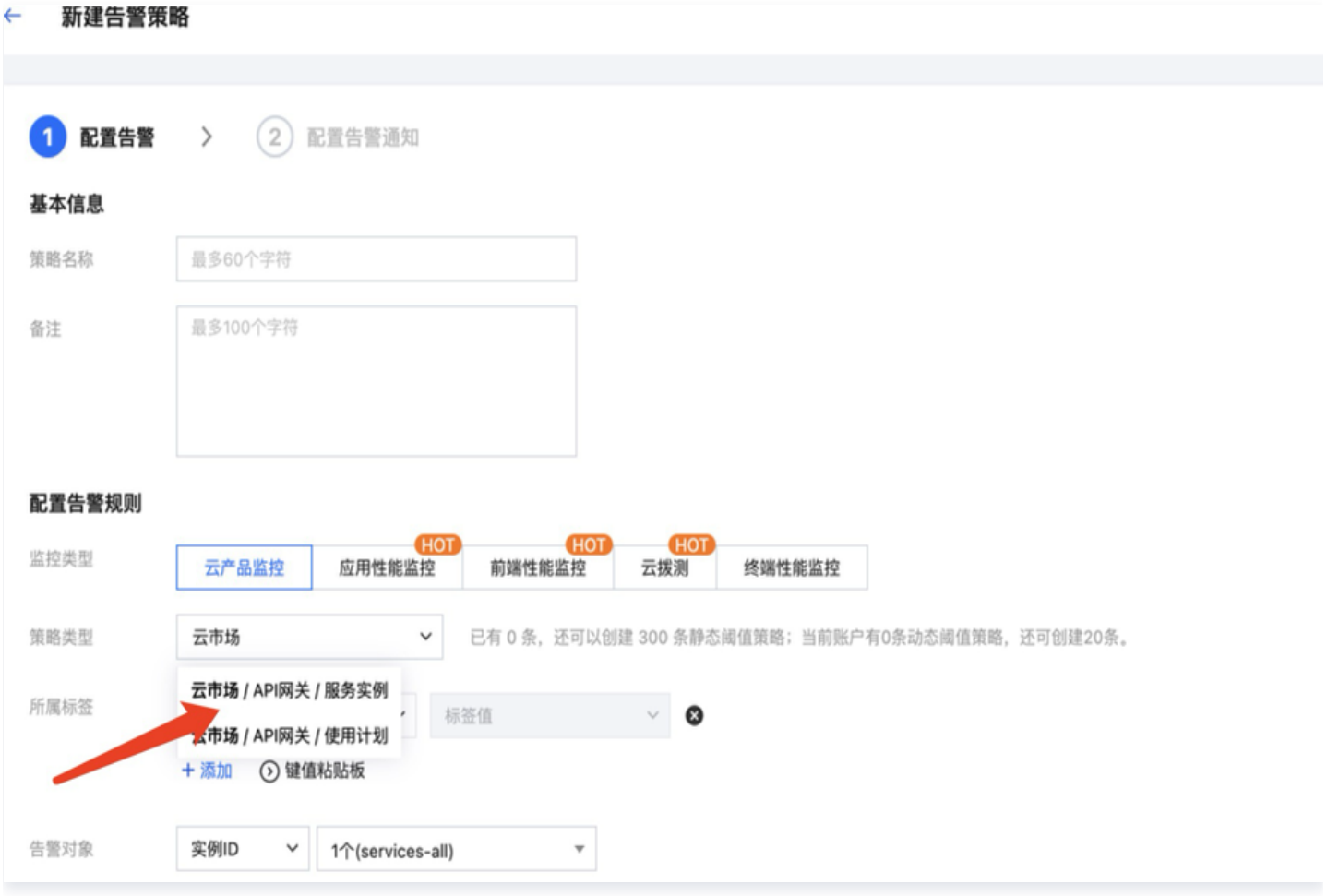
监控内容主要包含三个部分：

- 网关返回：这是指从用户发起请求后，在网关进行拦截后直接返回给用户的响应。
- 服务端返回：这是指经过网关转发到服务端后，最终返回给用户的响应。
- 所有请求：这包括用户发起的所有请求。例如，一个请求成功的响应必须经过网关和服务端。



告警

单击对应网关操作栏的“**监控与告警**”，单击**设置告警**，跳转到告警设置页面，根据策略类型，选择服务实例或者使用计划。详细说明可以参考 告警管理 。


新建告警策略
1 配置告警
2 配置告警通知
基本信息
策略名称
最多60个字符
备注
最多100个字符
配置告警规则
监控类型
云产品监控
应用性能监控
HOT
前端性能监控
HOT
云拨测
HOT
终端性能监控
策略类型
云市场
已有 0 条，还可以创建 300 条静态阈值策略；当前账户有0条动态阈值策略，还可创建20条。
所属标签
云市场 / API网关 / 服务实例
云市场 / API网关 / 使用计划
标签值
+ 添加
键值粘贴板
告警对象
实例ID
1个(services-all)

自动交付接入方案

最近更新时间：2024-10-10 14:33:21

简介

本文档描述了 SaaS 应用接入到云市场所需实现的接口定义，服务商通过提供以下接口，即可获得商品购买成功的信息，并将成功信息返回给云市场展示给用户。

术语信息

文中涉及相关术语解释如下：

- 发货 URL： 由服务商开发，用于接收云市场实例相关消息的地址。
- Token：由服务商提供，用于校验发货 URL 有效性（**Token 应用于云市场和服务商间鉴权时使用，需谨慎保存**）。
- openId：当服务商的应用接入腾讯云开放平台后，可获得的腾讯云用户的唯一标识。
- 周期类商品：按周期计费的商品，例如：按年、月、日计费。
- 计量类商品：按时间或数量计费的商品，例如：100元/50分钟、100元/50次、100元/2000MB。

准备工作

在一个 SaaS 商品正式通过审核上架前，服务商需要进行以下准备工作：

1. 云市场发货接口开发（必选）。
2. 控制台的参数配置（必选）。
3. 接入腾讯云 OAuth（可选）。

接口开发

接口要求

在进行接口开发前，请了解以下相关要求：

项目	说明
传输协议	仅支持 HTTPS 传输协议（443端口）
提交方式	均采用 POST 方法提交
数据格式	提交和响应均为 JSON 格式
字符编码	统一使用 UTF-8 字符编码
签名算法	SHA256
签名要求	云市场的通知会使用签名

请求超时时间	5s（为保证网络畅通，推荐接口层服务器使用腾讯云广州区域。）

服务商在控制台配置发货接口 URL 和 Token 后，云市场会以 URL PARAMS（GET 参数）的方式添加到接口 URL 上，携带的参数如下：

参数	类型	说明
signature	String	加密签名，signature 结合了服务商填写的 Token 参数和请求中的 timestamp 参数、eventId 等参数。
timestamp	Integer	UNIX 时间戳（单位秒）
eventId	Integer	随机数

接口调试规则

- 接口创建成功后需要进行对应的调试才可以发布接口，上架 SaaS 交付类商品。
- 在服务商管理控制台的 **在线接口调试** 页面编辑调试 URL 和调试Token，并进行对应的接口调试，发布接口前必须将“创建实例”、“续费实例”、“实例过期”、“实例销毁”等接口调试成功，“实例配置变更”，“计量查询”、“预警设置”、“计量提醒”可选择性进行调试。
- “创建实例”、“续费实例”、“实例过期”、“实例销毁”这四个接口是必须调试通过的，如果未调试通过会影响商品正常的销售。如果商品没有试用版，则可跳过“实例配置变更”接口调试。另如果没有发布计量类商品的需求，则可跳过“计量查询”、“预警设置”、“计量提醒”接口调试。
- 接口调试通过后需点击发布接口按钮进行接口发布，发布后调试 URL 和调试 Token 信息会更新并保存到发货 URL 和发货 Token。

签名规则

服务商通过对 signature 进行校验（校验方式如下）。加密/校验流程如下：

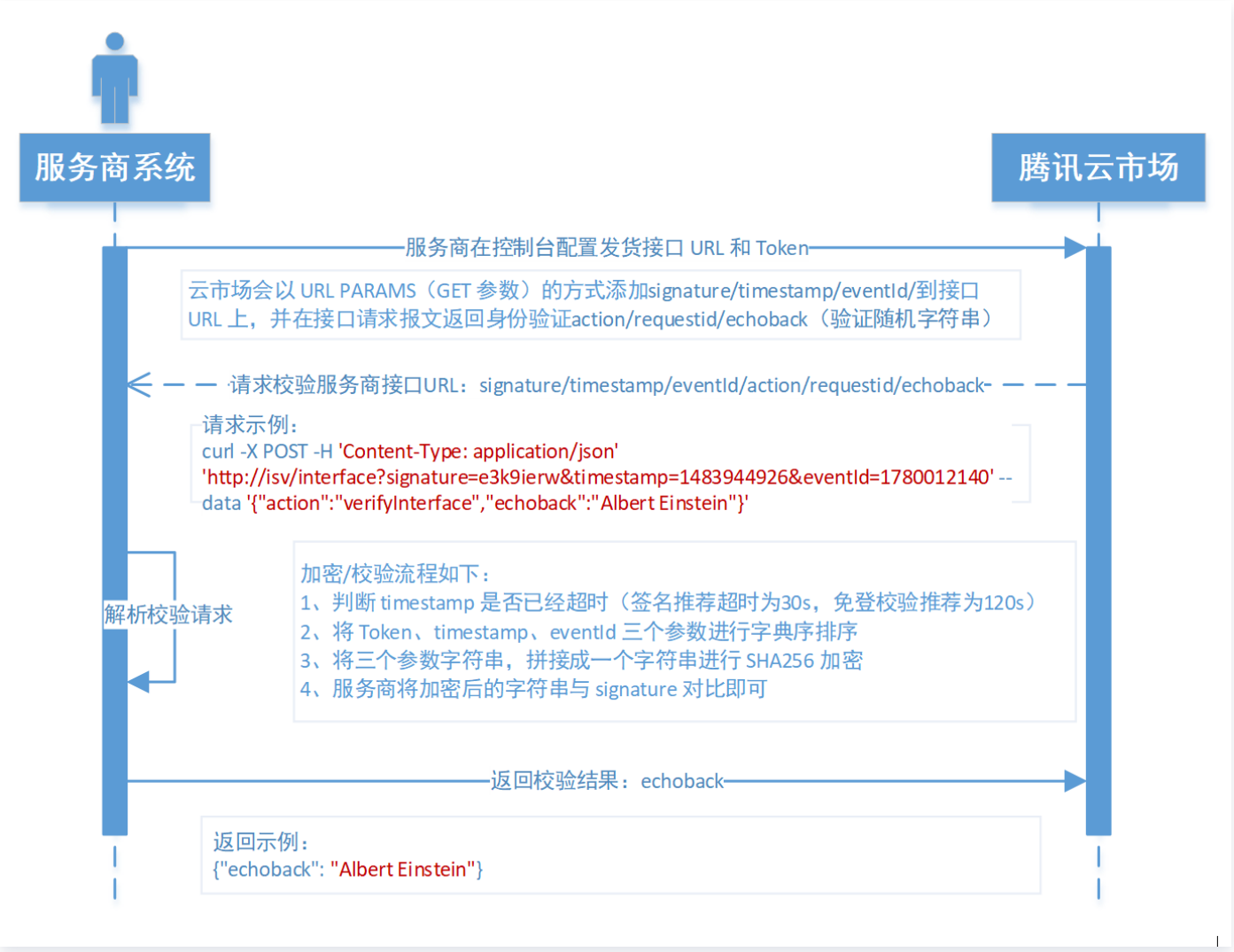
1. 判断 timestamp 是否已经超时（签名推荐超时为30s，免登校验推荐为120s）。
2. 将 Token、timestamp、eventId 三个参数进行字典序排序。
3. 将三个参数字符串，拼接成一个字符串进行 SHA256 加密。
4. 服务商将加密后的字符串与 signature 对比即可。

检验 signature 的 PHP 示例代码：

```
function checkSignature($signature, $token, $timestamp, $eventId)
{
    $currentTimestamp = time();
    if ($currentTimestamp - $timestamp > 30) {
      return false;
    }
    $timestamp = (string)$timestamp;
```

```
    $eventId = (string)$eventId;
    $params = array($token, $timestamp, $eventId);
    sort($params, SORT_STRING);
    $str = implode('', $params);
    $requestSignature = hash('sha256', $str);
    return $signature === $requestSignature;
}
```

接口验证过程



身份校验接口

- 接口名：verifyInterface。
- 接口说明：用户在 云市场服务商管理控制台 更改发货 URL 和 Token 时，后台会调用接口 URL 对 Token 进行实时校验，校验通过才可以设置成功。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	verifyInterface
requestId	String	是	接口请求标识，主要应用于问题排查。
echoback	String	是	随机字符串。

响应参数说明

参数名	类型	是否必须	描述
echoback	String	是	请求中的 `echoback` 参数的值。

请求示例

```
curl -X POST -H 'Content-Type: application/json' 'https://{isv/interface}?signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data '{"action":"verifyInterface","requestId":"6a02a01f-d420-43d9-be38-fd8eed6bb53a", "echoback":"Albert Einstein"}'
```

> **注意**
> 请求示例里的 `{isv/interface}` 需替换为服务商发货地址。

响应示例

```
{"echoback": "Albert Einstein"}
```

> **注意**
> 响应示例里的 echoback 应返回请求参数里的 echoback 值。

实例创建通知接口

- 接口名：createInstance。
- 接口说明：用户购买商品并支付后，云市场将通过实例创建通知接口发送信息至发货 URL。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	createInstance

orderId	String	是	订单 ID。
accountId	String	是	购买者的腾讯云账号 ID。
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位。如果没有接入开放平台，此字段为空。
productId	Integer	是	云市场产品 ID。
resourceId	String	是	云市场的实例 ID。
requestId	String	是	接口请求标识，主要应用于问题排查。
productInfo	JSON	是	产品信息。
productInfo.productName	String	是	购买的产品名称。
productInfo.isTrial	Bool	是	是否为试用，true：是；false：否。
productInfo.spec	String	是	产品规格，是试用时为空。
productInfo.timeSpan	Integer	是	购买时长，是试用时为空。
productInfo.timeUnit	String	是	购买时长单位（y、m、d、h、t 分别代表年、月、日、时、次），是试用时为空。 **注：这里所描述的年、月为自然年、自然月的概念。** 举例：02月01日买的包月商品，03月01日到期
productInfo.flowSpan	String	否	计量数量，仅当是计量类商品才存在。
productInfo.flowUnit	String	否	计量单位，仅当是计量类商品才存在。
productInfo.cycleNum	Integer	是	批量购买的规格数量，默认为1。
extendInfo	JSON	否	扩展字段，支持 comment 等字段。

extendInfo.comment	String	否	备注信息。

响应参数说明

参数名	类型	是否必须	描述
signId	String	是	实例标识 ID，服务商侧的实例唯一标识。不可为空，长度最长为11位。当为"0"时，系统会认为是异步发货。异步发货下，云市场会一直重试该接口，直至返回非0。
appInfo	JSON	否	应用信息。
appInfo.website	String	否	服务商的网站。
appInfo.authUrl	String	否	服务商提供给客户的免登地址。
additionalInfo	JSON	否	自定义数据，会显示在实例详情中。格式为 `[{"name":"","value":""}]`

请求示例

```
curl -X POST -H 'Content-Type: application/json' 'https://{isv/interface}?signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data '{"action":"createInstance","orderId":"20170109199524","accountId":"123545678","openId":"xz_D4XL_u7hKY5zt","requestId":"6a02a01f-d420-43d9-be38-fd8eed6bb53a","productId":1024,"resourceId":"market-78123as","productInfo":{"productName":"云服务市场测试商品","isTrial":false,"spec":"普通版","timeSpan":2,"timeUnit":"m"}}'
```

响应示例

```
{"signId": "36441d902ba", "appInfo": {"website":"http://www.example.com", "authUrl": "http://www.example.com/oauth/login"},"additionalInfo": [{"name":"注意","value":"这是一条注意"},{"name":"说明","value":"这是说明"}]}
```

注意：

- 服务商需保证该接口的幂等性。
- 针对新购接口调用失败的情况，云市场会每隔1s、5s、10s、30s、1m、2m、3m、4m、5m、6m、7m、8m、9m、10m、20m、30m、1h、2h调用一次后停止调用。若服务商接口问题在4小时45分调用

时间内解决，则在下一次调用接口响应成功，订单开通成功；若服务商接口问题在4小时45分调用后仍未解决，则判断实例创建失败，系统将自动取消该订单，并会为用户返还款项。

实例续费通知接口

- 接口名：renewInstance
- 接口说明：用户续费商品后，云市场将通过实例续费通知接口发送消息至发货 URL。该接口需要服务商立即返回响应。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	renewInstance
orderId	String	是	订单 ID。
accountId	String	是	购买者的腾讯云账号 ID。
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位；如果没有接入开放平台，此字段为空。
productId	Integer	是	云市场产品 ID。
resourceId	String	是	云市场的实例 ID。
requestId	String	是	接口请求的 ID。
signId	String	是	实例标识 ID。
instanceExpireTime	DateTime	是	新的实例到期时间（yyyy-MM-dd HH:mm:ss）。
productInfo	JSON	是	产品信息。
productInfo.productName	String	是	购买的产品名称。

productInfo.spec	String	是	产品规格。
productInfo.timeSpan	Integer	是	购买时长。
productInfo.timeUnit	String	是	购买时长单位（y、m、d、h、t 分别代表年、月、日、时、次）。 **注：这里所描述的年、月为自然年、自然月的概念。** 举例：02月01日买的包月商品，03月01日到期。
productInfo.flowSpan	String	否	计量数量，仅当是计量类商品才存在。
productInfo.flowUnit	String	否	计量单位，仅当是计量类商品才存在。
extendInfo	JSON	否	扩展字段，支持 comment 等字段。
extendInfo.comment	String	否	备注信息。

响应参数说明

参数名	类型	是否必须	描述
success	String	是	true/false

请求示例

```
curl -X POST -H 'Content-Type: application/json' 'https://{isv/interface}?signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data '{"action":"renewInstance","orderId":"20170109199524","accountId":"123545678","openId":"xz_D4XL_u7hKY5zt","requestId":"6a02a01f-d420-43d9-be38-fd8eed6bb53a","productId":1024,"resourceId":"market-asd12asd","signId":"kjsadkjhdskjh3k","instanceExpireTime":"2017-02-09 19:59:59","productInfo":{"productName":"云服务市场测试商品","spec":"普通版","timeSpan":2,"timeUnit":"m"}}'
```

响应示例

```
{"success":"true"}
```

注意

服务商需保证该接口的幂等性。

实例配置变更通知接口

- 接口名：modifyInstance。
- 接口说明：用户将实例从试用版转为正式版时，云市场将通过实例配置变更通知接口发送消息至发货 URL。

> **说明**
> 如果用户仅是配置变更，则参数中只会包含实例的新规格，而不会包含实例价格参数。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	modifyInstance
orderId	String	是	订单 ID。
accountId	String	是	购买者的腾讯云账号 ID。
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位。如果没有接入开放平台，此字段为空。
productId	Integer	是	云市场产品 ID。
requestId	String	是	接口请求的 ID。
resourceId	String	是	云市场的实例 ID。
signId	String	是	实例标识 ID。
spec	String	是	实例新规格。
timeSpan	Integer	是	购买时长，仅在试用版转为正式购买时传递。
timeUnit	String	是	购买时长单位（y、m、d、h、t 分别代表年、月、日、时、次），是试用时为空 。

			注：这里所描述的年、月为自然年、自然月的概念。 举例：02月01日买的包月商品，03月01日到期。
instanceExpireTime	Datetime	是	新的实例到期时间，仅在试用版转为正式购买时传递。
productInfo	JSON	是	产品信息。
productInfo.productName	String	是	购买的产品名称。
productInfo.spec	String	是	产品规格，与外层 spec 一致。
productInfo.timeSpan	Integer	是	购买时长，与外层 timeSpan 一致。
productInfo.timeUnit	String	是	购买时长单位（y、m、d、h、t 分别代表年、月、日、时、次），是试用时为空 。 **注：这里所描述的年、月为自然年、自然月的概念。** 举例：02月01日买的包月商品，03月01日到期。
extendInfo	JSON	否	扩展字段，支持 comment 等字段。
extendInfo.comment	String	否	备注信息。

响应参数说明

参数名	类型	是否必须	描述
success	String	是	true/false
appInfo	JSON	否	新的应用信息。
appInfo.authUrl	String	否	新的免登地址。

请求示例

```
curl -X POST -H 'Content-Type: application/json' 'http://isv/interface?signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data '{"action":"modifyInstance","orderId":"20170109199524","accountId":"123545678","openId":"xz_D4XL_u7hKY5zt","requestId":"6a02a01f-d420-43d9-be38-fd8eed6bb53a","productId":1024,"resourceId":"market-asd12asd","signId":"kjsadkjhdskjh3k","spec":"高级
```

```
版","timeSpan":2,"timeUnit":"m","instanceExpireTime":"2021-02-09
19:59:59","productInfo":{"productName":"云服务市场测试商品","spec":"普通
版","timeSpan":2,"timeUnit":"m"}}'
```

响应示例

```
{"success":"true"}
```

> **注意：**
> 服务商需保证该接口的幂等性。

实例过期通知接口

- 接口名：expireInstance。
- 接口说明：实例到期后（用户最后操作后的 instanceExpireTime），云市场将通过实例过期通知接口发送消息至发 货URL，服务商收到该通知后需对资源进行隔离。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	expireInstance
accountId	String	是	购买者的腾讯云账号 ID。
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位。如果没有接入开放平台，此字段为空。
productId	Integer	是	云市场产品 ID。
requestId	String	是	接口请求标识。
resourceId	String	是	云市场的实例 ID。
signId	String	是	实例标识 ID，服务商提供的实例唯一标识。长度最长为11位。

orderId	String	是	订单 ID。

响应参数规范

参数名	类型	是否必须	描述
success	String	是	true/false

请求示例

```
curl -X POST 'https://{isv/interface}?
signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data
'{"action":"expireInstance","accountId":"123545678","openId":"xz_D4XL_u7hKY5
zt","requestId":"6a02a01f-d420-43d9-be38-
fd8eed6bb53a","productId":1024,"resourceId":"market-
asd12","signId":"kjsadkjhdskjh3k", "orderId":"20170109199524"}'
```

响应示例

```
{"success":"true"}
```

注意：

- 服务商需保证该接口的幂等性。
- 服务商务必需要实现该接口，以便在实例过期时及时收到云市场通知，并对资源进行隔离。

实例销毁通知接口

- 接口名：destroyInstance。
- 接口说明：当**用户退款**或**实例到期后的七天内用户没有进行续费操作**时，云市场会通过实例销毁接口发送消息至发货URL，服务商收到通知后应及时对资源进行回收。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	destroyInstance
orderId	String	是	订单 ID。
account	Strin	是	购买者的腾讯云账号 ID。

Id	g		
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位。如果没有接入开放平台，此字段为空。
productId	Integer	是	云市场产品 ID。
requestId	String	是	接口请求标识。
resourceId	String	是	云市场的实例 ID。
signId	String	是	实例标识 ID，服务商提供的唯一标识。长度最长为11位。
destroyType	String	是	销毁类型。 • refund：退款触发的销毁。 • lifeCycle：生命周期触发的销毁。

响应参数说明

参数名	类型	是否必须	描述
success	String	是	true/false

请求示例

```
curl -X POST 'https://{isv/interface}?
signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data
'{"action":"destroyInstance","orderId":"20170109199524","accountId":"1235456
78","openId":"xz_D4XL_u7hKY5zt","requestId":"6a02a01f-d420-43d9-be38-
fd8eed6bb53a","productId":1024,"resourceId":"market-
asd12asd","signId":"kjsadkjhdskjh3k"}'
```

响应示例

```
{"success":"true"}
```

注意：

- 服务商需保证该接口的幂等性。
- 服务商务必需要实现该接口，以便在**用户退款**或**实例过期7天后**及时收到云市场通知，并对资源进行回收。

- 针对接口调用失败的情况，云市场会持续调用并告警7天后停止调用。如因接口响应失败，导致用户过期后仍能正常使用所造成的资源损失，由服务商自行承担。

计量商品计量信息查询接口

说明：
该接口仅会应用于计量类 SaaS 商品。周期类商品不需实现该接口。

- 接口名：flowQuery。
- 接口说明：当用户查询已购买实例的计量信息时，云市场会通过该接口发送消息至服务商发货 URL 查询。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	flowQuery
accountId	String	是	购买者的腾讯云账号 ID。
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位。如果没有接入开放平台，此字段为空。
requestId	String	是	接口请求标识。
resourceId	String	是	云市场的实例 ID。
signId	String	是	实例标识 ID，服务商提供的唯一标识。长度最长为11位。
productId	Integer	是	云市场产品 ID。

响应参数说明

参数名	类型	是否必须	描述
success	String	是	true/false
totalFlow	String	是	总流量。

costFlow	String	是	已消耗流量，没有消耗时返回"0"。
flowUnit	String	是	流量单位，取值范围m/h/Mb/Gb，分别代表分钟/小时/Mb/Gb。

请求示例

```
curl -X POST 'http://isv/interface?signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data '{"action":"flowQuery","accountId":"123545678","openId":"xz_D4XL_u7hKY5zt","requestId":"6a02a01f-d420-43d9-be38-fd8eed6bb53a","productId":1024,"resourceId":"market-4odto1yji","signId":"kjsadkjhdskjh3k"}'
```

响应示例

```
{"success":true,"totalFlow":"2000","costFlow":"600","flowUnit":"Mb"}
```

计量商品通知阈值设置接口

> **说明：**
> 该接口仅会应用于计量类 SaaS 商品。周期类商品不需实现该接口。

- 接口名：flowSetting
- 接口说明：计量类的商品用户在购买之后，可以通过此接口设置计量提醒阈值。云市场会通过该接口发送消息至发货URL。接收到该通知后，服务商需记录该阈值，并且在阈值到达时回调云市场接口 计量商品流量告警通知接口 FlowProductRemind 。

请求参数说明

参数名	类型	是否必须	描述
action	String	是	flowSetting
accountId	String	是	购买者的腾讯云账号 ID。
openId	String	是	用户在腾讯云开放平台的标识，此标识对于同一服务商是相同的，对于不同服务商是不同的，长度为32位。如果没有接入开放平台，此字段为空。
requestId	String	是	接口请求的 ID。

resourceId	String	是	云市场的实例 ID。
signId	String	是	实例标识 ID，服务商提供的唯一标识。长度最长为11位。
warnSpan	String	是	告警阈值。
warnUnit	String	是	告警阈值单位。
switch	String	是	告警开关，表示是否开启告警。 • ON 表示开启。 • OFF 表示关闭。

响应参数说明

参数名	类型	是否必须	描述
success	String	是	true/false
info	String	否	错误信息。

请求示例

```
curl -X POST 'https://{isv/interface}?
signature=e3k9ierw&timestamp=1483944926&eventId=1780012140' --data
'{"action":"flowSetting","accountId":"123545678","openId
":"xz_D4XL_u7hKY5zt","requestId":"6a02a01f-d420-43d9-be38-
fd8eed6bb53a","resourceId":"market-
4odto1yji","signId":"kjsadkjhdskjh3k","warnSpan":"1200","warnUnit":"Mb","swi
tch":"ON"}'
```

响应示例

```
{"success":"true"}
```

参数配置

在完成了相关开发后，服务商可登录 云市场服务商管理控制台，在**开发配置 > SaaS 接入设置**页面中，填写相关信息：

> **注意：**
> 为保证数据的安全，发货 URL 必须为 HTTPS 协议，且发货 URL 不能包含查询字符串。如果配置保存失败，请检查 verifyInterface 接口是否正常。

在线接口调试

在接口开发过程中，您可以登录 云市场服务商管理控制台，在**开发配置 > 在线接口调试**中，可使用在线调试功能，用于模拟各种类型的发货行为。

> **注意：**
> 此为调试环境，请勿使用正式环境的接口 URL 或数据库对接。

接入腾讯云 OAuth

为了提升用户使用 SaaS 产品的体验，建议服务商将应用接入腾讯云开放平台 OAuth ，实现用户在腾讯云控制台登录后，直接免登访问 SaaS 应用管理后台。

申请接入开放平台

由于腾讯云暂未开放申请腾讯云开放平台的入口，因此申请者需要先发邮件至：mqcloud@tencent.com 协助开通。邮件内容如下：

- 腾讯云账户的 ID：您的账号 ID 可在 腾讯云控制台 总览页面右上角处查看。
- 平台名称：平台名称会展示在授权页面。
- 平台 Logo：建议尺寸：260 x 48，PNG 格式，Logo 将会展示在授权页面中。
- 平台官网地址：您可以跳转到的第三方平台官网，即服务商的 SaaS 地址。

- 平台回调地址：去掉 HTTP[s] 的域名部分，不能只是顶级域名，例如可以为 `api.example.com`，而不允许为 `example.com`。

申请成功后您将会得到如下的信息：

- AppId：第三方平台唯一标识。
- AppSecretId/AppSecretKey：用来请求腾讯云 API 时的密钥对。
- EncryKey：用来校验回调地址中带入的 code 参数。

OAuth 接入说明

账号打通

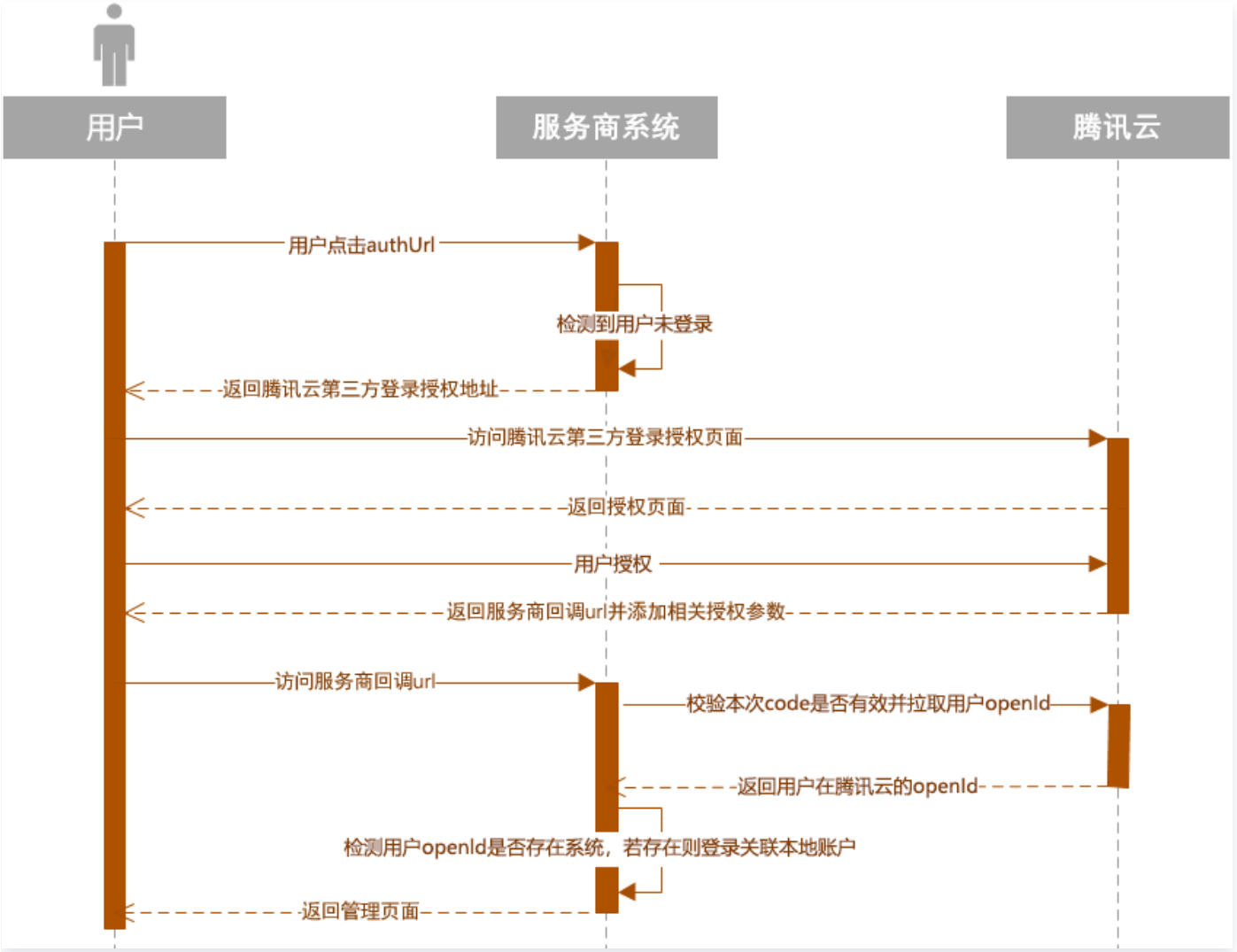
云市场在发货通知中加入用户在腾讯云的标识 OpenID （对于不同服务商用户 OpenID 不同），服务商在获取到 OpenID 之后需要首先要查询该用户是否已与本地系统某个账户绑定，如果已经绑定，则直接处理发货逻辑；若未绑定，则应该在本地系统生成一个账号并与 OpenID 绑定。

免登校验

服务商对于发货的响应数据中应该返回一个 `authUrl`，该 URL 最终会展示给用户。用户单击该 URL 后，服务商应该让用户登录到控制台以进行资源相关操作。

授权流程说明

服务商授权过程如下：



1. 用户单击 `authUrl`（假设为：`http://example.com/qcloud/auth`）后，若未检测到用户登录，则跳转（302跳转）到：
```
https://cloud.tencent.com/open/authorize?scope=login&app_id=123456789012&redirect_url=https%3A%2F%2Fexample.com%2Fapi%2Foauth%2Fqcloud%2Fcallback&state=1234
```
，其中 `app_id` 为申请 OAuth 后获得的**第三方平台唯一标识**，`redirect_url` 为提交腾讯云开放平台的**平台回调地址域名**。
2. 用户在腾讯云开放平台页面进行登录并且授权。
3. 页面跳转回第三方网站地址 `redirect_url`，并且带上参数 code 和 signature，类似：
```
https://example.com/api/oauth/qcloud/callback?code=04f82b0d6fcfc0c2d967d808e6010bd8&signature=eafc9653bd5c17c6adea55bb516ba8b9&state=123
```
， 其中 signature = md5(code+EncryKey)。

> **说明：**
> - 为了防止暴力破解，signature 参数对 code 的合法性做了一个校验。
> - 该 code 一次性有效，并且有效期为6分钟。

4. 获取 code 并且校验合法之后，调用 code 校验接口，获取用户的以下信息：
   - userOpenId：用户在该第三方平台下的身份唯一标识。`userOpenId` 即为用户在腾讯云的 `OpenID`（不同第三方平台获取的标识不同）。
   - userUnionId：如果同一个腾讯云账户有多个第三方平台，用户在这些第三方平台的 userUnionId 一致。
   - userAccessToken：用户访问 Token。
   - expiresAt：用户访问 Token 过期时间（时间戳，当前时间 + 2小时）。
   - userRefreshToken：刷新 Token，有效期为60天。

code 校验接口

1. 接口描述

- 接口请求域名：open.tencentcloudapi.com
- 接口说明：用于获取用户第三方开放平台的 access token

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见 公共请求参数。该接口使用分配给第三方平台的密钥调用。

参数名称	必选	类型	描述
Action	是	String	公共参数，本接口取值：GetUserAccessToken。
Version	是	String	公共参数，本接口取值：2018-12-25。

Region	否	String	公共参数，本接口不需要传递此参数。
UserAuthCode	是	String	auth code

3. 输出参数

参数名称	类型	描述
AppId	String	App ID
UserOpenId	String	第三方 openId。
UserUnionId	String	第三方 unionId。
UserAccessToken	String	第三方 access token。
ExpiresAt	Integer	过期时间。
UserRefreshToken	String	refresh token
Scope	String	授权范围。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 示例

- 输入示例：

```
https://open.tencentcloudapi.com/?Action=GetUserAccessToken
&UserAuthCode=testCode
&<公共请求参数>
```

- 输出示例：

```
{
  "Response": {
      "AppId": "10******99",
      "UserOpenId": "391f920b807ecbaa38f7e77ef5260cd4",
      "UserUnionId": "438344612f5e181dbb76d2fcf2634a7b",
```

```
        "UserAccessToken": "a649830709416d07be8f0dba1c7675ce",
        "ExpiresAt": 1581670707,
        "UserRefreshToken": "607202ece53c20a8ad91fa3512fa8ac7",
        "Scope": "login",
        "RequestId": "5bc7a27e-ba54-4b68-b37e-aaee60a2c5e2"
    }
}
```

商品审核标准

最近更新时间：2024-04-17 16:52:21

商品使用性审核标准

微信小程序商品

- 交付的商品可实现商品详情页，商品/使用文档声称的功能特性。
- 使用界面所呈现的信息和商品详情页以及商品使用文档内介绍的信息不得有冲突和不一致。
- SaaS 小程序商品体验顺畅，操作响应快，无明显卡顿。
- SaaS 小程序商品达到云市场 “自动化 + 免登” 的交付要求。
- SaaS 小程序商品功能完善，对用户友好，必须包含但不限于可视化编辑、数据分析的功能模块。
- 内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
- 禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
- 不得包含其他云厂商的广告 / 宣传内容。
- SaaS 小程序商品视觉和交互体验友好。

网站建设商品

- 交付的商品可实现商品详情页，商品/使用文档声称的功能特性。
- 使用界面所呈现的信息和商品详情页以及商品使用文档内介绍的信息不得有冲突和不一致。
- SaaS 建站商品需能提供超过50套优质建站模板供客户选择。
- SaaS 建站商品有保证商品运行稳定性的措施（提供相应证明文件）。
- SaaS 建站商品有保证网站安全性的措施（提供相应证明文件）。
- SaaS 建站商品需支持页面的可视化编辑，或拖拽编辑能力。
- SaaS 建站商品需达到云市场 “自动化 + 免登” 的交付要求。
- 内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
- 禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
- 不得包含其他云厂商的广告 / 宣传内容。
- SaaS 建站商品需支持在 PC 端、手机端、微信端等多端展示。
- 电商网站商品能提供完整的数据统计、订单管理、商品管理、顾客管理和推广营销等电商功能。

API 服务商品

- 交付的商品可实现商品详情页，商品/使用文档声称的功能特性。
- 使用界面所呈现的信息和商品详情页以及商品使用文档内介绍的信息不得有冲突和不一致。
- 接口测试易操作，返回数据准确。

- 接口响应快，无明显卡顿。
- 数据更新及时。
- 内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
- 禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
- 不得包含其他云厂商的广告 / 宣传内容。

镜像服务商品

- 交付的商品可实现商品详情页，商品 / 使用文档声称的功能特性。
- 使用界面所呈现的信息和商品详情页以及商品使用文档内介绍的信息不得有冲突和不一致。
- 在推荐的云服务器配置下（如无推荐则默认最低 CVM 配置）下，安装镜像后交付给用户的系统操作流畅，无明显延迟和报错。
- 软件操作界面无默认预设的用户名密码，或有预设但给予用户强提示进行修改调整并给出可执行方法。
- 镜像内不得包含漏洞，病毒，恶意软件。未经用户授权镜像不可安装外部插件 / 软件，向外部发送信息，泄露用户信息。
- 内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
- 禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
- 不得包含其他云厂商的广告 / 宣传内容。

运维服务商品

- 交付的服务可实现商品详情页，商品 / 使用文档声称的功能特性。
- 用户下单后2个工作日内响应用户需求。
- 使用界面所呈现的信息和商品详情页以及商品使用文档内介绍的信息不得有冲突和不一致。
- 内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
- 禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
- 不得包含其他云厂商的广告 / 宣传内容。

其余类目商品

- 交付的商品可实现商品详情页，商品 / 使用文档声称的功能特性。
- 使用界面所呈现的信息和商品详情页以及商品使用文档内介绍的信息不得有冲突和不一致。
- 内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
- 禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
- 不得包含其他云厂商的广告/宣传内容。

商品 logo 图片审核标准

- 图片基础要求如下：
  - 图片大小：尺寸为390 * 260px，分辨率为72dpi，图片大小不超过2M。
  - 图片内容：非纯白色背景图，图片主题需为公司名称或者产品名称，可以是案例界面或内容相关图标。
  - 图片格式：需为 PNG 格式图片。
  - 严禁出现国家法律法规所禁止的内容，包含但不限于：敏感类目、违禁产品、政治敏感、宗教敏感等相关内容。
- 各类目配图模板参考：
  - 微信小程序商品配图模板素材下载
  - 网站建设商品配图模板素材下载
  - 企业服务和运维服务商品配图模板素材下载
  - 镜像服务和 API 服务商品配图模板素材下载

商品文案审核标准

商品标题

- 商品名称应描述准确，与内容相符，商品名称长度不超过50个字符。
- 商品名称仅用于对商品命名，介绍、价格、版本、电话号码、免费等与命名无关内容，请勿出现在商品名称中。
- 商品名称不得出现营销广告类信息，包括但不限于：微信号、代理、满199-100、买一赠一、打折、热卖、疯抢、直降、清仓、推荐、爆款、首发、让利、特价等信息。
- 商品名称不得出现法律法规中明令禁止的内容和法律法规及腾讯云市场规则禁止的其他情形。
- 商品名称中的商品属性、品名、规格参数描述应语言精练，并突出商品特质，禁止使用和商品真实信息无关的文字或符号，且不得重复、互斥关键词或出现无关的关键词。

商品详情页

- 内容呈现：商品详情页内容信息结构完整，包含但不限于以下内容：功能特性、应用场景、使用指南、服务流程、售后支持等。
- 内容合规：
  - 商品详情页内容信息符合国家法规，无涉黄 / 暴 / 恐等不当信息，无广告法极限用语禁用词。
  - 商品详情页禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如其他云友商或服务商自己网页下单、咨询、采购的页面。
  - 商品详情页所呈现的信息和服务商的主体信息、承诺的服务时间，联络方式不得有冲突和不一致。
  - 商品详情页不得包含其他云厂商的广告/宣传内容。

商品/使用文档

> **注意**
> 镜像服务 / 运维服务商品必须包含商品 / 使用文档,且可下载使用，其余类目商品/使用文档非必要存在。

- 内容呈现：商品/使用文档内信息结构完整，包含但不限于以下内容：商品的使用指南、关键性的用户操作轨迹和界面截图等，具备让用户通过文档完整使用该商品功能的能力。

- 内容合规：
  - 文档内内容信息符合国家法规，无涉黄/暴/恐等不当信息，无广告法极限用语禁用词。
  - 文档内禁止有引导腾讯云用户离开云市场在外部界面进行购买的链接，如跳转到其他云友商或服务商自己网页下单、咨询、采购的页面。
  - 文档内所呈现的信息和商品详情页介绍的信息不得有冲突和不一致。
  - 文档内不得包含其他云厂商的广告/宣传内容。

商品规格

> **注意**
> 镜像商品不需填写商品规格。

- 商品规格命名需浅显易懂，且不得出现招代理、加盟合作等字眼。
- 若表示用户可终身使用该商品可将商品规格使用时长设置为10年，商品规格使用时长最长只能设置为10年。

服务与支持

> **注意**
> 至少需保障5 * 8小时的服务支持。

- 联络电话：商品详情页必须有服务商联络电话并可在服务商承诺的服务时间内接通。
- 客服：需要有能提供商业化服务能力的客服坐席进行 QQ 响应，且客服 QQ 需设置为无需添加好友即可沟通，并可在服务商承诺的服务时间内接通。

其他

- 商品名称字数不能超过50个字，且不得出现免费使用等引流字眼。
- 定制化商品需选择人工交付方式，且有标准化定制服务交付流程和文档。
- 不得服务商以需要客户授权获取用户信息。
- 商品服务协议中不得出现银行账号以误导用户线下汇款。
- SaaS 小程序商品需达到云市场“自动化”的交付要求。
- SaaS 建站商品需达到云市场“自动化”的交付要求。

违规预防

若商家 / 供应商发布信息不符合上述标准，一经发现，腾讯云市场有权删除相关内容。

镜像服务和 API 类商品配图规范

最近更新时间：2024-09-14 15:23:01

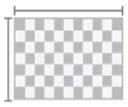
腾讯云云市场希望商品配图能够达到辅助用户理解商品内容的目的，为用户提供所见即所得的体验，以此更快速的抓住用户的注意力，提升商品的点击率和转化率。所以云市场对于配图清晰、有实质内容、有吸引力的商品会给予更多的曝光。为了让商品能够更高效的通过上架审核，您需要遵循云市场提供的配图规范，并且只有遵循配图规范的商品才有机会出现在首页等推荐位上。

以下是镜像服务和 API 类商品配图设计规范，您可以查看以下模板中的规范说明，并下载云市场提供的 镜像服务和 API 类商品配图规范 快速生成配图。

> **注意：**
> 以下配图模板仅限于服务商在腾讯云云市场页面内展示使用。模板内容仅作为参考样式提供，请按照商品实际内容填充，并且**模板的布局、颜色和字体均可根据商品实际内容进行变动设计**。视觉上需确保配图主体突出、清晰美观。

• 配图要求

图片大小



- 尺寸390*260px
- 分辨率72dpi
- 图片不能超过2M

图片内容

- 主题（公司名称或产品名称）
- 案例界面或内容相关图标
- 非纯白色背景图

图片格式

- PNG格式图片

严厉禁止

- 敏感类目
- 违禁产品
- 政治敏感
- 宗教敏感

• 配图模版参考

镜像服务类目

01

02

03

04

05

06

07

08

09

10

11

12

API类目

13

14

15

16

17

18

19

20

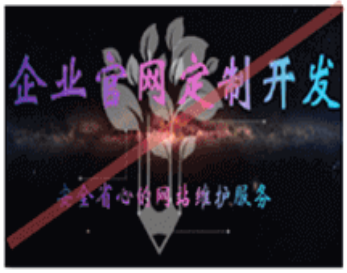
21

22

23

24

- 常见素材驳回原因



文案内容不明

背景颜色过多

排版零乱，干扰主题

素材图与产品内容不符

颜色怪异

不能使用图片描边

主题不清晰

文字过大

不能使用直接使用模版

尺寸不对，不能出现标签按钮等操作的元素

文字图片变形

不能使用纯白色背景

使用大面积红色产生紧张焦虑感

不同的产品，不能使用一样的配图。削弱用户对产品的辨识度

- 优秀案例


租车拼车
• 一直被模仿
• 从未被超越


上线了
企业
官网制作
响应式建站+多行业模板


企业展示官网
NiceBox
H5响应式建站


sitestar
建站营销版
PC\手机\微信网站...等
五站合一


FrontJS
快你一步捕捉 Bug


.NET
• asp
• asp.net
• mysql


程序漏洞修复
木马清除


云产品
日常代维护服务
站点、环境、数据库设
置排查