阿里云
爬虫风险管理

产品定价

文档版本：20190816

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
##	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 计费方式

爬虫风险管理（Anti-Bot Service，简称Anti-Bot）采用包年包月（预付费）的计费方式。

计费模式

计费项：按所选购的套餐版本计费。

付费方式：预付费。

计费周期：按月/年计费，购买时生成账单付费。

扣费周期：自购买当日起，根据所选择的购买时长（月/年）计算；购买时长支持选择一个月、三个月、半年、一年、两年、三年。

到期说明：当您购买的防护服务到期时，服务自动停止。

- 距离服务到期前7天，您会收到短信或邮件，提醒您服务即将到期并提示您及时续费。如在服务到期前没有续费，则在服务到期时您将失去防护效果。
- 服务到期后Anti-Bot实例中的相关配置将为您继续保留7天。如果在7天内完成续费，您可以直接使用原有配置继续进行防护；7天后仍未续费，系统将自动释放您在Anti-Bot实例中的配置，您必须重新购买实例并完成配置后方能恢复使用。

说明:

购买爬虫风险管理实例后，您可启用自动续费避免服务到期。更多详情，请参见设置自动续费。

产品定价

Anti-Bot实例的定价根据所选择的地域和模块配置计算。

是否必选	模块名称	功能概述	默认规格	产品定价			
				中国大陆		海外地区	
				元/年	元/月	元/年	元/月
必选	基础防护模块	提供通用爬虫攻击防护能力，覆盖Web网页、HTML5、App、API接口等全面业务： · 根据请求的具体特征定制自定义规则实现精准访问控制 · 基于IP、Cookie、请求头部参数字段，对特定URL实现请求限速控制 · 针对可疑请求提供基于JS脚本的人机识别、滑块验证、拦截等处置方式 · 针对重要业务接口进行数据风控，防御各类活动作弊风险 · 提供基础的爬虫风险管理报表和风险监控功能	· 支持HTTP、HTTPS、HTTP2.0、Websocket协议API接口，同时支持最多50个特定的非标端口 · 域名包：1个，支持添加10个域名，仅限一个一级域名和该一级域名的子域名或泛域名。 说明：如果需要添加更多网站域名，需购买域名扩展包（单价为1,500元/月）。 · 业务每秒请求数（QPS）：500次 说明：如果业务QPS超过默认规格，需要购买QPS扩展（每100 QPS单价为800元/月）。 · 业务带宽：阿里云上业务100 Mbps，非阿里云上业务10 Mbps 说明：如果业务带宽超出默认规格，需要购买带宽扩展（每10 Mbps单价为800元/月）。	54,000	4,500	81,000	6,750

是否必选	模块名称	功能概述	默认规格	产品定价			
				中国大陆		海外地区	
				元/年	元/月	元/年	元/月
可选	云端爬虫情报	提供丰富的爬虫情报资源，针对行业的集中式攻击，实时更新策略。爬虫情报来源包括： · 阿里巴巴集团业务沉淀的恶意IP库、恶意指纹库等 · 云端威胁情报，包括IDC机房信息、已知爬虫库、实时拨号池IP等 · 行业内爬虫攻击情报	-	54,000	4,500	81,000	6,750

是否必选	模块名称	功能概述	默认规格	产品定价			
				中国大陆		海外地区	
				元/年	元/月	元/年	元/月
可选	App场景	通过集成SDK实现针对App端的增强爬虫攻击防护，包括： · 提供阿里云自研App增强防护SDK和集成指导 · 实现App端与服务端的可信通信，确保只有来自合法且可信的设备的请求才会被转发至服务端 · 共享阿里巴巴集团十亿级别全球范围的恶意设备指纹库 · 有效识别模拟器、手机牧场、恶意篡改等数十种高风险身份或设备信息		72,000	6,000	10,8000	9,000

是否必选	模块名称	功能概述	默认规格	产品定价			
				中国大陆		海外地区	
				元/年	元/月	元/年	元/月
可选	智能算法	提供贴近业务风险的机器学习能力，通过定制化爬虫模型进行精准对抗。 基于对业务流程的深度学习，定制贴合业务风险的算法策略，结合其它通用爬虫防护模块，实现精细化的爬虫风险识别和管理，大幅提升防护效果。	默认包含1个算法实例且算法实例支持的最大QPS为500。您可根据业务需要扩展算法实例数和算法QPS。 · 算法实例数扩展单价： - 中国大陆地区：5,000 元/月 - 海外地区：7,500 元/月 · 算法QPS扩展单价（每100QPS）： - 中国大陆地区：1,000 元/月 - 海外地区：1,500 元/月	60,000	5,000	90,000	7,500

是否必选	模块名称	功能概述	默认规格	产品定价			
				中国大陆		海外地区	
				元/年	元/月	元/年	元/月
可选	安全专家服务	通过建立专属钉钉群，提供爬虫风险管理相关的在线咨询和技术支持服务： · 基础服务：爬虫风险管理相关咨询和技术支持，协助用户进行业务接入配置，包括域名接入、HTTPS配置、与其它云产品联动部署等。 · 增值服务：安全专家跟踪分析各种业务爬虫攻击行为，及时根据攻击手法的变化定制爬虫防护策略，减少业务层攻击对业务造成的损失。 说明：提供5*8小时服务，30分钟内及时响应。	-	360,000	30,000	540,000	45,000

推荐配置

一般情况下，可以根据您的业务类型选择以下通用基础配置：

- 网站业务防护场景：基础防护 + 爬虫情报
- App端业务防护场景：基础防护 + App场景
- 网站和App端业务防护场景：基础防护 + 爬虫情报 + App场景

说明:

如果您业务的爬虫风险管理安全需求较为复杂，可在此基础上选购定制算法模型或安全专家服务模块。

2 购买爬虫风险管理

您可以购买爬虫风险管理（Anti-Bot Service，简称Anti-Bot）为网站业务提供有效的恶意爬虫攻击防护。

操作步骤

1. 登录阿里云爬虫风险管理购买页面。
2. 选择地域。
3. 根据您的业务需求，选择需要的防护模块。

说明:

同时，根据所需接入的业务情况，设置域名扩展包、QPS扩展和带宽扩展。您选择购买定制智能算法模块后，还可以进一步选择算法实例数和算法QPS预估值。

说明:

在后续使用过程中，您也可以升级Anti-Bot实例加购功能模块或业务扩展。

4. 选择购买时长。
5. 单击立即购买，并完成支付后您就可以在爬虫风险管理控制台中进行业务接入配置。

说明:

Anti-Bot实例不支持五天无理由退款，亦不支持非全额退款操作。

3 域名扩展包

什么是域名包

爬虫风险管理（Anti-Bot Service，简称Anti-Bot）实例默认包含一个域名包。单个域名包支持添加10个域名接入Anti-Bot进行防护，包含一个一级域名和该一级域名的子域名或泛域名。

例如，默认情况下，您可以添加一个一级域名（`abc.com`）和最多九个该域名的子域名或泛域名（例如，`www.abc.com`，`\*.abc.com`，`mail.abc.com`，`user.pay.abc.com`，`x.y.z.abc.com`等）。所添加的这些域名（包括一级域名`abc.com`）都将占用同一域名包中的防护域名额度。

什么是域名扩展包

如果您想要添加两个不同的一级域名或它们的子域名接入Anti-Bot进行防护，您需要额外购买域名扩展包。假设您已经添加`abc.com`或其子域名进行防护，当您尝试添加`xyz.com`（另一个一级域名）或其子域名进行防护时，您将收到以下域名数量限制提示：

当前主域名个数有限制，请升级服务，单独购买扩展域名包。

这种情况下，您需要升级Anti-Bot实例以购买域名扩展包。

您可以在配置变更页面，选择所需的域名扩展包数量并完成支付，即可将更多的网站域名接入Anti-Bot实例实现恶意爬虫流量防护。

4 业务QPS和带宽扩展

爬虫风险管理（Anti-Bot Service，简称Anti-Bot）实例默认支持接入最大100 Mbps（阿里云上业务）或10 Mbps（非阿里云上业务）的业务带宽流量和500 QPS的每秒请求数量。您可以通过增加额外的带宽扩展或QPS扩展量以满足更大的业务带宽需求。

什么是业务QPS

业务QPS指在未遭受攻击的情况下，Anti-Bot实例中所有正常业务（包括所有接入该Anti-Bot实例防护的网站域名）的并发每秒请求次数，单位为QPS。

Anti-Bot实例默认支持处理最大500 QPS的并发每秒请求数。

什么是业务带宽

业务带宽指在未遭受攻击的情况下，Anti-Bot实例中所有正常业务（包括所有接入该Anti-Bot实例防护的网站域名）的流量峰值，单位为Mbps。

> 说明:
> Anti-Bot实例中的实际业务带宽由Anti-Bot单独计算，与其他阿里云产品（如CDN、SLB、ECS等）的带宽或者流量限制不存在任何关联。

Anti-Bot实例默认支持接入最大100 Mbps（阿里云上业务）或10 Mbps（非阿里云上业务）的业务带宽流量。在阿里云内的源站服务器（ECS、SLB实例等）享有更高的业务带宽。

什么是带宽扩展和QPS扩展

如果您通过Anti-Bot防护的业务流量较大或并发请求次数较多，您需要额外购买扩展带宽以避免正常业务流量超出Anti-Bot实例支持的最大业务带宽或最大并发QPS。

例如，您当前的业务流量带宽需求为30 Mbps（业务源站服务器未部署在阿里云上）、并发每秒请求数为1,500 QPS，而默认Anti-Bot实例对于非阿里云上业务最大仅支持10 Mbps的正常业务带宽和500 QPS的正常业务QPS。这种情况下，您需要额外购买20 Mbps的带宽扩展和1,000 QPS的QPS扩展，确保您的正常业务访问。

您可以通过升级Anti-Bot实例变更带宽扩展和QPS扩展配置，满足更大的业务需求。

> 说明:
> 您也可以在购买Anti-Bot实例时，根据实际业务需求，选择额外的带宽扩展和QPS扩展。

超出最大业务带宽或业务QPS有什么影响

如果您的正常业务流量或并发请求数超过所购买的Anti-Bot实例的最大处理能力（业务带宽或业务QPS），您将收到告警提示，且在Anti-Bot实例中已配置的业务流量和请求的转发将可能受到影响。

超出最大业务带宽或业务QPS后，将出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内出现不可用、卡顿、延迟等问题。

如果已经出现这种情况，您需要尽快购买额外业务带宽扩展或业务QPS扩展，避免对您业务造成的影响。

如何选择业务QPS扩展量

您可以根据所有已经或将要接入Anti-Bot的业务的日常并发QPS峰值，判断是否需要额外购买业务QPS扩展以及所需的业务QPS扩展量。您购买的Anti-Bot实例的最大业务QPS应大于所需接入的所有业务的日常并发QPS的峰值总和。

示例

假设您需要将三个网站业务接入Anti-Bot进行防护，未遭受攻击状态下每个业务的并发每秒请求次数峰值不超过500 QPS，总和不超过1,500 QPS。这种情况下，您只需确保购买的Anti-Bot实例的最大业务QPS大于1,500 QPS即可。

如何选择业务宽带扩展量

您可以根据所有已经或将要接入Anti-Bot的业务的日常入方向和出方向总流量的峰值，判断是否需要额外购买业务带宽扩展以及所需的业务带宽扩展量。您购买的Anti-Bot实例的最大业务带宽应大于入、出方向总流量峰值中较大的值。

说明:

一般情况下，网络出方向的流量会比较大。

您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您业务源站服务器上的其它流量监控工具来评估您的实际业务流量大小。

说明:

此处的流量指的是正常的业务流量。

例如，您需要将业务的外部访问流量均接入Anti-Bot进行防护。在业务正常访问（未遭受攻击）时，Anti-Bot将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，Anti-Bot过滤、拦截异常流量后，将正常流量回源到源站服务器。因此，您在云服务器（ECS）管理控制台中

查看您源站服务器的入方向及出方向的流量即是正常的业务流量。如果业务部署在多台源站服务器，则需要统计所有源站服务器的流量总和。

示例

假设您需要将三个网站业务接入Anti-Bot进行防护，未遭受攻击状态下每个业务出方向的业务流量峰值均不超过10 Mbps，业务流量总和不超过30 Mbps。这种情况下，您只需确保购买的Anti-Bot实例的最大业务带宽大于30 Mbps即可。

5 非标端口支持

除80/8080（HTTP）和443/8443（HTTPS）端口外，爬虫风险管理（Anti-Bot Service，简称Anti-Bot）还支持对特定非标端口进行防护。

Anti-Bot实例支持添加最多50个不同的业务端口（包含80/8080/443/8443标准端口）进行防护。

说明:

Anti-Bot仅防护支持的业务端口。对于不支持的端口，Anti-Bot无法正常转发流量，更无法提供防护。例如，当Anti-Bot实例收到来自4444业务端口的请求时，将直接丢弃该请求。

HTTP协议支持的端口

针对HTTP协议，Anti-Bot支持以下业务端口的防护：

80、81、82、83、84、88、89、800、808、1000、1090、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7070、7081、7082、7083、7088、7097、7777、7800、8000、8001、8002、8003、8008、8009、8020、8021、8022、8025、8026、8077、8078、8080、8081、8082、8083、8084、8085、8086、8087、8088、8089、8090、8091、8106、8181、8334、8336、8800、8686、8888、8889、8999、9000、9001、9002、9003、9080、9200、9999、10000、10001、10080、12601、86、9021、9023、9027、9037、9081、9082、9201、9205、9207、9208、9209、9210、9211、9212、9213、48800、87、97、7510、9180、9898、9908、9916、9918、9919、9928、9929、9939、28080、33702

HTTPS协议支持的端口

针对HTTPS协议，Anti-Bot支持以下业务端口的防护：

443、4443、5443、6443、7443、8443、9443、8553、8663、9553、9663、18980