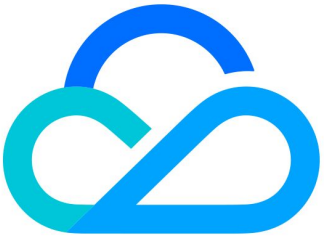
大模型安全网关

操作指南



腾讯云

【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

操作指南
新建实例

最近更新时间：2025-06-18 14:53:11

操作场景

本文档将指导您如何创建一个新的大模型安全网关实例。

操作步骤

1. 登录 大模型安全网关控制台 ，在左侧导航栏中，选择**实例管理**。
2. 在实例管理页面，单击**新购实例**，进入大模型安全网关购买页面选型。

参数	是否必选	说明
实例	必选	仅支持新购专享实例，默认选择专享实例。
实例名称	必填	请填写当前实例的名称。
地域	必选	建议选择与您的业务部署最近的地域，可降低访问时延、提高访问速度。
套餐版本	必选	提供多个套餐版本供您选择，套餐规格主要包含 QPS 及带宽约束，您可根据自己业务现状选择对应套餐。
网络	必选	部署需要选择私有网络及子网，如果现有网络不符合您的需求，可以选择 新建私有网络 。
自动续费	可选	账户余额足够时，到期后自动按月续费，建议开启。
协议条款	必选	购买前请您仔细阅读《 大模型安全网关服务协议 》。
时长	必选	您可以根据自身业务需求选择对应的服务市场。

3. 配置完成后会生成相对应的配置费用，单击立即购买，完成支付。

4. 支付完成后进入**控制台**，在左侧导航栏中，单击**套餐包**，可以查看购买实例状态。

实例升级

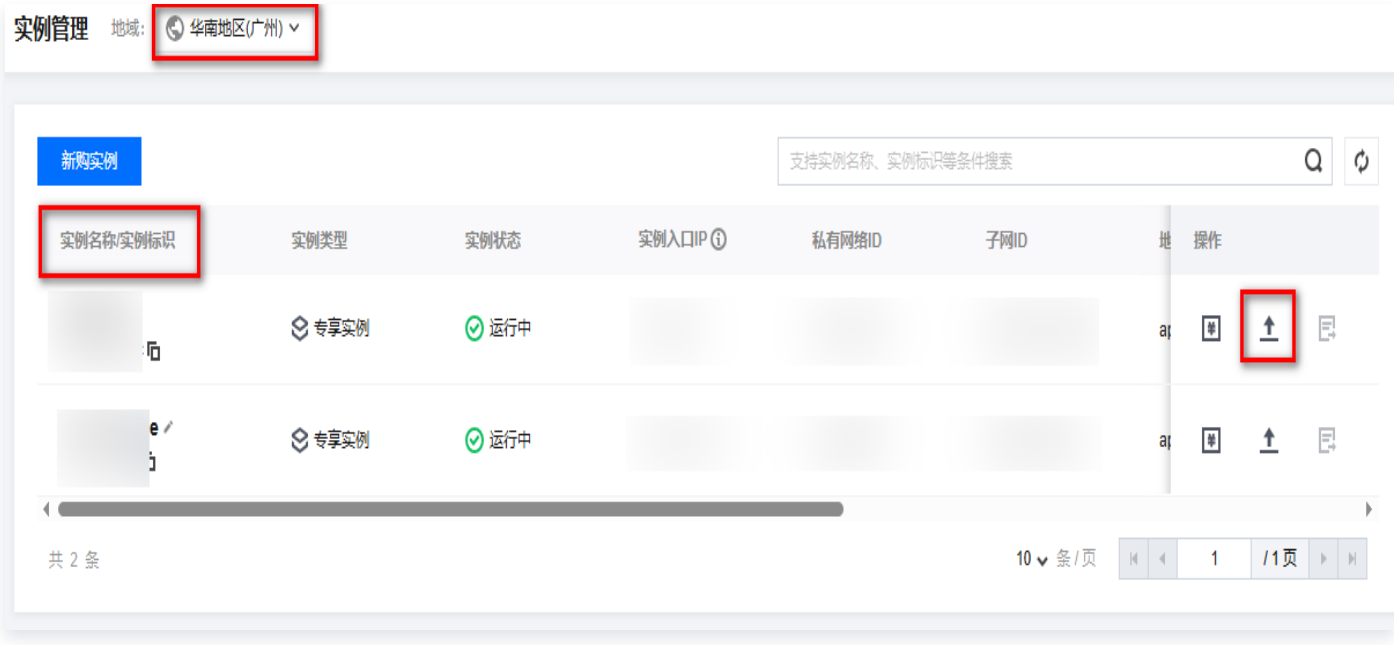
最近更新时间：2025-06-18 14:53:11

操作场景

本文档将指导您如何对大模型安全网关套餐实例进行升级。

操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择**实例管理**。
2. 确认要升级的**实例地域**，以及**实例名称**，单击右侧 ，将跳转至实例升级页面。



3. 在实例升级页面，您可以选择更高版本的套餐进行升级，不支持降级，选择完成支付即可。

> **注意：**
> 该页面不支持对实例类型、地域、网络、时长等参数进行修改。

实例续费

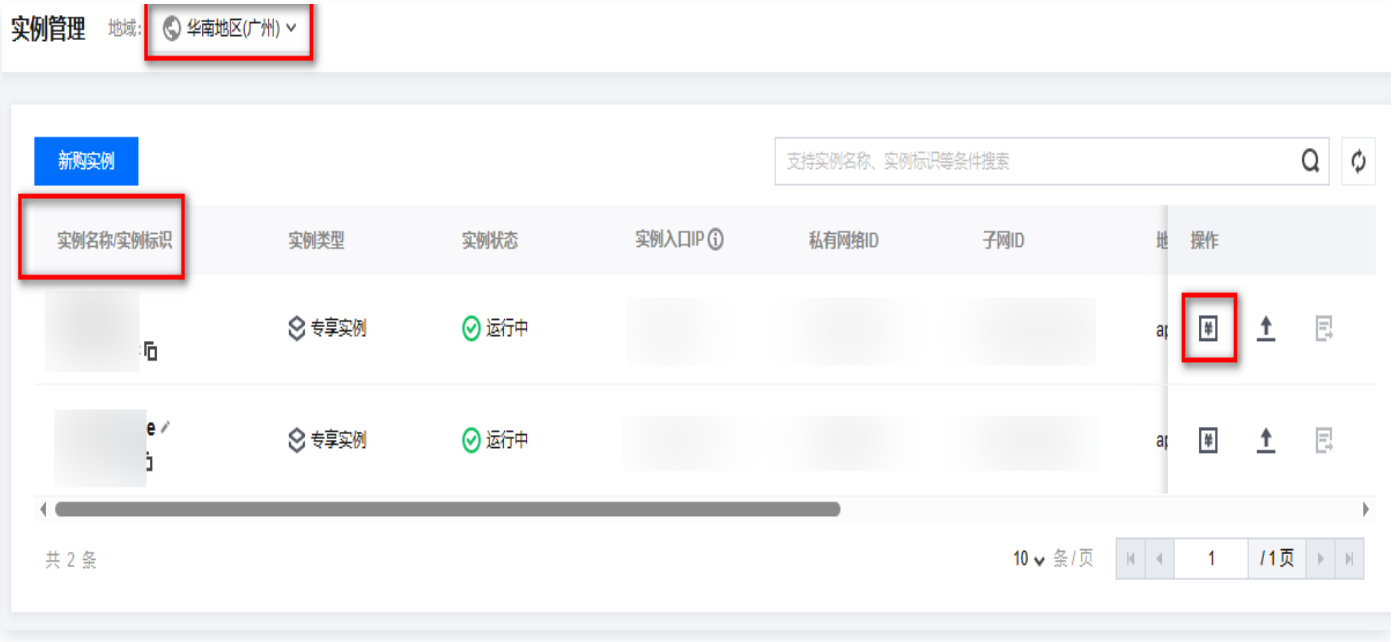
最近更新时间：2025-06-18 14:53:11

操作场景

本文档将指导您如何对大模型安全网关套餐实例进行续费。

操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择**实例管理**。
2. 确认要续费的**实例地域**，以及**实例名称**，单击右侧  ，将跳转至实例续费页面。



3. 在实例续费页面，您可以根据自身业务需求选择不同时长对当前套餐版本进行续费，选择完成后进行支付即可。

> **注意：**
> 该页面不支持对实例类型、地域、套餐版本、网络等参数进行修改。

安全日志

最近更新时间：2025-06-18 14:53:11

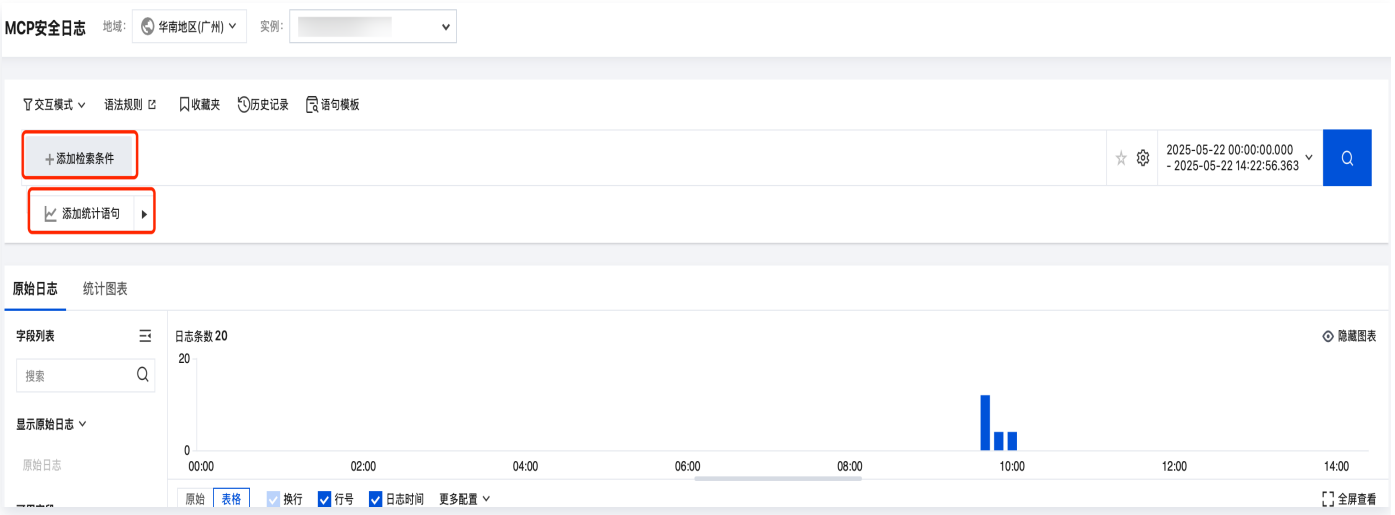
本文介绍如何利用安全日志进行索引、快速分析和查询。

背景信息

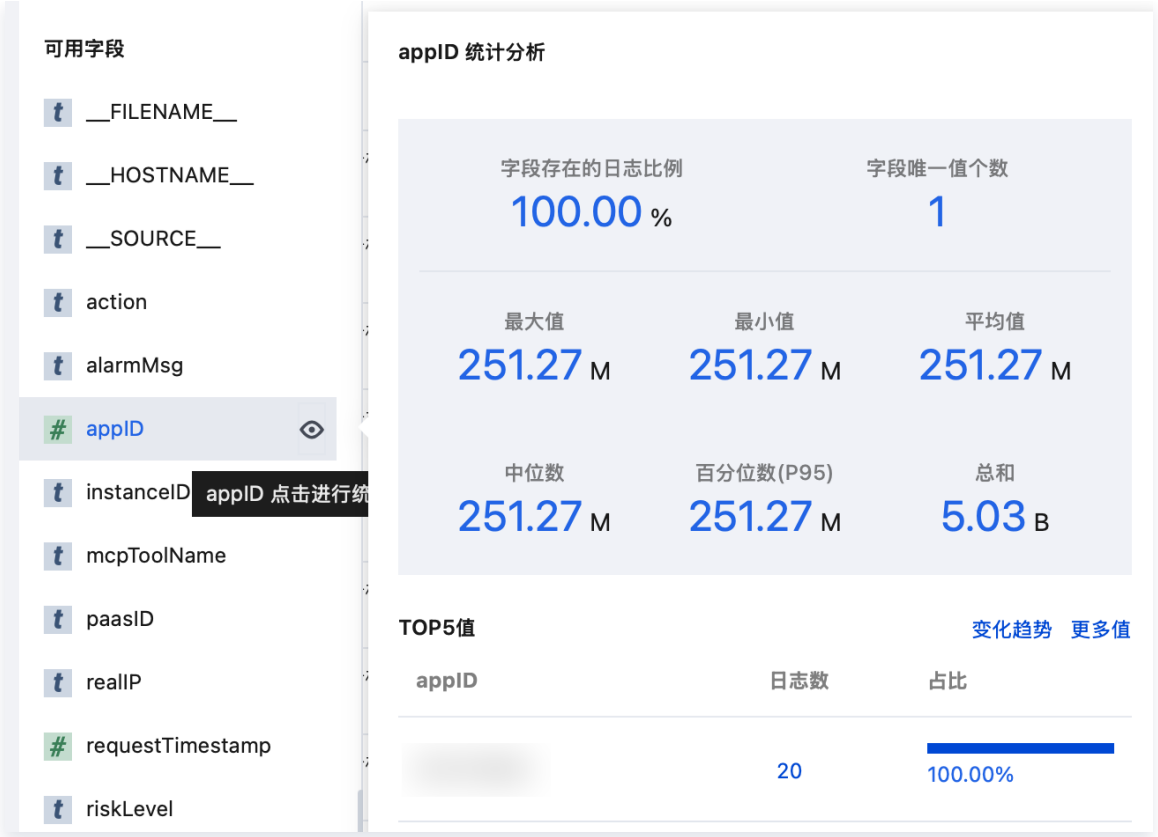
大模型安全网关默认提供攻击安全日志功能，详细记录安全规则被触发的时间、安全规则类型等信息。安全日志支持基于 SQL 的原始日志和统计图标的查看方式。

操作步骤

1. 登录 大模型安全网关控制台 ，在左侧导航栏中，选择**安全日志**。
2. 在安全日志页面，选择要检索的日志所属实例。
3. 在检索框中可添加检索条件与日志时间范围，对数据进行筛选。



4. 在原始日志页签，支持对字段进行快速统计分析，无需编写查询语句即可快速查看字段值的分布、时间变化趋势及数值统计。


可用字段
__FILENAME__
__HOSTNAME__
__SOURCE__
action
alarmMsg
appID
instanceID
appID 点击进行统
mcpToolName
paasID
realIP
requestTimestamp
riskLevel
appID 统计分析
字段存在的日志比例
100.00 %
字段唯一值个数
1
最大值
251.27 M
最小值
251.27 M
平均值
251.27 M
中位数
251.27 M
百分位数(P95)
251.27 M
总和
5.03 B
TOP5值
变化趋势
更多值
appID
日志数
占比
20
100.00%

订阅 API

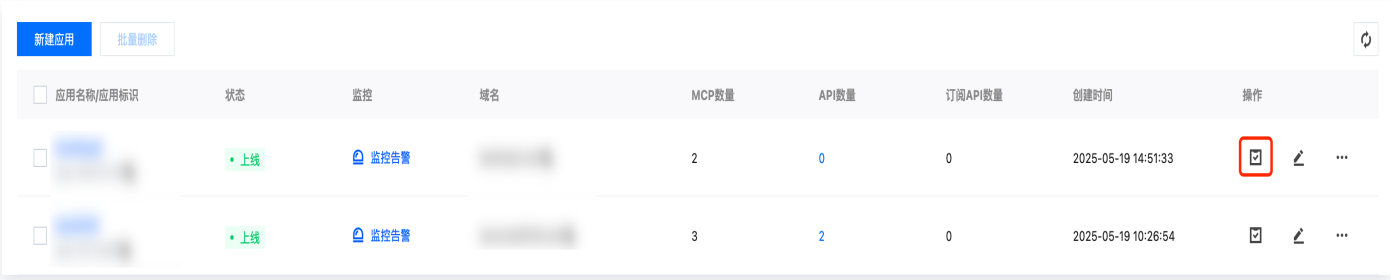
最近更新时间：2025-06-18 14:53:11

操作场景

本文档将指导您如何在应用中订阅已有 API。

操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择**应用**。
2. 在应用页面，选择您要订阅 API 的应用，单击 。



3. 在订阅 API 窗口中，您可以从 API 列表中选择需要订阅的 API，或者使用搜索栏根据 API 名称、标识、路径等条件进行快速检索，同时支持模糊搜索。

4. 选择您要订阅的 API，单击**申请订阅**。
5. 在申请订阅页面，您需要选择鉴权方式（**必选**），控制方法（**必选**），单击**确定**。

参数名称	说明
令牌桶	从固定容量的桶中取令牌，取不到的则触发限流，调整令牌桶容量可以限制请求的数量，调整令牌生成速率可以限制请求的速率。
漏斗	向固定容量的漏斗中加水，水溢出则触发限流，调整漏斗漏容量可以限制请求的数量，调整漏斗流速可以限制请求的速率。
滑动窗口	长度固定窗口向前滑动，请求固定进来占据位置，满则触发限流，调整窗口内最大请求次数可以限制请求的数量，调整窗口长度可以限制请求的速率。
时间窗口	调整时间内最大请求次数可以限制请求的数量，调整时间长度可以限制请求的速率。
出参配置	相关参数配置需要在原始 API 配置，**默认出参配置禁用**，开启后您可以进行配置，也可以选择是否开启数据脱敏。

	
数据脱敏	当前仅支持 String 参数类型下的数据脱敏,请输入0~10之间的数字，脱敏规则展示前 n 后 n，中间省略号显示。 **例如：输入2，则脱敏效果为10***31。**

新建 API

最近更新时间：2025-06-18 14:53:11

本文档将指导您如何新建 API 以用于 MCP Server 服务

操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择 API。
2. 在 API > API 列表页面，单击新建 API。

3. 在基础信息页面，选择 API 基本信息，单击下一步。

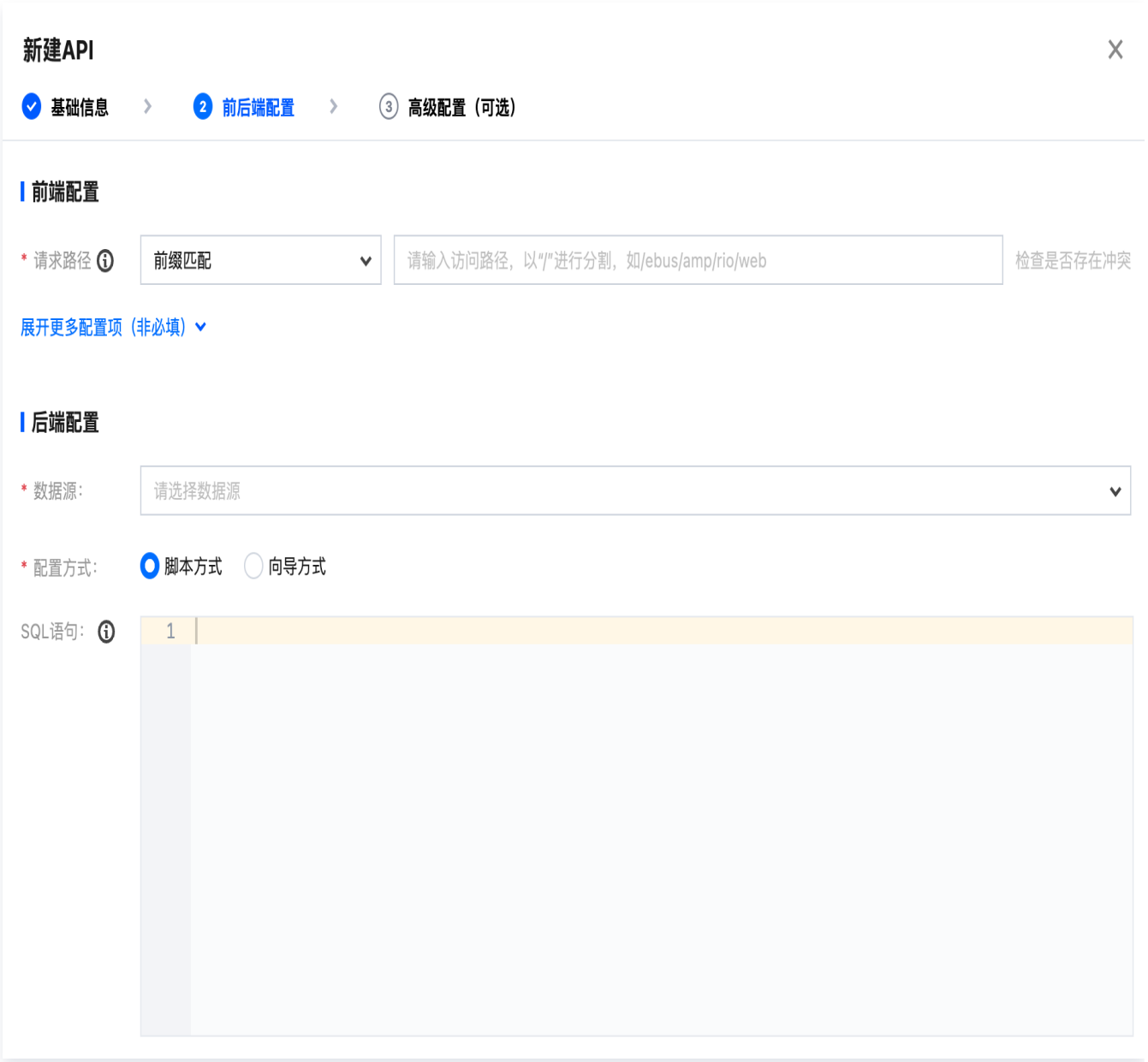
参数名称	参数说明
所属应用	当前 API 所属应用
API 名称	必填，最长32个字符，支持中文、大小写字母、数字、_、()、（ ），实例下唯一
后端服务类型	必填，当前 API 的后端服务类型
鉴权方式	• 签名：适用于需要通过 AKSK 鉴权保护的 API • 认证：适用于需要登录态会话保护的站点类 API，需额外配置认证信息，请参考 API 认证配置 • 免鉴权：适用于开放类 API

4. 在前后端配置页面，根据不同的后端服务类型，配置相关参数，单击**下一步**。
   - Restful：填写对应 Restful 前后端服务信息。

参数名称	参数说明
请求路径	此 API 的对外请求路径与匹配方式
后端服务方式	此 API 对应的后端服务的组织方式
后端服务类型	此 API 对应的后端服务的网络连接方式
后端服务	此 API 对应的后端服务的网络连接信息
负载方式	此 API 对应的多个后端服务间的请求分发策略
协议类型	此 API 对应的后端服务协议类型，支持 http 和 https
协议版本	此 API 对应的后端服务协议版本，支持 1.0、1.1 和 2.0

请求 host 类型	此 API 请求中的 host 头部信息处理方式
后端路径	此 API 对应的后端服务访问路径

- 数据库：填写对应数据库前后端服务信息。



参数名称	参数说明
请求路径	此 API 的对外请求路径与匹配方式
数据源	此 API 要操作的数据源
配置方式	• 脚本方式：自行编写脚本代码完成数据源服务配置 • 向导方式：根据服务引导完成数据源配置

- Mock：填写对应 Mock 测试的前后端服务信息。

参数名称	参数说明
请求路径	此 API 的对外请求路径与匹配方式
响应码	此 API 的请求处理结果

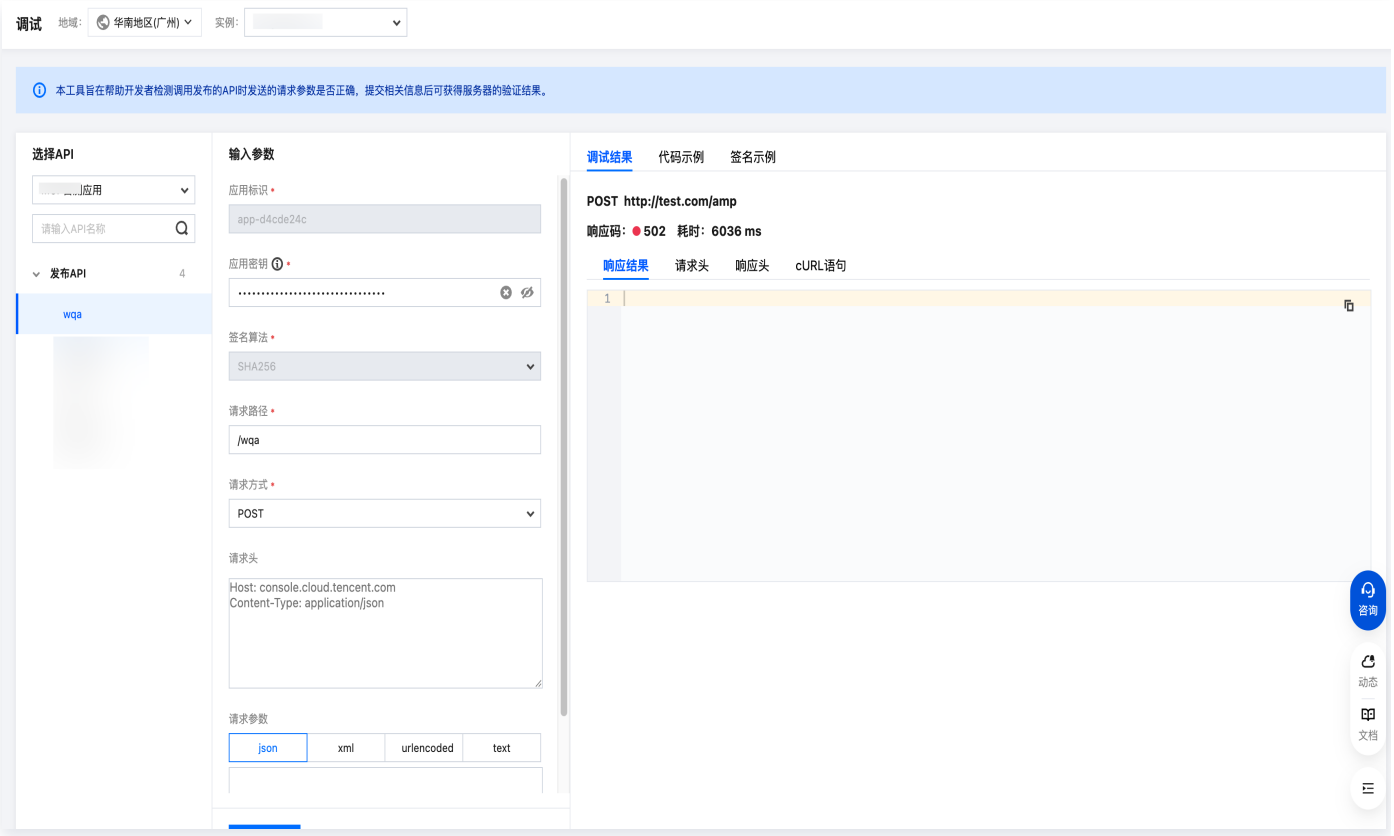
5. 在高级配置页面，配置相关参数。

参数名称	参数说明
流量控制	配置此 API 的限流算法、限流方案及超时控制
健康检查	配置此 API 对应的后端服务健康检查方案

格式转换	配置此 API 请求和响应的数据格式协议类型
IP 黑名单	配置此 API 的 IP 黑名单，和 IP 白名单互斥
IP 白名单	配置此 API 的 IP 白名单，和 IP 黑名单互斥

6. 单击**保存**，即可完成创建 API。

7. 通过 API 调试 页面，您可以在配置完 API 后立即验证 API 的正确性，发起模拟 API 调用并查看具体请求响应。如果 API 未按照您期望的方式工作，可以根据响应，重新修改配置以符合您的设计期望。在调试页面，选择应用及发布的 API 后，单击**调试**，即可查看本次调试的返回结果。



新建封装 MCP

最近更新时间：2025-06-18 14:53:11

本文档将指导您如何新建封装 MCP 服务。在此之前，请确认您已创建所需的 API。如需创建 API，请参考 新建 API 。

操作步骤

1. 登录 大模型安全网关控制台 ，在左侧导航栏中，选择 MCP。
2. 在 MCP 页面，单击**新建封装 MCP**。

3. 选择当前封装 MCP 所属的应用，输入 MCP 信息。

参数名称	参数说明
所属应用	选择当前 MCP 服务所属的应用。
MCP 名称	请仔细填写 MCP 名称，在调用时会被大模型理解，支持中/英文、数字、字符，字符长度1-64。
鉴权方式	后端服务的鉴权方式，支持 SM3/SHA256 的签名鉴权和免鉴权的方式。

4. 单击**下一步**，在 **API 列表**中选择需要导入的 **API**。

5. 单击**导入工具**，在高级配置中选择需要启用的检测规则和访问控制，并设置相应的处置动作。

6. 单击**保存**，根据请求路径进行调试。

新建封装MCP

您已新增MCP服务，MCP成功调用还需完成以下操作
如需修改MCP信息，可到MCP详情页面 编辑MCP

1 复制请求路径

请求路径 http: 或 可前往控制台【MCP 列表页面复制】

工具数量	接入模式	关联规则数	状态	请求路径	监控
1	封装模式	13	已上线	http://	

新建代理 MCP

最近更新时间：2025-06-18 14:53:11

本文档将指导您如何新建代理 MCP 服务。

操作步骤

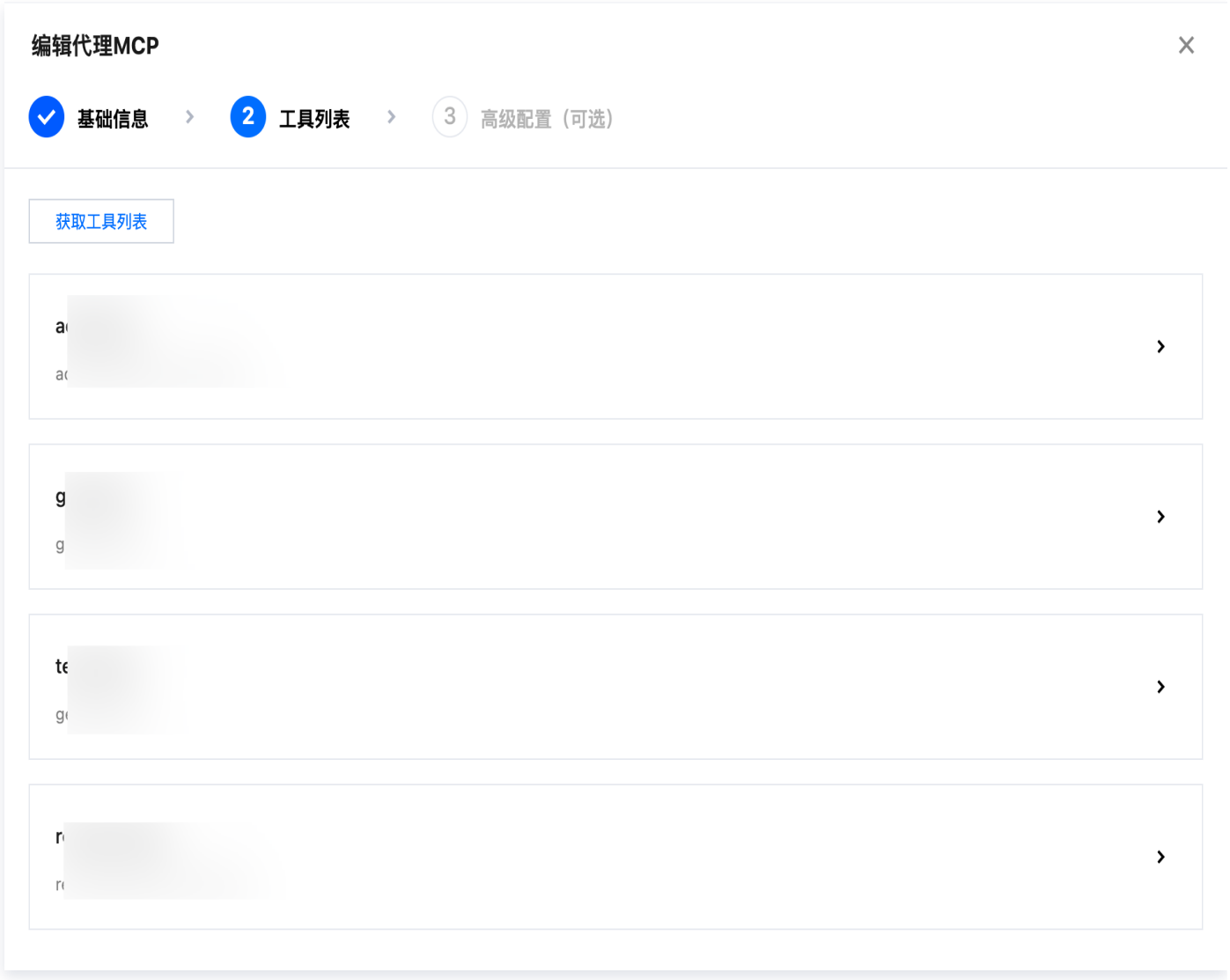
1. 登录 大模型安全网关控制台，选择左侧任务栏中，选择 MCP。
2. 在 MCP 页面，单击**新建代理 MCP**。

3. 选择当前代理 MCP 所属的应用，输入 MCP 信息。

参数名称	参数说明
所属应用	选择当前 MCP 服务所属的应用。
MCP 名称	请仔细填写 MCP 名称，在调用时会被大模型理解，支持中/英文、数字、字符，字符长度1-64。

后端服务	必填，选择代理 MCP 的后端服务实现方式。
负载方式	必选，此代理 MCP 对应的多个后端服务间的请求分发策略。
MCP 协议类型	必选，当前代理 MCP 的后端服务协议类型。
后端路径	服务部署的原始地址，通过访问路径访问时，请求会被转发到后端路径。
鉴权方式	后端服务的鉴权方式，支持 SM3/SHA256 的签名鉴权和免鉴权的方式。

4. 单击**下一步**，获取当前 MCP 协议下的工具信息。



5. 单击**下一步**，在高级配置中选择需要启用的检测规则和访问控制，并设置相应的处置动作。

6. 单击**保存**，根据请求路径进行相关调试。

新建代理MCP

您已新增MCP服务，MCP成功调用还需完成以下操作
如需修改MCP信息，可到MCP详情页面 编辑MCP

1 复制请求路径

请求路径 http 或 可前往控制台【MCP 列表页面复制】

工具数量	接入模式	关联规则数	状态	请求路径	监控
	代理MCP模式	14	已上线		

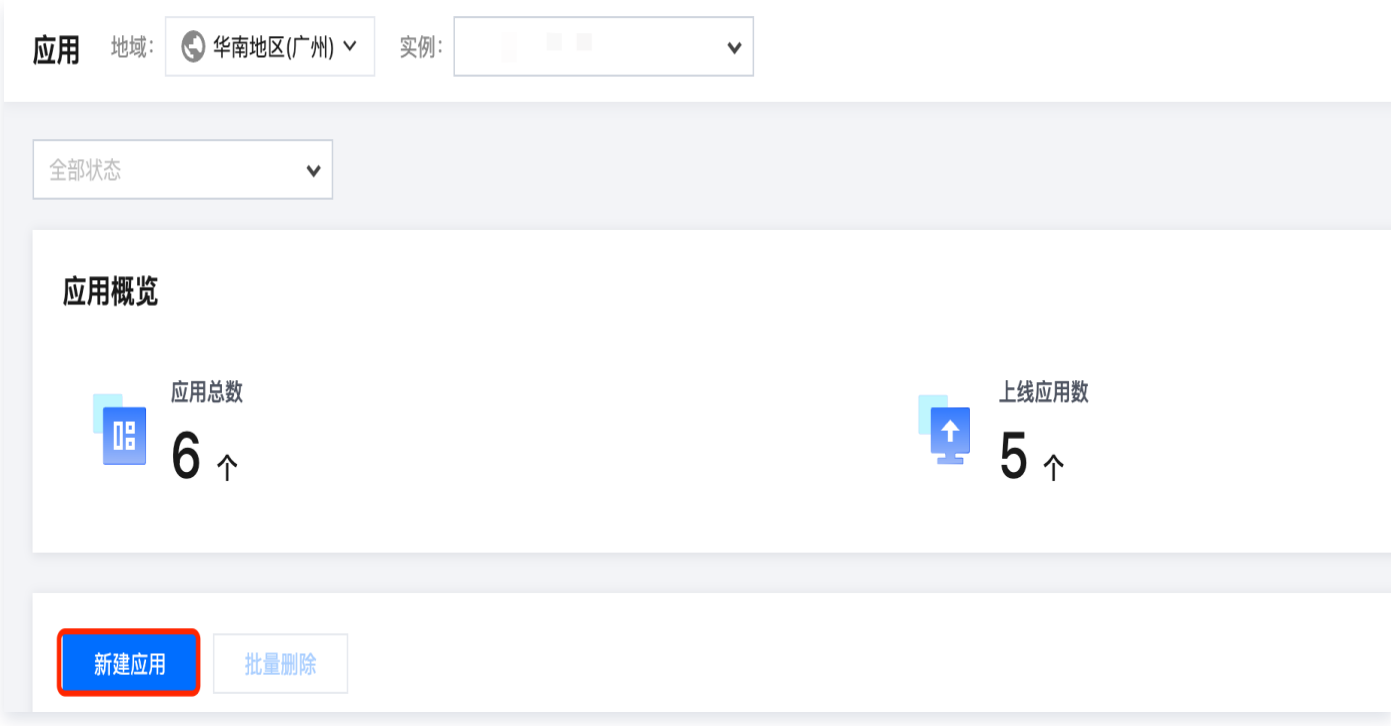
新建应用

最近更新时间：2025-06-18 14:53:11

通常，网关能力的实现需要通过相关的 API 来实现，大模型安全网关的应用管理模块可以帮您高效、便捷地管理一组有关联的 MCP Server 和 API。本文档将指导您如何在大模型安全网关创建一个应用。

操作步骤

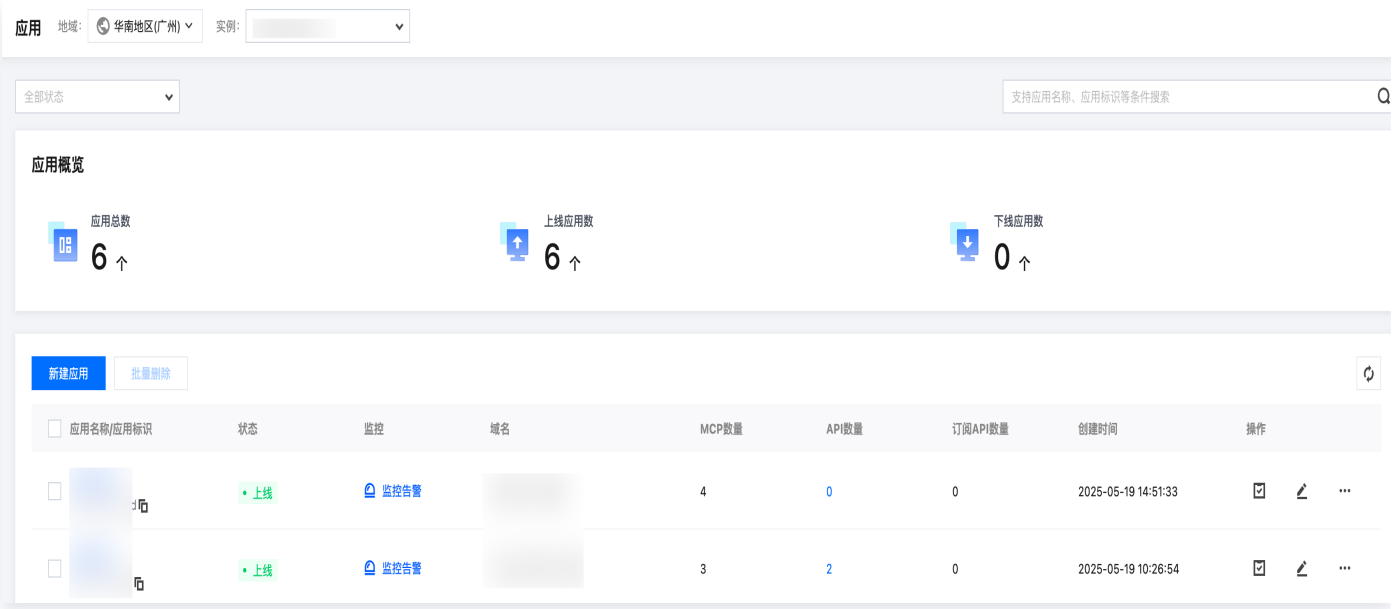
1. 登录 大模型安全网关控制台，在左侧导航栏中，选择**应用**。



2. 单击**新建应用**，输入应用配置信息。

参数名称	参数说明
应用名称	必填，最长64个字符，支持中文、大小写字母、数字、_、()、（），当前实例下唯一
域名	必填，API需要匹配的域名
协议	必选，支持HTTP、HTTPS等标准网络协议
应用密钥	必填，最长32个字符，支持中文、大小写字母、数字
描述	最长64个字符

3. 单击**确定**，即可创建应用。



4. 应用创建完成后，您可以根据实际需要继续创建 API 与 MCP 服务。

参数名称	参数说明
应用名称	用户自定义应用的名称
应用标识	系统自动生成的应用唯一 ID
状态	应用状态分为上线、下线两种
监控	您可以单击跳转监控告警页面，然后单击**设置告警**跳转腾讯云监控平台，针对您的应用设置告警策略
域名	MCP server和API需要匹配的域名
MCP 数量	该应用下的 MCP server 数量
API 数量	该应用下的 API 资产数量
订阅 API 数量	该应用订阅的 API 资产数量
创建时间	您创建该应用的时间
操作	您可以选择 订阅 API 、编辑应用、下线应用、删除应用

功能列表

最近更新时间：2025-06-18 14:53:11

本文介绍当前大模型安全网关所支持的功能，便于您更好地了解各个模块特性，并根据自身需要配置各项功能。

业务接入

功能名称	功能描述
应用	根据应用类型对 API 和 MCP 进行分组管理
MCP	根据应用需求，添加和管理应用下的 MCP Server，并差异化配置信息安全过滤规则
API	根据应用需求，添加和管理 API 服务、数据源、后端服务组，以用于 MCP 封装

日志管理

功能名称	功能描述
安全日志	记录接入业务中触发的安全事件信息
访问日志	记录接入业务中访问行为的相关信息

基础配置

MCP 安全类功能

功能名称	功能描述
安全检测规则	涵盖注入类、MCP 投毒类等复杂网络安全攻击行为的识别及应急响应
敏感规则检测	覆盖如身份证、手机号、邮箱等关键数据字段的检测，并支持敏感数据脱敏操作
内容安全规则	支持对于文本、图片等内容信息进行审核，保障当前业务合规性
其他规则	持续跟进新型攻击特征演变，实现防护体系的动态优化

API 调试及常用功能

功能名称	功能描述
API 调试	在线调试 API，校验 API 服务情况
插件	定制类 MCP Server 能力支持

公共配置	管理认证类 API 的认证信息、API 标签及目录

资源管理

功能名称	功能描述
套餐包	查看和管理实例下的套餐情况
实例管理	查看和管理当前接入大模型网关的实例情况

API 认证配置

最近更新时间：2025-06-18 14:53:11

大模型安全网关支持通过认证的方式完成对 API 的鉴权，本文档将指导您创建您的认证信息。

操作步骤

1. 登录 大模型安全网关控制台 ，选择左侧任务栏中，选择**公共配置** > **认证中心**。
2. 在**认证中心**页面，单击**新建认证**。

3. 在新建认证页面，根据 API 认证服务类型选择对应认证类，单击**下一步**。
   - 企业微信/政务微信认证

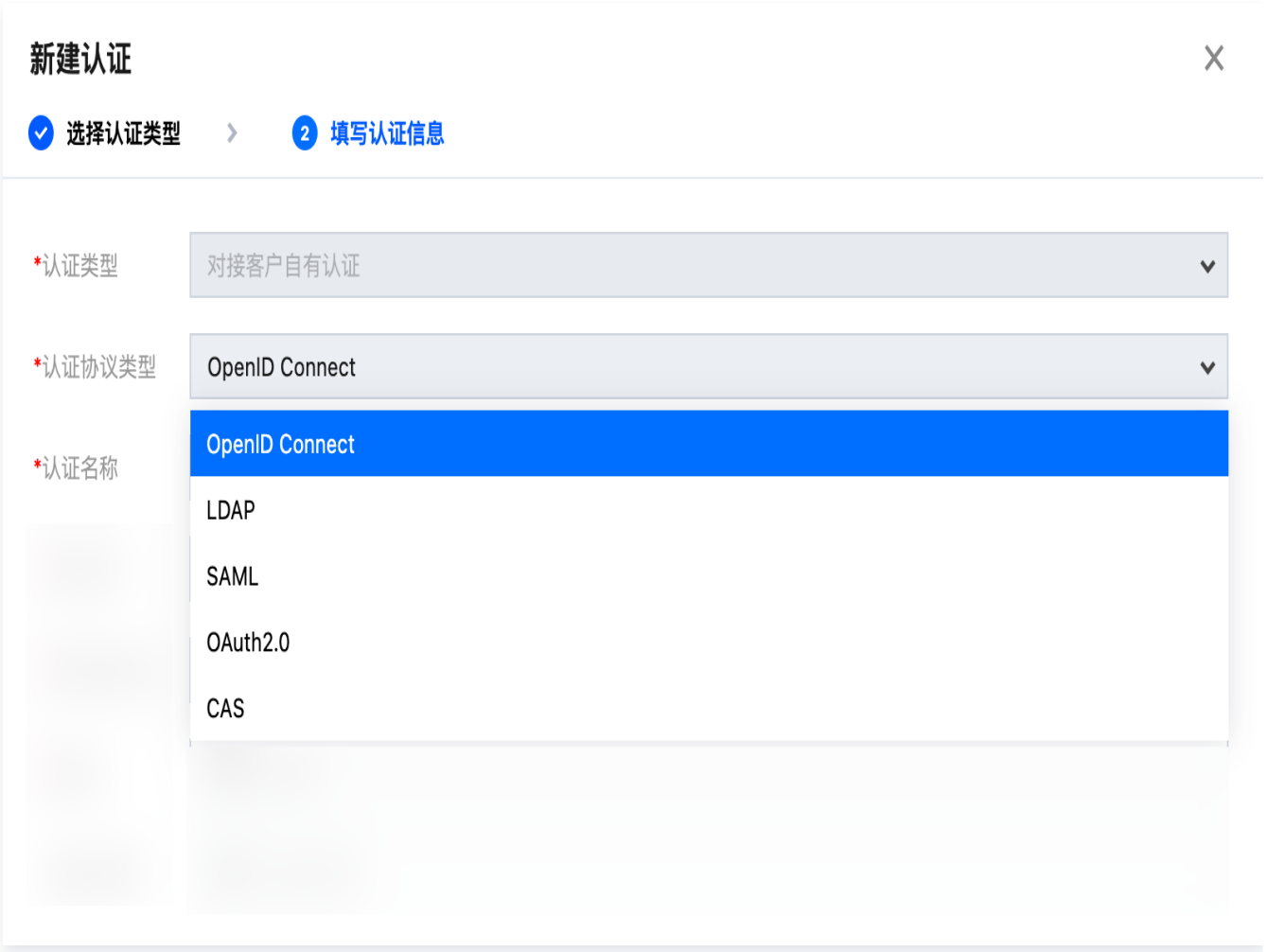
功能名称	功能描述
认证类型	选择通过企业微信网页扫码认证或政务微信网页扫码认证。
认证名称	由64以内的中文、大小写字母、数字、_、-、()、（）组成，实例下唯一。
CorpID	企业 CorpID 可以在 **企业微信管理后台-我的企业** 获取。
AgentID	应用 AgentID 可以在**企业微信管理后台-应用-具体应用**获取。
AppSecret	AppSecret 可以在**企业微信管理后台-应用-具体应用**获取。
Hostname	如果选择通过政务微信网页扫码认证，需要填写认证服务的 Hostname。

- 微信公众号认证

功能名称	功能描述
认证名称	由64以内的中文、大小写字母、数字、_、-、()、（）组成，实例下唯一。
AppID	AppID 可以在微信公众号-开发者中心获取。
AppSecret	AppSecret 可以在微信公众号-开发者中心获取。

- **对接客户自有认证**

  当前支持 OpenID Connect、LDAP、SAML、OAuth2.0、CAS 类型的认证协议，请根据自身业务情况选择并填写对应的认证服务信息。



4. 单击**下一步**，即可完成认证服务的创建。

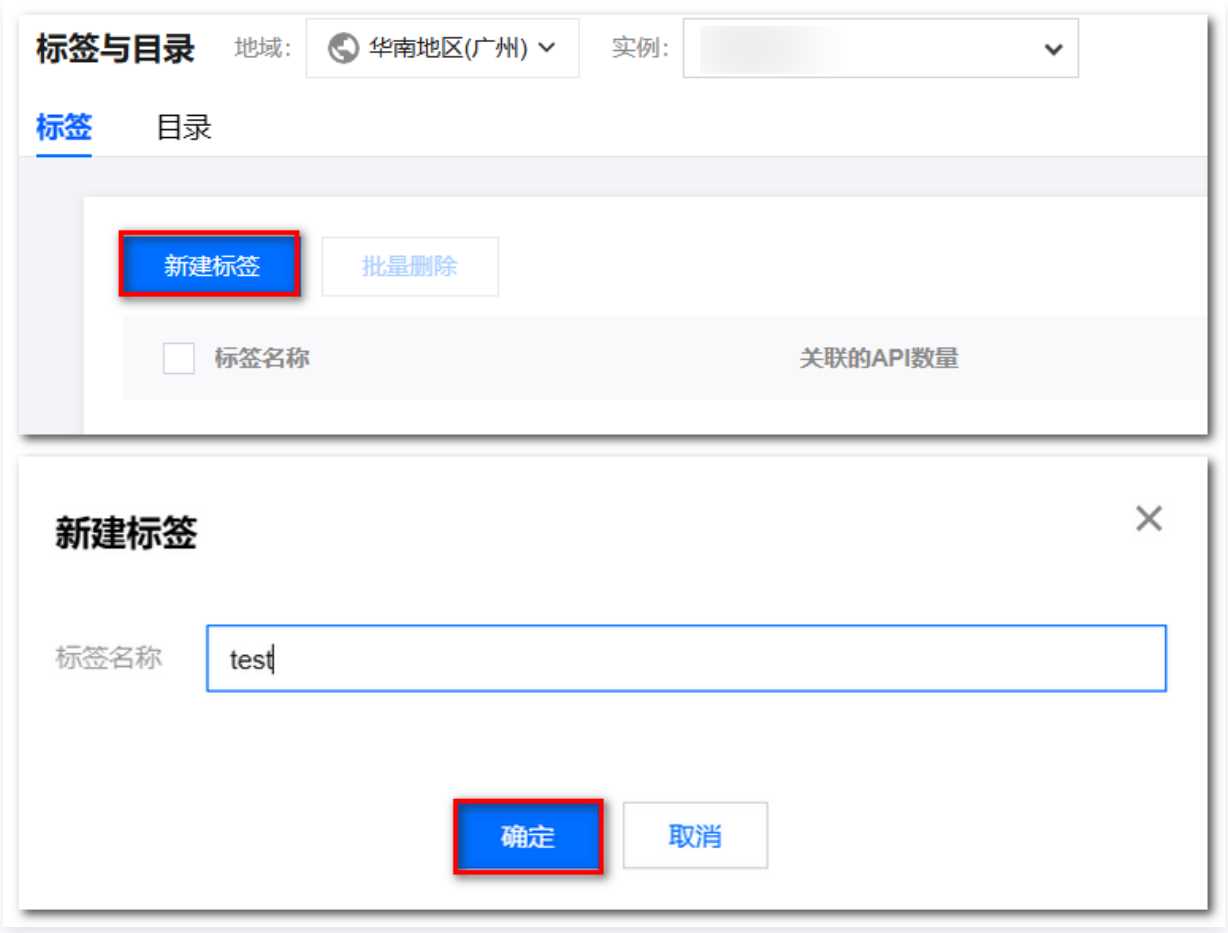
标签与目录创建

最近更新时间：2025-06-18 14:53:11

大模型安全网关支持标签与目录的方式完成对 API 的分类归纳，本文档将指导您创建您的标签与目录信息。

操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择**公共配置** > **标签与目录**。
2. 在**标签与目录**页面，分别创建标签和目录。
   - 单击**标签** > **新建标签**，输入标签名称，单击**确定**，创建您的 API 标签。



   - 单击**目录** > **新建目录**，输入目录名称，单击**确定**，创建您的 API 目录。

参数名称	参数说明
标签名称	由64以内的中文、大小写字母、数字、_、-、()、()组成，实例下唯一
目录名称	由64以内的中文、大小写字母、数字、_、-、()、()组成，实例下唯一

安全检测规则配置

最近更新时间：2025-07-01 21:41:21

大模型安全网关支持对 MCP 安全检测规则的统一管理，本文档将指导您进行 MCP 安全检测规则配置。

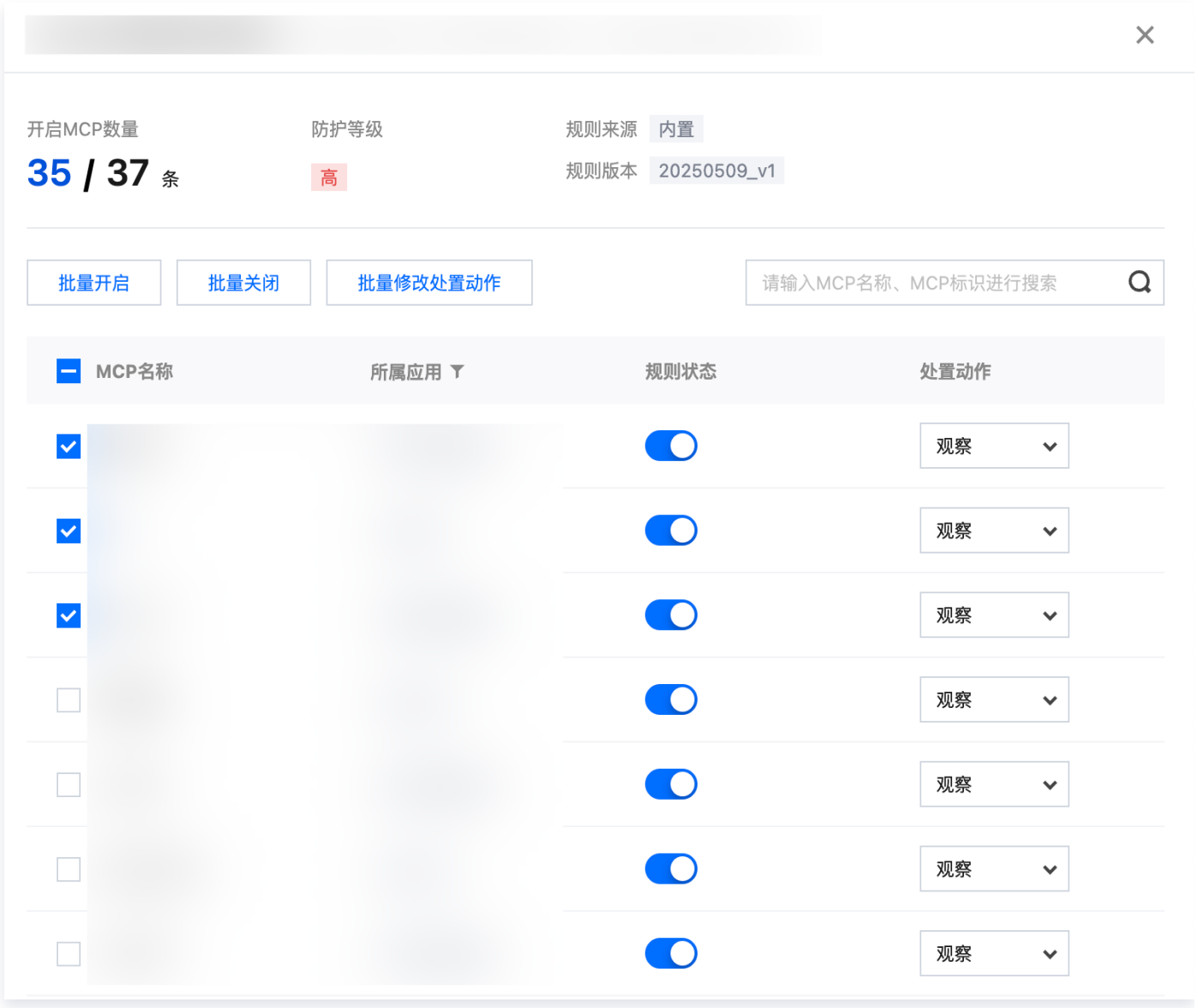
操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择 **MCP 安全 > 安全检测规则**。
2. 在安全检测规则页面，您可以根据实际业务需要，选择对应的规则进行配置。

安全检测规则名称	规则说明	处置动作
XSS 注入检测	识别 mcp 服务调用过程中，参数可能存在的 XSS 注入攻击	观察、拦截
SSRF 注入检测	识别 mcp 服务调用过程中，参数可能存在的 SSRF 注入攻击	观察、拦截
SQL 注入检测	识别 mcp 服务调用过程中，参数可能存在的 SQL 注入攻击	观察、拦截
路径遍历检测	识别mcp服务调用过程中，参数可能存在的路径遍历攻击	观察、拦截
mcpTool 投毒攻击检测	识别 mcp 服务的 Tool 列表的描述信息中，可能存在的投毒攻击内容	观察、过滤、拦截、脱敏
mcp 调用投毒攻击检测	识别 mcp 服务调用的响应信息中，可能存在的投毒攻击内容	观察、过滤、拦截、脱敏
命令注入检测	识别 mcp 服务调用过程中，参数可能存在的命令注入攻击	观察、拦截

3. 单击**规则设置**，您可以管理当前规则下的 MCP Server 配置情况。

4. 在规则设置中，您可以选择对应的 MCP Server 进行规则状态更改以及处置动作更改。



5. 在特殊情况下，您可以开启**一键 ByPass**，开启后当前规则下所有的应用及 MCP 不再进行相关规则的检测。

> **注意：**
> 开启一键 ByPass，仅适用于临时应急，不建议长期开启。

敏感检测规则配置

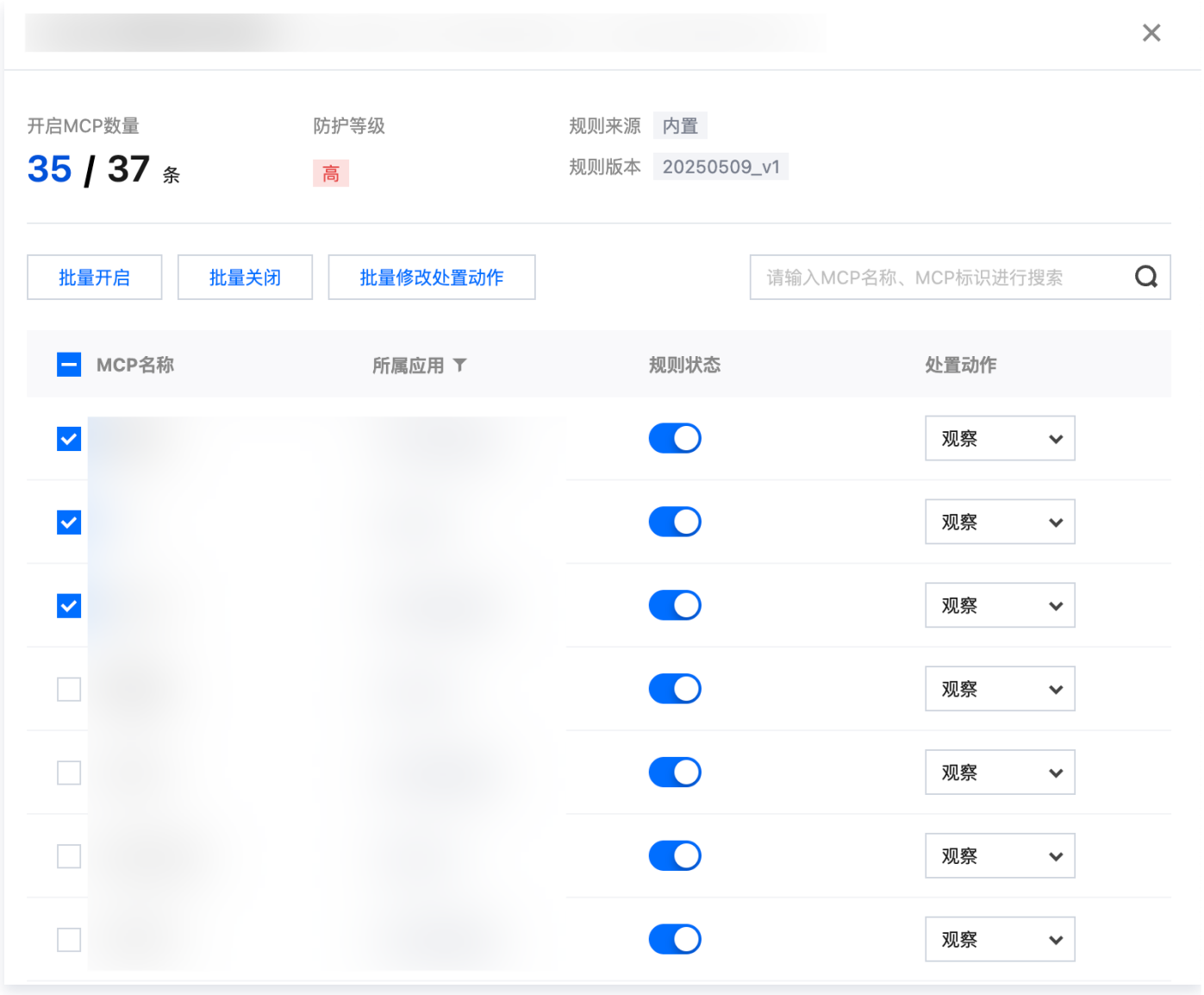
最近更新时间：2025-07-01 21:41:21

大模型安全网关支持对 MCP 敏感检测规则的统一管理，本文档将指导您进行 MCP 敏感检测规则配置。

操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择 **MCP 安全 > 敏感检测规则**。
2. 在敏感检测规则页面，您可以根据实际业务需要，选择对应的规则进行配置。当前支持如身份证、手机号、邮箱等关键数据字段的检测，并对敏感数据进行脱敏处理。
3. 单击**规则设置**，您可以管理当前规则下的 MCP Server 配置情况。

4. 在规则设置中，您可以选择对应的 MCP Server 进行规则状态更改以及处置动作更改。



5. 在特殊情况下，您可以开启**一键 ByPass**，开启后当前规则下所有的应用及 MCP 不再进行相关规则的检测。

> **注意：**
> 开启一键 ByPass，仅适用于临时应急，不建议长期开启。


MCP安全
地域:
华南地区(广州)
实例:
安全检测规则 (7)
敏感检测规则 (13)
内容安全规则 (2)
其他规则 (0)
敏感检测规则
覆盖如身份证、手机号、邮箱等关键数据字段的检测，并支持敏感数据脱敏。
一键ByPass
防护等级
关联MCP数
规则来源
规则版本
高
条
规则设置

内容安全规则配置

最近更新时间：2025-06-18 14:53:11

大模型安全网关支持对 MCP 内容安全规则的统一管理，本文档将指导您进行 MCP 内容安全规则配置。

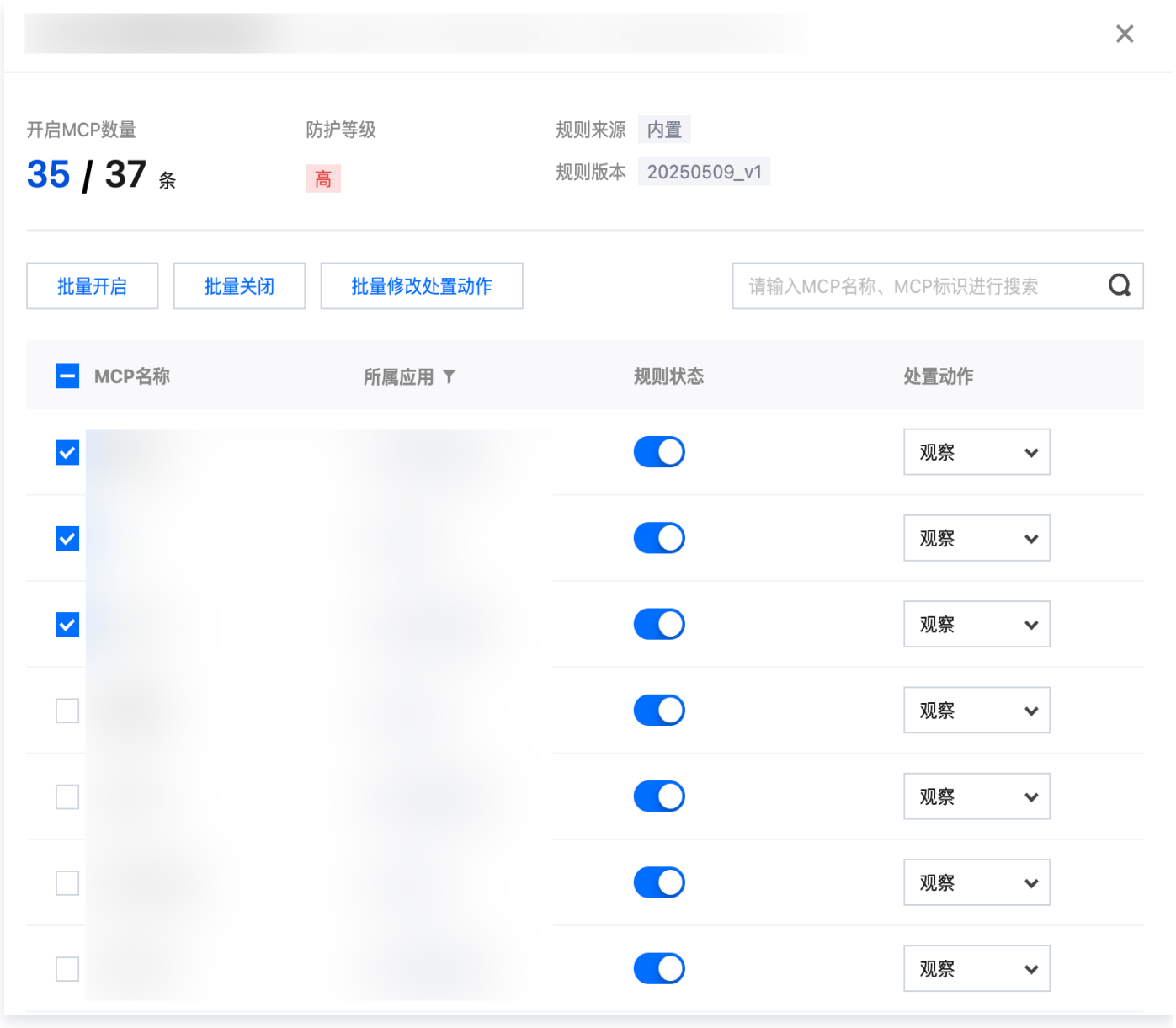
操作步骤

1. 登录 大模型安全网关控制台，在左侧导航栏中，选择 **MCP 安全 > 内容安全规则**。
2. 在内容安全规则页面，您可以根据实际业务需要，选择对应的规则进行配置。

安全检测规则名称	规则说明	处置动作
文本内容安全检测	识别 MCP 服务调用过程中，响应参数文本信息中可能涉及到的安全合规问题	观察、拦截
图片内容安全检测	识别 MCP 服务调用过程中，响应参数为图片时可能涉及到的安全合规问题	观察、拦截

3. 单击**规则设置**，您可以管理当前规则下的 MCP Server 配置情况。

4. 在规则设置中，您可以选择对应的 MCP Server 进行规则状态更改以及处置动作更改。



5. 在特殊情况下，您可以开启**一键 ByPass**，开启后当前规则下所有的应用及 MCP 不再进行相关规则的检测。

> ⚠ **注意：**
> 开启一键 ByPass，仅适用于临时应急，不建议长期开启。


MCP安全
地域:
华南地区(广州)
实例:
安全检测规则 (7)
敏感检测规则 (24)
内容安全规则 (2)
其他规则 (0)
内容安全规则
支持对于文本、图片等内容信息进行审核，保障业务合规性。
一键ByPass
防护等级
关联MCP数
规则来源
规则版本
高
条
规则设置