云安全中心

操作指南

腾讯云

文档目录

操作指南
资产中心

最近更新时间：2024-08-28 18:57:11

资产中心是公有云上的资产管理系统，可以自动同步腾讯云的多种云上资产，手动添加非腾讯云 IP、非腾讯云域名进行统一管理。可自动同步的腾讯云资产详情如下：

资产类型	资产详情	
主机资产	腾讯云	云服务器 CVM
		轻量应用服务器 Lighthouse
		边缘计算器
	其他云	亚马逊云服务器 AWS EC2
		微软云服务器 Azure VMs
容器资产	容器	
	本地镜像	
	仓库镜像	CCR 镜像
		TCR 镜像
		Harbor 镜像
		亚马逊云镜像 AWS ECR
		微软云镜像 Azure ACR
	主机节点	CVM
		Lighthouse
		超级节点
	集群	托管集群
		独立集群
		边缘集群
		弹性集群
		自建K8s集群
		自建Openshift集群
	Pod	
公网 IP 资产	公网 IP	
	高可用虚拟 IP	
	弹性 IP	
	弹性 IPv6	

	anycast IP	
	非腾讯云 IP	
域名资产	域名	
	非腾讯云上域名	
网络资产	网关	NAT 网关
		VPN 网关
		负载均衡 CLB
		NAT 防火墙
		探针 Probe
		亚马逊云负载均衡 ELB
		本地网络 Local Network
		虚拟网络 Virtual Network
	弹性网卡 ENI	
	私有网络 VPC	
	子网	
云数据库	腾讯云	云数据库 MySQL
		云数据库 Redis
		云数据库 MariaDB
		云数据库 PostgreSQL
		云数据库 MongoDB
	其他云	亚马逊云 DynamoDB
		亚马逊云OpenSearch
		微软云 Postgre
		微软云 MySQL
		微软云 Redis
其他云资源	云硬盘 CBS	
	对象存储 COS	
	文件存储	
	消息队列	
	Elasticsearch Service	
	密钥管理系统 KMS	
	操作审计 CloudAudit	

	API 网关 API Gateway
	SSL 证书
	安全组 SecurityGroup
	其他证书

更新资产

在 资产中心页面，单击左上角的**资产更新**，云安全中心会自动获取腾讯云上的资产信息，并展示在下发列表；如果资产较多，该过程可能需要3~5分钟，如需更新容器资产需要更长时间。

> **说明：**
> 资产更新可以自动同步腾讯云上的资产，非腾讯云上资产，请参见 添加云外资产 。

搜索资产

- 在 资产中心页面，支持按照资产类型，查询该账号下的主机资产、容器资产、域名资产和公网 IP 资产等情况。

- 在 资产中心页面，支持按照资产分组，在网络结构的视角，查询每个地域下，分别有哪些 VPC，每个 VPC 内分别有哪些资产。

- 在 资产中心页面，支持按照服务类型，查询不同 Web 服务下，分别有哪些 VPC，每个 VPC 内分别关联哪些资产。

标记核心资产

资产中心会自动识别一部分核心资产，我们也建议您根据自己的业务进行梳理，对关键系统所在的业务，标记为核心资产。

- 在 资产中心页面，选择目标非核心资产，单击**更多 > 标记核心资产**。为该资产打上标签，标签会显示在资产名称的右侧。

- 在 资产中心页面，选择目标核心资产，单击**更多 > 标记非核心资产**。

- 在 资产中心页面，可以根据防护状态筛选资产。云安全中心会自动同步展示资产的防护情况，对应关系为：
  - 主机资产，使用腾讯云主机安全防护。
  - IP 资产，使用腾讯云防火墙防护。
  - 域名资产，使用腾讯云 Web 应用防火墙防护。

> **说明：**
> 我们建议您关注自己的核心资产，确保核心资产都得到防护。

添加自定义资产标签

1. 在 资产中心页面，选择目标资产，单击资源标签列下的，可以添加自定义产品标签。

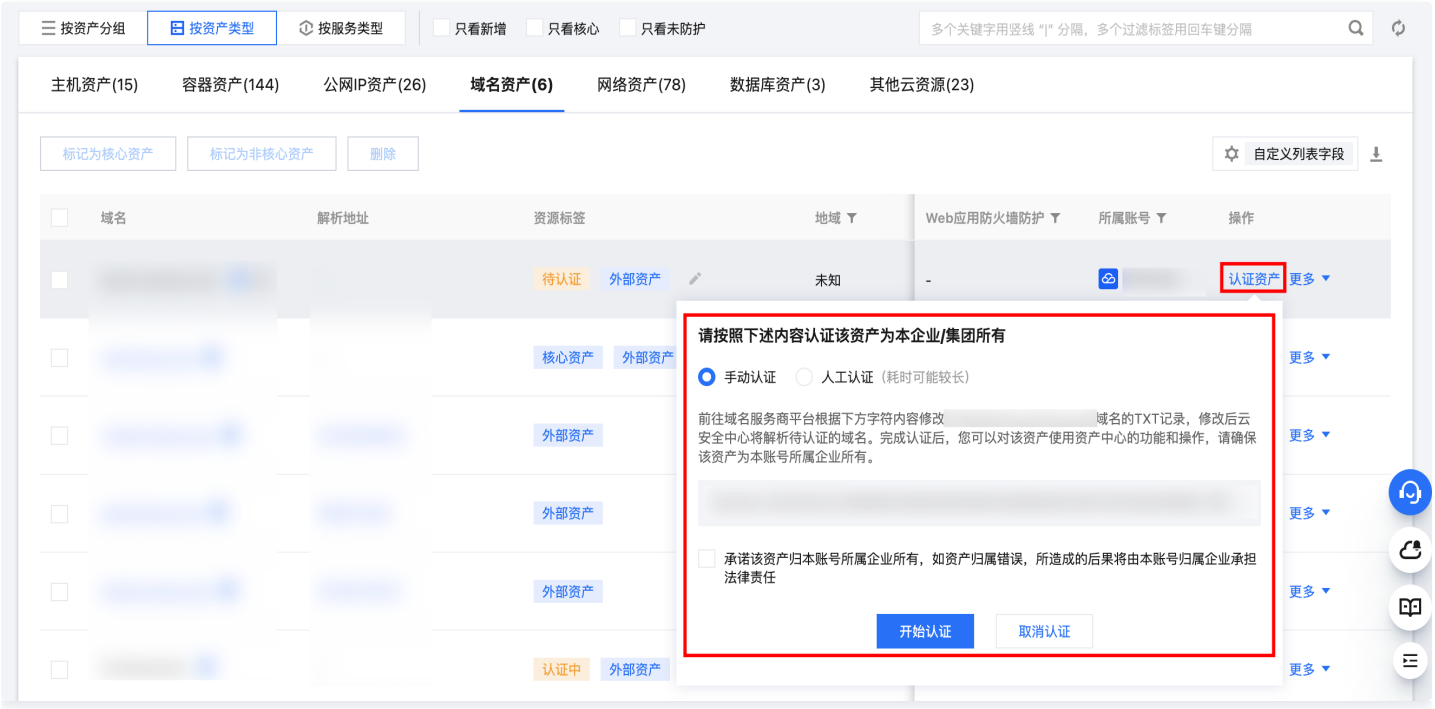
2. 在编辑标签弹窗中，选择标签键和标签值，单击**确定**。

3. 添加标签后，单击**资源标签**，可以按照自定义标签分类查看资产。

添加云外资产

如需管理非腾讯云资产，可以在 资产中心页面 ，选择**接入多云资产、手动添加资产、收集外部资产**。

其中公网 IP 资产、域名资产需经认证后，方可对该资产使用资产中心的功能和操作。



- **在接入多云资产弹窗中，填写相关信息完成配置，详细请参考 多云接入 。**

- **在手动添加资产弹窗中，输入云外公网 IP、域名资产，勾选服务协议，单击确定。**

- **在收集外部资产弹窗中，开启外部资产收集开关，开启后，云安全中心将会使用腾讯安全网络空间资产发现和情报信息收集能力，主动获取您所在企业的外部资产，并自动导入到对应资产列表中；输入企业关键词（为确保收集信息的准确性，建议输入企业或集团的注册公司名称、主站域名或证书），勾选服务协议，单击确定。**

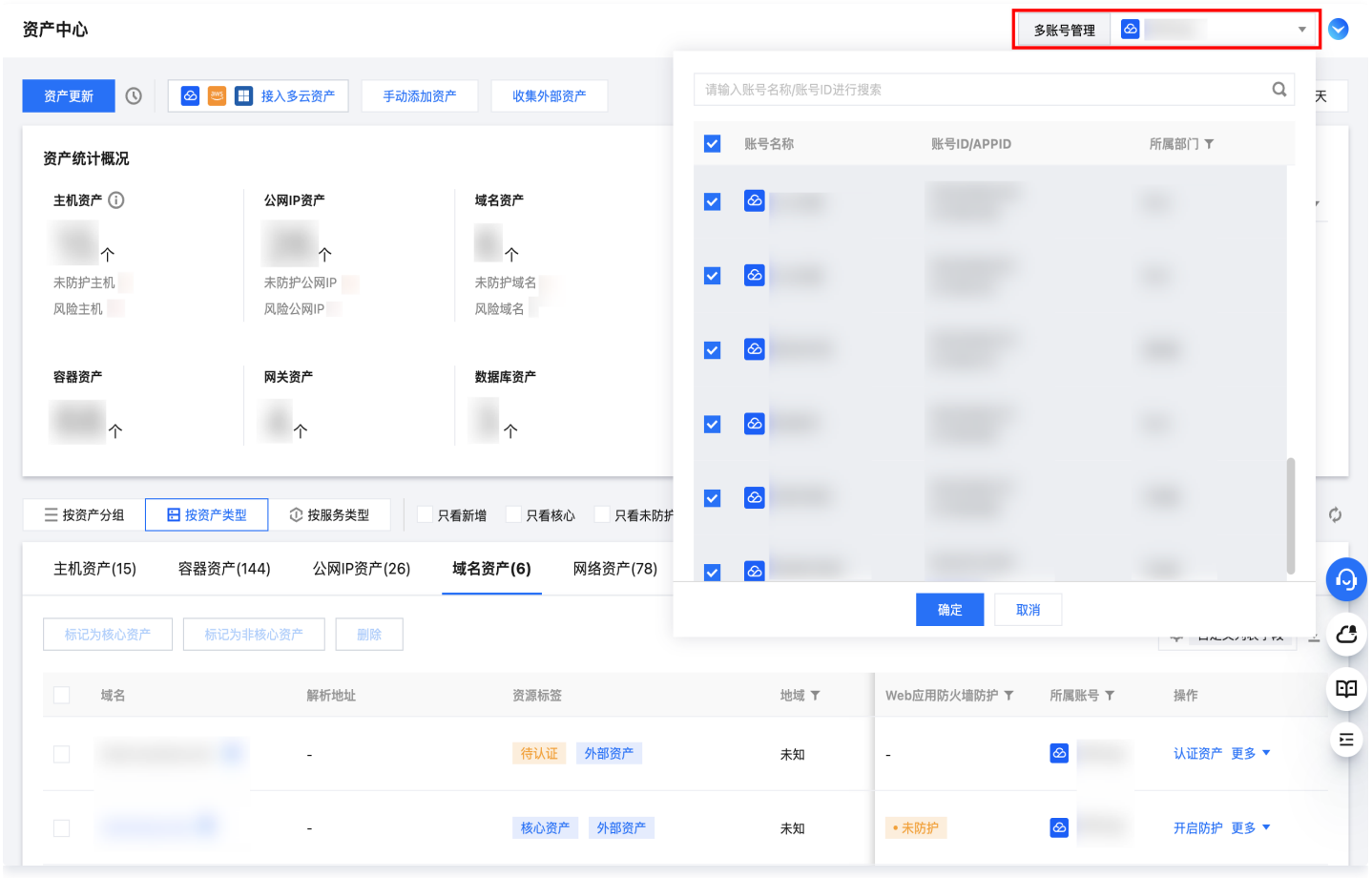
注意：

- **如需添加云外资产，请 提交工单 联系我们。**

- 请勿添加非本账号所有的资产，如使用他人资产将由本账号归属企业承担法律责任。

管理多账号资产

使用云安全中心 多账号管理功能 后，可以在资产中心查看其他账号的资产。单击左上角**多账号管理**，可以切换账号，或选择所有账号进行查看。



云资源配置风险

最近更新时间：2025-08-14 10:10:42

功能介绍

云资源配置风险是通过对云资源的配置进行检查以发现因配置不当引入的安全风险。

访问入口

1. 登录 云安全中心控制台，在左侧导览中，单击**漏洞与风险中心**。
2. 在**漏洞与风险中心** > **云资源配置风险**中，支持查询云资源配置风险。

风险检测

云资源配置风险检测会跟随您资产的同步周期进行检测，您也可以通过以下方式手动触发检测。

1. 登录 云安全中心控制台，在左侧导览中，单击**漏洞与风险中心**。
2. 在**漏洞与风险中心** > **云资源配置风险**中，单击**立即检测**，即可发起云资源配置风险检测。

3. 鼠标移至**立即检测**上方，您可以看到最近一次检测任务的运行时间。

配置项视角

1. 登录 云安全中心控制台，在左侧导览中，单击**漏洞与风险中心**。
2. 在**漏洞与风险中心** > **云资源配置风险**中，选择**配置项视角**，风险按配置项做了聚合统计，用于解决同类问题。

3. 列表按风险处理的优先级进行了风险排序，您可以按顺序进行风险治理。
4. 列表默认勾选了**仅展示高优修复风险**，将隐藏一部分修复优先级较低的风险，若您关注此类风险，可以取消该勾选，查看全部内容。

5. 页面还支持多种筛选条件：首次发现时间、最近发现时间、处理状态、风险等级、云厂商，您可以根据实际使用需求筛选数据。
6. 选择目标数据，单击**详情**，可以看到该条风险的全部详情数据。

7. 在详情页面，您可以查看风险危害、风险修复建议、风险详情。

8. 在风险详情中，您可以查看该配置风险项的完整风险列表，并对目标数据进行验证、标记忽略或标记处置等操作。

资产视角

1. 登录 云安全中心控制台，在左侧导览中，单击**漏洞与风险中心**。
2. 在**漏洞与风险中心** > **云资源配置风险**中，选择**资产视角**，风险按配置项和风险做了聚合统计，可以针对资产进行风险查询。

3. 列表按风险处理的优先级进行了风险排序，您可以按顺序进行风险治理。
4. 列表默认勾选了**仅展示高优修复风险**，将隐藏一部分修复优先级较低的风险，若您关注此类风险，可以取消该勾选，查看全部内容。

5. 页面还支持多种筛选条件：首次发现时间、最近发现时间、资产id、资产名称、处理状态、风险等级、云厂商，您可以根据实际使用需求筛选数据。
6. 选择目标数据，单击**详情**，可以看到该资产对应风险的全部详情数据。

7. 在详情页面，您可以查看风险危害、风险修复建议、风险详情。

8. 在**风险详情**中，您可以查看该配置风险项的完整风险列表，并对目标数据进行验证、标记忽略或标记处置等操作。

策略配置

1. 登录 云安全中心控制台，在左侧导览中，单击**漏洞与风险中心**。
2. 在**漏洞与风险中心** > **云资源配置风险**中，单击**策略配置**，您可以查看风险配置项列表，也可以选择策略进行禁用。

支持的云产品列表

云厂商	产品分类	产品名称
腾讯云	计算	云服务器
		轻量应用服务器
	容器与中间件	容器服务
		容器镜像服务
		云函数
		消息队列 CKafka 版
		消息队列 TDMQ 版
	网络	负载均衡
		弹性公网 IP
		弹性网卡
		NAT 网关
		私有网络
	CDN 与边缘	内容分发网络 CDN
	安全	Web 应用防火墙
		云防火墙
		密钥管理系统
	数据库	云数据库 MySQL
		云数据库 MariaDB
		云数据库 SQL Server
		云数据库 MongoDB
		云数据库 PostgreSQL
		云数据库Redis
		云数据库 KeeWiDB
		向量数据库
		TDSQL MySQL 版
		TDSQL-C MySQL 版
	存储	对象存储
		云硬盘
		文件存储
	大数据	Elasticsearch Service

		弹性 MapReduce
	云通信与企业服务	SSL 证书
	开发与运维	访问管理
		操作审计
		腾讯云可观测平台
阿里云	计算	云服务器 ECS
	容器	容器服务
		容器镜像服务
	网络与 CDN	负载均衡 SLB
		内容分发网络CDN
		弹性公网IP
		弹性网卡 ENI
		NAT 网关
		任播弹性公网 IP
		私有网络
	大数据计算	检索分析服务 Elasticsearch 版
		大数据开发治理平台
	Serverless	函数计算
	中间件	微服务引擎
		API 网关
	数据库	云数据库 RDS
		云数据库 MongoDB 版
		云数据库 Tair（兼容 Redis）
		云数据库 ClickHouse
		云数据库 OceanBase 版
		云原生分布式数据库
		云原生数据仓库 AnalyticDB PostgreSQL版
		云原生数据仓库AnalyticDB MySQL版
		云原生数据库 PolarDB
		数据管理服务 DMS
	存储	对象存储 OSS
		日志服务

	安全	Web 应用防火墙
		云安全中心
		云防火墙
		云身份服务
		堡垒机
	迁移与运维管理	访问控制
AWS	计算	Amazon EC2
		AWS Lambda
	容器	Amazon EKS
		Amazon ECR
	存储	Amazon S3
		Amazon EFS
	数据库	Amazon RDS
		Amazon DynamoDB
		Amazon MemoryDB
		Amazon ElastiCache
	联网和内容分发	Amazon VPC
	前端 Web 和移动应用程序	Amazon API Gateway
	应用程序集成	Amazon SQS
	安全性、身份与合规性	Amazon IAM
	分析	Amazon MSK
		Amazon EMR

安全体检
功能简介

最近更新时间：2024-09-03 10:32:21

功能背景

随着网络攻击和数据泄露等安全事件的频繁发生，企业面临着越来越多的安全威胁和风险，并且企业需要落实相关法规政策的要求、不断提升自身的安全能力建设。因此云安全中心提供一键安全体检功能，帮助企业发现云上业务资产6大潜在安全威胁。

应用场景

日常安全体检

为了及时了解安全状况、定期监测网络安全状况，用户可以根据企业的业务状况、安全需求和安全风险，发起安全体检来评估企业的安全状况。安全体检可以帮助企业在早期发现潜在的安全问题，并采取相应的措施来提高企业的安全水平。

等保合规检测

为了帮助用户满足安全合规要求，安全产品提供了安全体检功能，可以检测云上资产的安全状况，并根据检测结果提供相应的加固建议，用户可以根据自己的需求对云上资产的合规风险进行持续监测和评估。

功能详情

体检项目

体检项目	项目内容	识别来源
端口风险	针对公网 IP、域名的业务，由云安全中心、云防火墙提供的端口暴露检测能力。	云安全中心
漏洞风险	多年的安全能力建设积累了丰富而全面的漏洞规则库，覆盖 OWASP TOP 10的 Web 漏洞，例如：SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、弱密码等。同时，系统还具备专业高效的 0Day/1Day/NDay 漏洞检测能力。	云安全中心、联动主机安全和容器安全
弱口令风险	针对主机资产、公网 IP、域名的通用业务，由云安全中心、主机安全提供的弱口令检测。	云安全中心、联动主机安全
云资源配置风险	提供云资源配置风险的自动化检查评估功能，覆盖云服务器、容器、对象存储、云数据库及负载均衡等多种云资源。	云安全中心、联动主机安全和容器安全
风险服务暴露	针对云上向互联网暴露的资产，提供互联网攻击面测绘功能，快速识别云上资产的暴露端口、暴露服务及暴露组件等潜在攻击面。	云安全中心
网站内容风险	快速准确识别敏感图片、文字信息等网站风险内容，针对网站进行挂马、暗链、垃圾广告、矿池等风险的多维度智能检测。	云安全中心

说明：
当识别来源为云安全中心时，我们可以推断出可能存在的漏洞、弱口令和风险服务暴露内容，但需基于端口扫描获取目标系统上开放的端口和服务信息。例如，如果目标主机开放了80端口（HTTP 服务），则可能存在 Web 应用程序漏洞的风险。

体检资产

体检资产	体检项目
云服务器、轻量应用服务器、边缘计算器	漏洞、弱口令、云资源配置风险

已授权的本地镜像、仓库镜像	漏洞风险
组件运行正常的集群	漏洞、云资源配置风险
公网 IP、域名资产	端口、漏洞、弱口令、网站内容风险
负载均衡、子网、MySQL、Redis、MariaDB、PostgreSQL、MongoDB、云硬盘 CBS、对象存储 COS、Elasticsearch Service	云资源配置风险

注意：
风险服务暴露为云安全中心企业版、旗舰版专属能力，不会消耗体检配额；目前检测子网、云硬盘 CBS 的云资源配置风险也不消耗体检配额。

体检消耗

体检资产	体检项目	消耗体检配额
公网 IP、域名资产	漏洞、弱口令、网站内容风险	1次体检消耗体检配额 = 体检资产数

云安全中心版本功能对比

体检项目	免费版	高级版	企业版	旗舰版
端口风险	✓	✓	✓	✓
应急漏洞	–	✓	✓	✓
漏洞风险	–	✓	✓	✓
弱口令风险	–	✓	✓	✓
云资源配置风险	–	✓	✓	✓
风险服务暴露	–	–	✓	✓
网站内容风险	–	–	✓	✓
体检配额	端口风险检查不消耗配额	400次/月，可扩展	1200次/月，可扩展	4800次/月，可扩展
任务配额	1个	10个	20个	50个，可扩展至不限制

按照表格所述内容，云安全中心将根据版本提供不同体检项目，体检配额、任务配额进行每次安全体检的校验。

操作指引

最近更新时间：2024-09-05 10:12:51

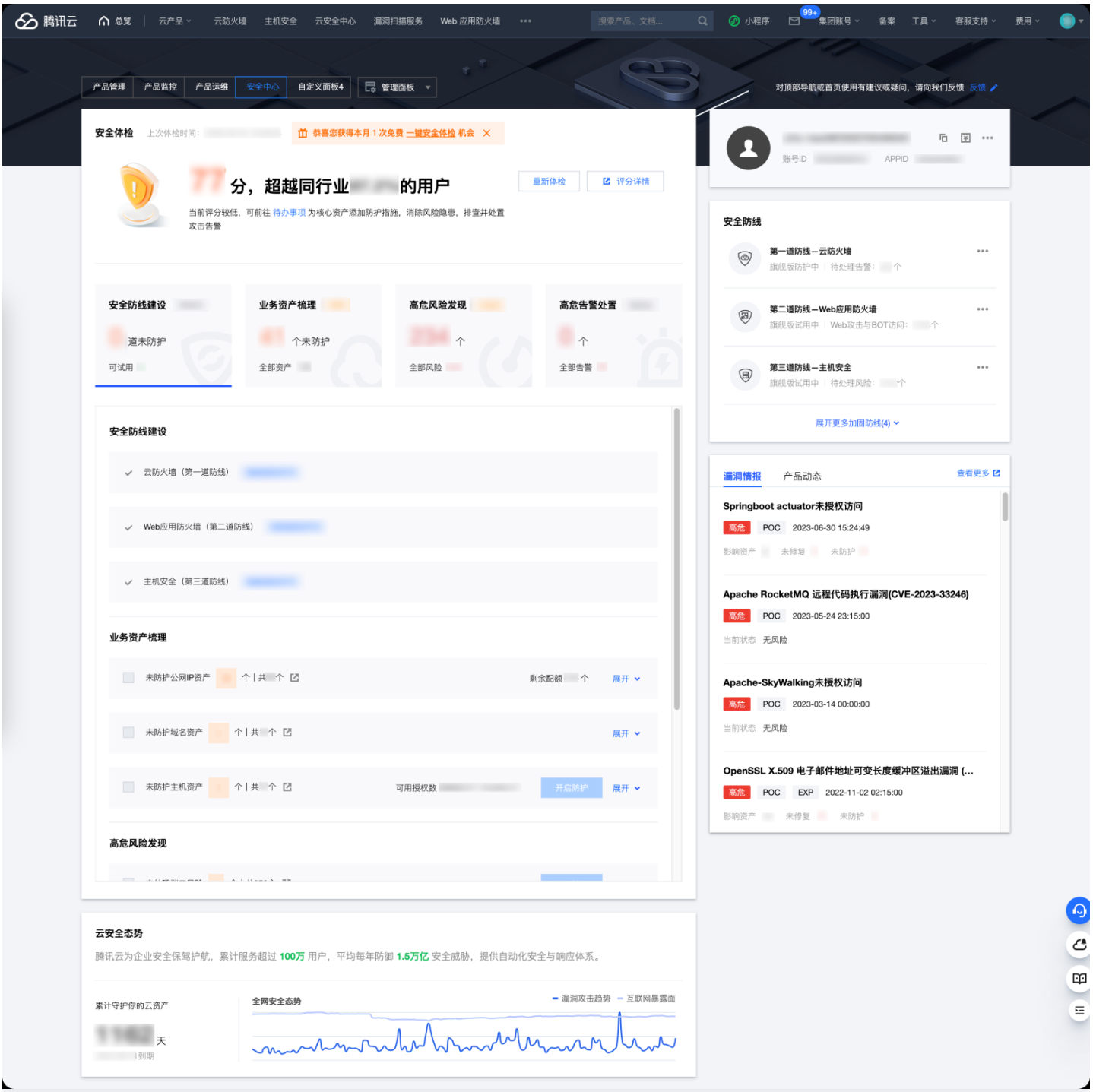
安全体检入口

安全体检

在 安全体检页面，排查用户云上业务暴露在外的端口、敏感信息及服务，发现潜在漏洞、弱口令、云资源配置等安全威胁，支持多种体检模式选择，安全体检将联动云安全中心、主机安全、容器安全三款产品。

总览体检

在 总览体检页面，涵盖防线建立、资产梳理、风险发现和告警统计四个模块，一站式解决开启试用、资产授权、风险处理和告警处置的问题。



创建任务

1. 登录 云安全中心控制台，在左侧导览中，单击**安全体检**。
2. 在体检任务页面，单击**创建安全体检任务**。
3. 在创建安全体检任务弹窗中，配置相关参数，单击**确定**。

参数名称	说明
任务名称	在风险中心中可以直接使用任务名称检索体检结果。
体检模式	• 快速体检：一键快速发起对端口风险、应急漏洞风险、风险服务暴露进行扫描。 • 标准体检：支持对端口风险、漏洞风险、弱口令风险、云资源配置风险、风险服务暴露、网站内容风险等6种风险进行选择性扫描。 • 高级体检：通过创建高级体检任务自定义配置体检项，允许用户手动录入或文件导入方式添加离散端口进行暴露端口检测。针对不同的安全问题进行扫描和检测，及时发现和处理安全漏洞和威胁，提高组织的安全性，排查更加细致和深入的安全风险指标，提高体检的全面性和深度。
体检计划	• 立即体检：在出现安全问题或有明显安全威胁时进行的体检。这种体检是为了及时了解安全状况、发现安全漏洞或问题，并采取相应的修复措施。立即体检通常是根据安全事件或安全威胁来决定，可以随时进行。 • 定时体检：按照设定时间进行的体检，无论是否有明显安全威胁。这种体检是为了定期监测网络安全状况，早期发现潜在的安全问题，并采取预防措施。定时体检的时间间隔可以根据企业的业务状况、安全需求和安全风险来确定。 • 周期体检：按照一定的周期进行的体检，通常是在特定的时间段或安全生命周期中进行。这种体检是为了全面评估网络安全状况，筛查潜在的安全风险，并采取相应的预防和修复措施。周期体检的时间间隔和内容可以根据不同的安全标准和安全建议来确定。

体检资产	根据实际需求选择。
体检项目	基于端口扫描获取目标系统上开放的端口和服务信息，推断出可能存在的漏洞、弱口令和风险服务暴露内容。例如，如果目标主机开放了 80 端口（HTTP 服务），则可能存在 Web 应用程序漏洞的风险。

编辑任务

1. 登录 云安全中心控制台，在左侧导览中，单击**安全体检**。
2. 在体检任务列表，选择目标任务，单击**编辑**。

> **注意：**
> 不支持编辑立即执行的任务、待开始的非周期任务、正在进行中的周期和定时任务。

3. 在编辑资产体检任务弹窗中，修改相关参数，单击**确定**。

删除任务

1. 登录 云安全中心控制台，在左侧导览中，单击**安全体检**。
2. 在体检任务列表，选择目标任务，单击**删除**。

3. 在确认删除弹窗中，单击**确定**，即可删除该任务。

> **注意：**
> - 删除任务不可恢复，但会保留任务生成的扫描报告。
> - 不支持删除正在进行中的任务。

下载报告

当安全体检任务完成后，云安全中心会自动生成 PDF 格式的安全报告，并提供预览或下载。此外，用户还可以通过关注服务号来随时随地接收报告。

1. 登录 云安全中心控制台，在左侧导览中，单击**报告下载**。
2. 在报告下载页面，选择目标报告，单击操作列的**预览**，可以在线查看报告。

3. 在报告下载页面，支持通过如下两种方式下载报告：
   - 单个：选择目标报告，单击操作列的**下载**。

   - 批量：选择一个或多个报告，单击左上角的**一键下载**。

多账号模式

在多账号模式下，管理员可以指定集团组织下的某个账号为安全体检任务体检消耗配额方，管理员、委派管理员可以为集团组织下任意账号下发安全体检任务，体检配额消耗对象为指定配额方，任务配额占用对象为安全体检任务对应账号。

编辑任务

管理员创建的安全体检任务允许管理员进行编辑操作，委派管理员创建的任务允许管理员、委派管理员进行编辑操作，成员创建的任务允许成员进行编辑操作。由于集团组织下可能存在多个委派管理员，允许进行编辑任务操作的委派管理员应为创建该任务的委派管理员。

删除任务

管理员创建的安全体检任务允许管理员、委派管理员、被创建的成员进行删除操作，委派管理员创建的任务允许管理员、委派管理员、被创建的成员进行删除操作，成员创建的任务允许成员 进行删除操作。由于集团组织下可能存在多个委派管理员，允许进行删除任务操作的委派管理员为所有委派管理员。

添加白名单 IP

最近更新时间：2025-05-30 15:48:51

本文档将为您详细介绍如何将腾讯云安全中心的监测 IP 加入到白名单。

操作场景

云安全中心通过公网进行资产发现和风险监测时会使用模拟黑客入侵攻击的方式。如果您的服务器有安全防护或监控部署（例如 WAF），建议您将腾讯云云安全中心的监测 IP 加入到白名单中，开启扫描访问权限，保证监控服务正常运行，云安全中心扫描节点 IP 如下，共84个 IP。

129.211.162.110
129.211.162.87
129.211.163.253
129.211.164.19
129.211.166.123
129.211.167.182
129.211.167.200
129.211.167.70
129.211.162.158
129.211.162.23
129.211.166.134
129.211.167.108
129.211.167.181
129.211.166.142
129.211.166.163
129.211.167.128
129.211.167.166
43.139.244.231
43.139.243.246
119.28.101.45
119.28.101.51
150.109.12.53
129.226.197.194
129.226.197.196
129.226.197.199
129.226.197.200
129.226.197.201
129.226.197.204
129.226.197.205
129.226.197.207
129.226.197.209
129.226.197.21
43.134.229.58
101.33.220.146
182.254.192.73
175.178.79.94
106.55.172.224
119.91.226.99
43.139.53.159
106.55.100.23
106.53.104.226
123.207.45.218

43.136.98.102
43.139.150.105
175.178.22.156
122.152.222.70
159.75.140.45
193.112.176.100
43.136.103.134
101.33.244.20
114.132.180.83
159.75.80.121
43.136.56.35
106.52.219.11
42.193.249.24
43.136.123.68
123.207.72.172
43.139.233.146
119.91.227.203
175.178.108.10
43.136.85.179
111.230.104.109
119.91.226.24
119.91.48.196
101.33.203.139
134.175.222.22
175.178.72.188
175.178.90.4
119.29.244.62
123.207.72.179
175.178.79.108
111.230.243.60
43.138.175.184
134.175.53.125
43.139.204.202
122.152.233.202
175.178.176.234
43.139.244.105
43.139.188.254
159.75.154.2
106.52.244.65
43.138.233.4
159.75.110.155
134.175.248.145

若您的网站需登录才可以访问，则需要先解除安全策略（即确保所有 IP 都能访问），待您的 cookie 有效性验证通过后再恢复限制。

操作步骤

说明

- 适用于腾讯云 Web 应用防火墙，如果您使用的是其他 WAF 产品，请自行添加。
- 已购买 Web 应用防火墙 。
- 完成防护域名的添加及正常接入，当前域名处于正常防护，且开启 BOT 管理规则总开关，详情请参见 快速入门 。

方式1：通过 IP 查询添加白名单

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击 **IP 查询**。
2. 在 IP 查询页面，左上角选择需要防护的域名，输入需要查询的 IP，单击**查询**。

3. 在查询结果中，可查看具体的 IP 详情，单击**加入黑白名单**，可手动添加黑白名单。

4. 在添加黑白 IP 页面，可手动添加白名单。配置相关参数，单击**添加**，即完成白名单添加。

参数说明：

- **类别：选择白名单。**
- **IP 地址：填写需要添加到白名单的地址。**

- 截止时间：填写白名单有效期的截止时间。
- 备注：自定义描述。

方式2：直接添加 IP 白名单

登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心** > **黑白名单**，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。

手动添加白名单

1. 在 IP 白名单页面，单击**添加地址**，进入添加白名单页面。

2. 在添加白名单页面，配置相关参数，单击**确定**。

字段说明

- **IP 地址：**支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或 FF05:B5::/60，使用换行符进行分隔，一次最多添加100个。

  > **说明**
  > - 选择域名为 ALL 时，添加的 IP 地址或 IP 段为全局的白名单。
  > - 各个版本每个域名规格限制为：高级版1000条/域名、企业版5000条/域名、旗舰版:20000条/域名，每个 IP 地址或者 IP 段占用一条额度。

- **截止时间：**永久生效或限定日期。
- **备注：**自定义，50个字符以内。

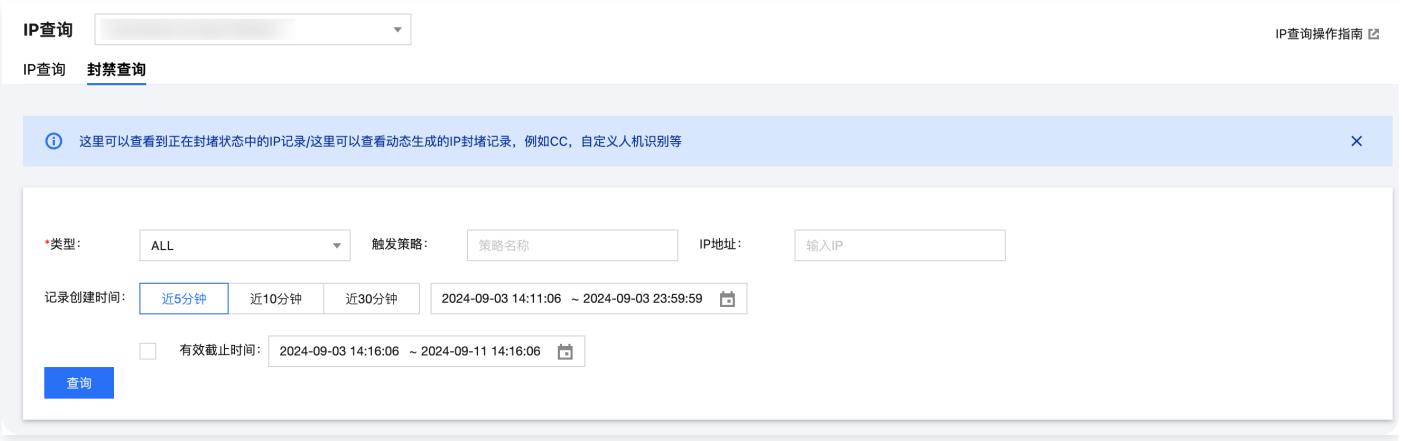
批量导入白名单

1. 在 IP 白名单页面，单击**导入数据**，将弹出“导入 IP 名单”窗口。

2. 在“导入 IP 名单”窗口中，单击**导入**，选择导入白名单文件，上传完成后，单击**确认导入**即可。

方式3：将已封堵 IP 添加白名单

1. 登录 Web 应用防火墙控制台，在左侧导航中，选择 **IP 查询** > **封禁查询**，进入 封禁查询。
2. 在 封禁查询页面，输入相关信息，单击**查询**，可以查询云安全中心的相关 IP 信息，即可对已封堵 IP 进行加白操作。



评分详情

最近更新时间：2024-09-05 10:12:51

云安全中心将结合各类安全场景下的监控数据，对用户的腾讯云风险情况做出整体评价，并助力提升云上安全水位。
评价方法采用100分制，最高分100分。如果用户存在相关的安全风险，可以按照对应得分途径从当前体检分数提升至 100 分。具体风险点与得分途径如下：

评分维度	风险点	得分途径	得分分值	得分上限
安全防线建设	云防火墙	云防火墙普惠版、高级版、企业版、旗舰版防护中或试用中	0道防线未开通：+10分；1 道防线未开通：+8 分；2 道防线未开通：+4 分；3 道防线未开通：+0 分。	10
	Web 应用防火墙	Web 应用防火墙高级版、企业版、旗舰版、独享版防护中或试用中		
	主机安全	主机安全专业版、旗舰版防护中或试用中		
业务资产梳理	公网 IP 资产	公网 IP 已开启互联网边界防火墙的防护	+（1 – 未防护核心资产数量 / 全部资产数量）*10分;若资产数为0，则+10分。	30
	域名资产	域名资产已接入 SaaS 型 Web 应用防火墙实例或负载均衡型 Web 应用防火墙实例	+（1 – 未防护核心资产数量 / 全部资产数量）*10分; 若资产数为0，则+10分。	
	主机资产	主机资产已授权开通了主机安全专业版或旗舰版。	+（1 – 未防护核心资产数量 / 全部资产数量）*10分; 若资产数为0，则+10分。	
资产风险发现	端口风险	及时处理云上业务潜在的端口风险	+（1 – 有高危风险的资产数量 / 全部资产数量）*10分;若资产数为0，则+10分。	30
	漏洞风险	及时处理云上业务潜在的漏洞风险	+（1 – 有高危风险的资产数量 / 全部资产数量）*10分;若资产数为0，则+10分。	
	弱口令风险	及时处理云上业务潜在的弱口令风险	+（1 – 有高危风险的资产数量 / 全部资产数量）*10分;若资产数为0，则+10分。	
高危告警处置	高危告警	及时处置云上业务的高危告警	+（1 – 有高危告警的资产 / 全部资产）*30	30

说明

- 每个风险点均设计有最高得分上限。
- 评分解读：
  - 评分低于 60 分时，安全性较差，系统将按照红色呈现安全评分。
  - 评分大于等于 60 分，小于 80 分时，风险较为可控，系统将按照黄色呈现安全评分。
  - 评分大于等于 80 分，小于 95 分时，风险可控，系统将按照蓝色呈现安全评分。
  - 评分大于等于 95 分时，安全性较高，系统将按绿色呈现安全评分。

热点问题

最近更新时间：2024-08-28 09:25:01

如何选购体检配额?

为降低资产安全风险，建议每月进行4次自动检测和1次手动全面检测，请根据您的云上资产数量计算购买的资产体检数。

计算消耗体检配额公式

一次安全体检中，选定1个域名、1个 IP 资产分别消耗1个体检配额，共计2个体检配额；若选定云资源配置风险体检项目时，消耗的体检配额为已勾选的云资源数。

安全体检是否会影响业务运行?

不会，安全体检模拟真实用户的访问，同时有精准的速率控制，不会影响业务的正常运转。

安全体检能支持多少企业 IT 资产的扫描?

安全体检依托腾讯云的计算能力，能够做到快速扩容，支持对千万级 IT 资产的扫描。

体检时间过长是否有异常?

安全体检任务如涉及检测 Web 网站，需要根据您的授权利用爬取技术对您指定的 URL进行内容识别分析，并且执行体检过快容易给业务带来影响，因此体检时间较慢为正常现象。

体检任务被中止后是否还有报告生成?

若安全体检任务被中止则不生成报告，但风险中心中存在已被检测出的风险，可以根据报告 ID 查询到已发现的风险。

体检任务异常是否会消耗体检、占用任务配额?

若安全体检任务无法执行，则占用任务配额但不消耗体检配额；若安全体检任务开始执行，则执行时立即消耗体检配额并占用任务配额。

安全体检有哪些扫描 IP?

安全体检通过公网模拟黑客入侵（无害的攻击）的方式进行安全扫描。如果您的服务器有相关防护措施或者限制了访问的 IP，为保证扫描的正常进行，建议您将以下 IP 地址加到白名单。
安全扫描节点 IP 为：
129.211.162.110
129.211.162.87
129.211.163.253
129.211.164.19
129.211.166.123
129.211.167.182
129.211.167.200
129.211.167.70
129.211.162.158
129.211.162.23
129.211.166.134
129.211.167.108
129.211.167.181
129.211.166.142
129.211.166.163
129.211.167.128
129.211.167.166
43.139.244.231

43.139.243.246

除了主机和容器之外，配置风险检测还包括哪些云资源的配置检测项?

检查项名称	检查类型	检查对象	风险等级	所属规范	配置风险说明
TDSQL MySQL 版不应该开放公网访问	数据安全	tdmysql	中危	默认安全规范	数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高；本检查项会检查TDSQL MySQL 版，如果启用了公网访问，则不满足要求。
网络 ACL 不应存在全部放通的入站规则	网络访问控制	subnet	高危	默认安全规范	网络 ACL 是子网粒度的访问控制攻击，如使用全部放通的入站规则，即：入站方向源为0.0.0.0/0，动作为允许的规则，则可能导致该子网开放范围过大，资产产生非必要暴露，本检查项会检查网络 ACL 服务入站规则，如存在来源地址为0.0.0.0/0，端口为所有，动作为允许的规则，则不满足要求。
网络 ACL 不建议存在非业务端口全部放通的入站规则	网络访问控制	subnet	高危	默认安全规范	网络 ACL 是子网粒度的访问控制攻击，如使用非业务外（默认：80,443）全部放通的入站规则，即：入站方向源为0.0.0.0/0，端口为80/443以外的端口，动作为允许的规则，则可能导致该子网开放范围过大，资产产生非必要暴露；本检查项会检查网络 ACL 服务入站规则，不应该存在来源地址为0.0.0.0/0，端口为所有或者为非业务端口（默认：80,443），动作为允许的规则。
SSL 证书应在有效期内	数据安全	ssl	中危	默认安全规范	检查 SSL 证书是否超出有效期，证书到期前需及时续费或更换新证书，否则您将无法继续使用 SSL 证书服务，导致数据安全风险，目前检查范围为全部 SSL 证书，您需要根据证书是否关联资源、域名是否还需使用判断是否应修复或删除不再使用的证书。
镜像仓库权限应合理设置	数据安全	repository	中危	默认安全规范，网络安全等级保护三级技术要求	仓库分为公有仓库和私有仓库。 公有仓库可以允许所有互联网中用户进行访问和下载镜像。 如果镜像内部有敏感信息，建议配置成私有仓库，防止信息的泄漏。
云数据库 Redis 应该禁用高危命令	数据安全	redis	中危	默认安全规范	数据库往往安全保护级别较高，若未禁用高危命令（默认：flushall、flushdb、keys、hgetall、eval、evalsha、script），容易出现应用阻塞，数据误删等风险；本检查项会检查 Redis 实例禁用命令配置，若高危命令未禁用（默认包括：flushall、flushdb、keys、hgetall、eval、evalsha、script），则不符合要求。
Nosql 数据库-Redis 应该开启自动备份	数据安全	redis	中危	默认安全规范，网络安全等级保护	判定 Redis 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。

				三级技术要求	
Nosql 数据库-Redis 不应该对全部网段开放	网络访问控制	redis	高危	默认安全规范，网络安全等级保护三级技术要求	判定 Redis 数据库的服务端口是否对全IP开放访问，正常情况下，数据库服务端口应该只针对可信 IP 或范围开放。
Nosql-Redis 应该位于中国大陆 region	基础设施位置	redis	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
云数据库 PostgreSQL 数据库不建议对公网开放访问	网络访问控制	postgres	高危	默认安全规范	数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。
关系型数据库-PostgreSQL 应该启用备份	数据安全	postgres	中危	默认安全规范，网络安全等级保护三级技术要求	判定 PostgreSQL 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。
关系型数据库-PostgreSQL 数据库应该位于中国大陆 region	基础设施位置	postgres	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
Nosql-MongoDB 应该位于中国大陆 region	基础设施位置	mongodb	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
云数据库 MariaDB 应该限制高危命令使用	数据安全	mariadb	中危	默认安全规范	数据库往往安全保护级别较高，若所有账号都拥有全局命令权限 drop、delete，容易出现数据误删除或恶意删除风险，本检查项会检查MariaDB，如果所有用户都未禁止 drop、delete命令，则不满足要求。
云数据库 MariaDB 数据库不建议对公网开放访问	网络访问控制	mariadb	高危	默认安全规范	数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。
云数据库 MariaDB 不应对全部网段开启访问	网络访问控制	mariadb	高危	默认安全规范	云数据库如果对全部网段开启访问，则增大了该数据库的攻击面，增加了数据库被攻击、数据泄露的风险。
关系型数据库-MariaDB 应该启用备份	数据安全	mariadb	中危	默认安全规范，网络安全等级保护三级技术要求	判定 MariaDB 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。
关系型数据库-MariaDB数据库应该位于中国大陆 region	基础设施位置	mariadb	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
Elasticsearch 集群不应该开放公网访问	数据安全	es	高危	默认安全规范	Elasticsearch 集群往往存储数据，如开放公网访问，则可能导致不必要的攻击面

					暴露，产生数据完整性、机密性、可用性风险。
Elasticsearch 集群的 Kibana 组件不应该开放公网访问	数据安全	es	高危	默认安全规范	Elasticsearch 集群往往存储数据，可以通过 Kibana 组件进行数据访问与命令控制，如开放公网访问，则可能导致不必要的攻击面暴露，产生数据完整性、机密性、可用性风险。
安全组不应放通全部网段任何端口	网络访问控制	cvm	高危	默认安全规范，网络安全等级保护三级技术要求	安全组是一种虚拟防火墙，建议根据最小粒度原则，配置防火墙策略。添加服务端口的可信 IP 白名单访问。
CVM 应该位于中国大陆 region	基础设施位置	cvm	中危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
CVM 应使用密钥对登录	身份认证及权限	cvm	中危	默认安全规范	检查 CVM 是否利用 SSH 密钥进行登录，相对于传统的密码登录，SSH 密钥登录方式更为方便，且安全性更高。（仅检查 Linux 系统机器）
CVM 上的主机安全代理应正常运行	基础安全防护	cvm	高危	默认安全规范，网络安全等级保护三级技术要求	腾讯云主机安全提供木马查杀、密码破解拦截、登录行为审计、漏洞管理、资产组件识别等多种安全功能。未安装主机安全客户端会面临网络安全，数据泄露的风险。
COS 存储桶建议开启存储桶复制	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	跨地域复制是针对存储桶的一项配置，通过配置跨地域复制规则，可以在不同存储区域的存储桶中自动、异步地复制增量对象。启用跨地域复制后，COS 将精确复制源存储桶中的对象内容（如对象元数据和版本 ID 等）到目标存储桶中，复制的对象副本拥有完全一致的属性信息。此外，源存储桶中对于对象的操作，如添加对象、删除对象等操作，也将被复制到目标存储桶中。建议进行跨区域复制以提升您的数据容灾能力。
COS 存储桶应配置合理的桶策略	数据安全	cos	高危	默认安全规范，网络安全等级保护三级技术要求	存储桶策略是指在存储桶中配置的访问策略，允许指定用户对存储桶及桶内的资源进行指定的操作。应依据“最小化权限”原则来配置，不推荐对任意用户开放读取操作权限，有遍历文件名或文件被下载的风险。
COS 存储桶应该位于中国大陆 region	基础设施位置	cos	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
COS 存储桶应开启防盗链功能	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	为了避免恶意程序使用资源 URL 盗刷公网流量或使用恶意手法盗用资源，给您带来不必要的损失。建议您通过控制台的防盗链设置配置黑/白名单，对存储对象进行安全防护。

COS 存储桶应开启服务端加密	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	存储桶支持在对象级别上应用数据加密的保护策略，并在访问数据时自动解密。加密和解密这一操作过程都是在服务端完成，这种服务端加密功能可以有效保护静态数据。建议您对敏感数据类型开启此项配置。
COS 存储桶应开启日志记录	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	日志管理功能能够记录对于指定源存储桶的详细访问信息，并将这些信息以日志文件的形式保存在指定的存储桶中，以实现对存储桶更好的管理。日志管理功能要求源存储桶与目标存储桶必须在同一地域，目前支持北京、上海、广州、成都地域。如果所在区域支持日志管理功能，建议开启此项功能。
COS 存储桶 ACL 公共权限不应该设置为公共读写	数据安全	cos	高危	默认安全规范，网络安全等级保护三级技术要求	存储桶的公有读和公有写权限可以通过匿名身份直接读取和写入存储桶中的数据，存在一定的安全风险。为确保您的数据安全，不推荐将存储桶权限设置为公有读写或公有读私有写，建议您选择私有读写权限。
CLB 绑定的证书应该在有效期内	监控告警	clb	中危	默认安全规范	检查同 CLB 绑定的证书是否过期，如果过期则需要进行替换，以免影响业务正常使用。
CLB 后端服务器组的健康检查状态应保持正常	监控告警	clb	低危	默认安全规范	检测负载均衡 CLB 服务的健康状态，用以判定 CLB 的后端服务是否异常。
CLB 不应转发高危端口	网络访问控制	clb	高危	默认安全规范，网络安全等级保护三级技术要求	应依据“最小服务”原则来设定 CLB 转发策略，只对必要的公共服务端口（如：80、443等）做转发，其他端口不应该进行转发。
CLB 不应对全部网段开启非业务端口访问	网络访问控制	clb	高危	默认安全规范，网络安全等级保护三级技术要求	检查 CLB 负载均衡实例访问控制配置，对非业务端口开放0.0.0.0/0存在潜在的安全风险，建议对非 http/https 服务启用访问控制。
云数据库 MySQL 应该开启数据库审计	数据安全	cdb	中危	默认安全规范	数据库往往存储重要性较高数据，若不开启数据库审计，如发生误操作、恶意操作等问题，难以回溯，发现源头，本检查项会检查 MySQL 数据库是否开启了数据库审计，如果没有开启，则不符合要求。
云数据库 MySQL 网络类型应使用私有网络	数据安全	cdb	中危	默认安全规范	私有网络可基于租户需求，进行不同网络间隔离，数据库往往存储重要性较高的数据，如使用非私有网络，需要维护较为精确的访问控制规则，如果漏维护、错维护，则可能会导致您的数据库产生不必要的暴露，本检查项会检查 MySQL 数据库类型，如果为私有网络，则满足要求，否则不满足。

云数据库 MySQL 数据库应该为管理员账户设置密码	网络访问控制	cdb	高危	默认安全规范	云数据库 MySQL 是数据库服务，如您未对数据库管理员配置账号密码，则该数据库可能被恶意登录，导致数据泄露。
云数据库 MySQL 数据库应该创建非 root 用户使用	数据安全	cdb	中危	默认安全规范	数据库往往存储重要性较高数据，而数据库若只存在 root 账号，没有其他应用账号，说明权限过大，存在误操作或恶意操作影响数据安全的风险，本检查项会检查 MySQL 已经完成初始化的主实例数据库用户列表，如果除了 root 用户以及腾讯云默认创建的 mysql.*以外没有其他用户，则不符合要求。
云数据库 MySQL 数据库实例应在不同可用区进行部署	数据安全	cdb	低危	默认安全规范	云数据库 MySQL 提供多种高可用的架构，选择主备可用区不同时（即多可用区部署），可保护数据库以防发生故障或可用区中断，本检查项会检查 MySQL 数据库，同一个数据库主备实例如果在同一个区域同一个可用区内，则不满足要求。
云数据库 MySQL 数据库审计保留时间应满足要求	数据安全	cdb	中危	默认安全规范	数据库往往存储重要性较高数据，基于合规要求，数据库审计日志至少应保留6个月及以上，本检查项会检查 MySQL 数据库审计保留时间，如果保留时间小于审计时间（默认180天），则不符合要求。
云数据库 MySQL 数据库建议限制非 root 用户高危命令权限	数据安全	cdb	中危	默认安全规范	数据库非 root 账号应该进行权限控制，若应用账号拥有高危命令权限，如 drop、delete 等，容易出现数据误删除或恶意删除风险，本检查项会检查Mysql 数据库（检查主实例，不检查只读实例和灾备实例），检查 root 用户以外用户的配置，如果配置中允许执行命令：drop，delete，则不满足，对于不存在非 root 用户的实例，本检查项满足，采用其他检查项进行合规检查。
云数据库 MySQL 数据库不建议对公网开放访问	网络访问控制	cdb	高危	默认安全规范	云数据库 MySQL 是数据库服务，数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。
关系型数据库-MySQL 应该启用备份	数据安全	cdb	中危	默认安全规范，网络安全等级保护三级技术要求	判定 MySQL 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。
关系型数据库-MySQL 数据库应该位于中国大陆 region	基础设施位置	cdb	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
关系型数据库-MySQL 不应该对全部网段开放	网络访问控制	cdb	中危	默认安全规范，网络安全等级保护三级技术要求	判定 MySQL 数据库的服务端口是否对全 IP 开放访问，正常情况下，数据库服务端口应该只针对可信 IP 或范围开放。
CBS 数据盘应该设置为加密盘	数据安全	cbs	中危	默认安全规范，网络安全等级保护	检查云硬盘的数据盘是否为加密盘。加密盘不仅可以提供更好的数据保密性，同时

				三级技术要求	也可以满足安全合规等要求。（仅支持检查非系统盘）
CBS 应开启定期快照功能	数据安全	cbs	中危	默认安全规范，网络安全等级保护三级技术要求	检查云硬盘是否开启了自动定期快照的功能。定期创建快照，可以提高数据的安全性，实现业务的低成本和高容灾。
子账号应使用 MFA 进行登录保护	基础安全防护	cam	中危	默认安全规范	子账号未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险，本检查项会检查子账号，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
子账号应使用 MFA 进行操作保护	基础安全防护	cam	中危	默认安全规范	子账号未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险，本检查项会检查子账号，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
子账号密码应定期更换	基础安全防护	cam	中危	默认安全规范	子账号密码是用户访问的主要凭据，长期(90天)不更换密码，会导致密码泄露的可能性增加。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应删除废弃的子账号	基础安全防护	cam	高危	默认安全规范	子账号长期(30天)不登录使用，可能该账户已经被废弃，废弃账户可能被不再属于您组织的成员使用，导致您的资产不可用或数据泄露。
应该删除子账号废弃的 API 密钥	基础安全防护	cam	高危	默认安全规范	子账号 API 密钥长期(30天)不使用，可能该 API密钥已经被废弃，废弃 API 密钥可能被不再属于您组织的成员使用，导致您的资产不可用或数据泄露。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应该删除废弃的协作者 API 密钥	基础安全防护	cam	高危	默认安全规范	协作者的 API 密钥长期(30天)不使用，可能该 API 密钥已经被废弃，废弃 API 密钥可能被不再属于您组织的成员使用，导致您的资产不可用或数据泄露。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应该定期更换子账号的 API 密钥	基础安全防护	cam	中危	默认安全规范	子账号 API 密钥是编程访问的主要凭据，长期(90天)不更换密钥，会导致密钥泄露的可能性增加。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应定期更换协作者的 API 密钥	基础安全防护	cam	中危	默认安全规范	协作者 API 密钥是编程访问的主要凭据，长期(90天)不更换密钥，会导致密钥泄露的可能性增加。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
协作者应使用 MFA 进行登录保护	基础安全防护	cam	中危	默认安全规范	协作者未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险；本检查项会检查协作者，

					是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
协作者应使用 MFA 进行操作保护	基础安全防护	cam	中危	默认安全规范	协作者未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险；本检查项会检查协作者，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
协作者应开启登录保护	基础安全防护	cam	中危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，如协作者账号泄露，可能会导致该协作者有权限的资产被破坏或者数据泄露，开启登录保护后，对协作者登录进行二次校验，降低协作者账号泄露导致的风险。
协作者应开启操作保护	基础安全防护	cam	中危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，如协作者账号泄露，可能会导致该协作者有权限的资产被破坏或者数据泄露，开启操作保护后，对协作者敏感操作进行二次校验，降低协作者账号泄露导致的风险。
协作者不应该同时使用编程访问与用户界面访问	基础安全防护	cam	高危	默认安全规范	协作者账号具备两种访问方式，如同时开启，则可能导致一个账号的暴露面增加，且可能导致机器账号与人工账号混用，增加账号被恶意使用的可能性。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
具备高风险权限的协作者应开启登录保护	基础安全防护	cam	高危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，且高权限协作者具有超级管理员权限，如协作者账号泄露，您的云上资产会面临非常高的安全风险，开启登录保护后，对协作者登录进行二次校验，降低协作者账号泄露导致的风险。
具备高风险权限的协作者应开启操作保护	基础安全防护	cam	高危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，且高权限协作者具有超级管理员权限，如协作者账号泄露，您的云上资产会面临非常高的安全风险，开启操作保护后，对协作者敏感操作进行二次校验，降低协作者账号泄露导致的风险。
建议子账号的 API 密钥不超过1个	基础安全防护	cam	低危	默认安全规范	一个子账号维护多个 API 密钥，会增大密钥的暴露面，增加密钥泄露的风险。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
高风险权限子账号应该开启登录保护	基础安全防护	cam	高危	默认安全规范	高权限子账号具备超级管理员权限，如果高风险子账号被恶意登录，您云上的资产会面临非常高的风险，登录保护为您的子账号提供账号登录的二次校验，降低高风险子账号被恶意登录的可能性。
高风险权限子账号应该开启操作保护	基础安全防护	cam	中危	默认安全规范	高权限子账号具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，操作保护为您的

					敏感操作提供二次校验，降低误操作或恶意操作的风险。
高风险权限子账号不建议启用 API 密钥	基础安全防护	cam	低危	默认安全规范	高权限子账号具有超级管理员的权限，而 API 密钥是账号编程访问的身份凭证，通常会被写入配置中，易泄露，如果 API 密钥泄露，攻击者可利用该密钥操控您在云上的所有资产，风险较高。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
不能同时为子账号开启编程访问与用户界面访问	基础安全防护	cam	中危	默认安全规范	子账号具备两种访问方式，如同时开启，则可能导致一个账号的暴露面增加，且可能导致机器账号与人工账号混用，增加账号被恶意使用的可能性。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
主账号应使用 MFA 进行登录保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，如果主账号被盗用，您的云资产会面临非常高的安全风险，MFA（Multi-Factor Authentication）即多因子认证，是一种简单有效的安全认证方法，它可以在用户名和密码之外，再增加一层保护，登录保护可使用腾讯云虚拟 MFA 设备，降低主账号被恶意登录的可能性。
主账号应使用 MFA 进行操作保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，MFA（Multi-Factor Authentication）即多因子认证，是一种简单有效的安全认证方法，它可以在用户名和密码之外，再增加一层保护，操作保护中启用虚拟 MFA，可为您的敏感操作提供二次校验，降低误操作或恶意操作的风险。
主账号应开启登录保护	基础安全防护	account	高危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，如果主账号被盗用，您的云资产会面临非常高的安全风险，登录保护为您的账号登录提供二次校验，降低主账号被恶意登录的可能性。
主账号应开启操作保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，操作保护为您的敏感操作提供二次校验，降低误操作或恶意操作的风险。
主账号建议开启异地登录保护	基础安全防护	account	低危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，如果主账号被盗用，您的云资产会面临非常高的安全风险，异地登录保护为您的账号登录提供登录地校验，如发现异地登录，则会进行二次校验，降低主账号被恶意登录的可能性。

主账号不应该启用 API 密钥	基础安全防护	account	高危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，而 API 密钥是账号编程访问的身份凭证，通常会被写入配置中，易泄露，如果API 密钥泄露，攻击者可利用该密钥操控您在云上的所有资产，风险较高。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。

云边界分析
功能简介

最近更新时间：2025-06-24 11:29:42

云安全中心将展示您云租户互联网边界的整体状态，帮助您进行日常的边界管理。该功能包含了**互联网边界**与**扫描结果**，数据来源于**边界梳理**与**安全体检**。

- **互联网边界**：通过分析云上资产关联关系（如 CLB/CDN 绑定关系等），绘制资产面向互联网暴露的路径，同时结合资产状态、安全组策略，得到资产面向互联网的开放状态，即互联网边界。
- **扫描结果**：通过安全体检对您的公网资产进行扫描，获取开放的端口服务、Web 服务，并检查存在的高危端口、风险页面、漏洞、弱口令等风险。

前提条件

已购买 云安全中心旗舰版 。

边界开放状态

云安全中心，将根据资产的属性、关联关系、访问控制状态等梳理互联网边界。根据网络状态分为：

网络状态	详情
完全开放	互联网所有地址均可访问该端口。
受限访问	云资源设置了访问控制，仅白名单里地址可访问该端口。
无法访问	云资源状态异常或关机，因此无法被访问。

示例：您的负载均衡资产（IP：1.1.1.1）创建了80端口的监听器，监听器的后端服务是两台云服务器。以下不同情况对应不同的开放状态：

- 负载均衡的安全组开放了允许0.0.0.0/0访问80端口，两台云服务器均处于正常运行状态。

IP	端口	开放状态
1.1.1.1	80	完全开放

- 负载均衡的安全组开放了允许2.2.2.0/24访问80端口，两台云服务器均处于正常运行状态。

IP	端口	开放状态
1.1.1.1	80	受限访问（白名单：2.2.2.0/24）

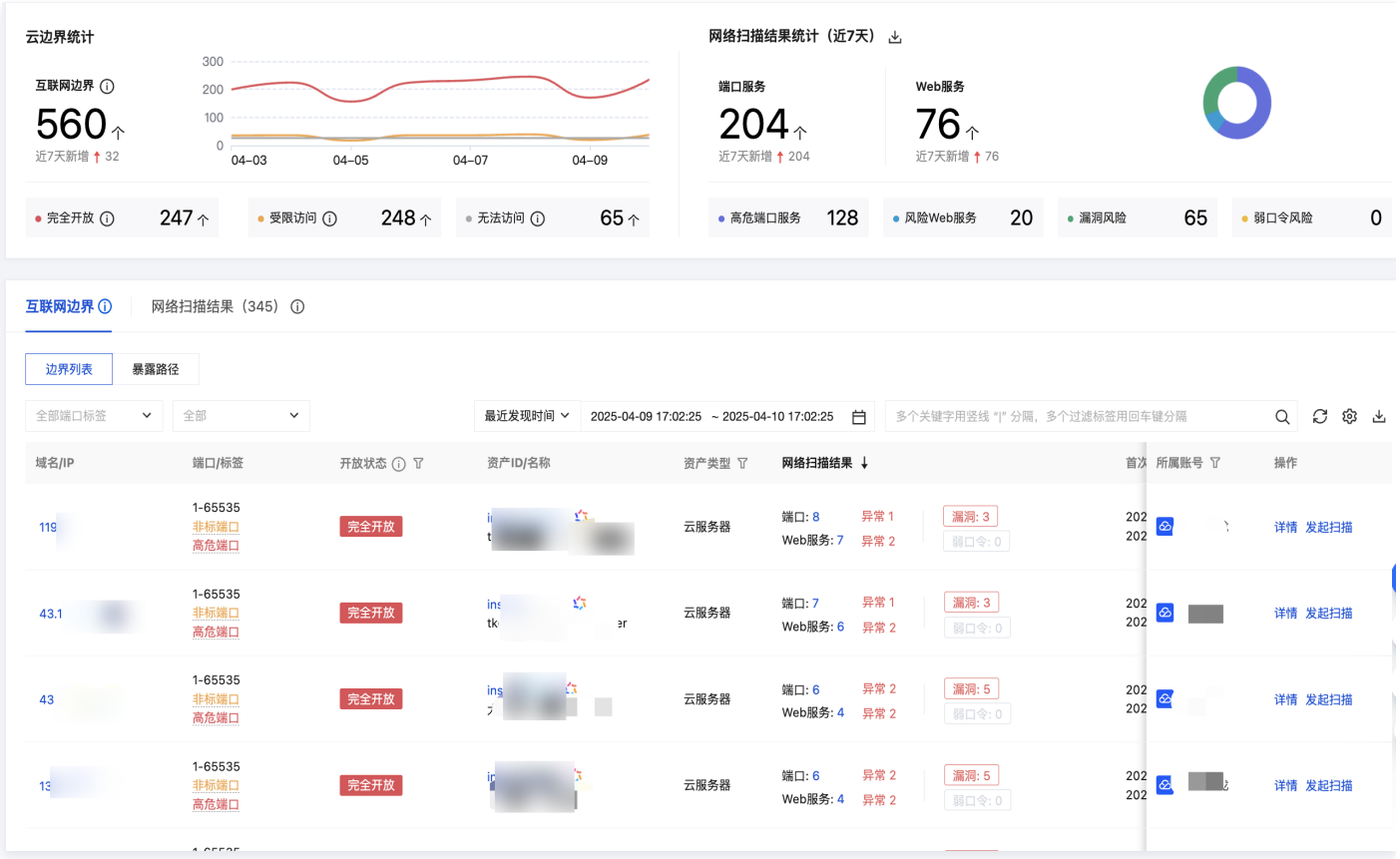
- 负载均衡的安全组开放了允许0.0.0.0/0访问80端口，两台云服务器均处于关机状态。

IP	端口	开放状态
1.1.1.1	80	无法访问

> **说明：**
> 实际上，决定开放状态的因素还包括负载均衡状态、监听器状态、以及云服务器安全组是否允许负载均衡的访问。这些可能的影响因素都被视为判断开放状态的条件。

查看数据

1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 在云边界分析页面，支持查看统计面板、数据详情，其中统计面板包含**云边界统计**和**扫描结果统计**。



数据详情的数据内容如下表：

主标题	二级标题	功能简介
互联网边界	边界列表	展示互联网边界数据台账，每个边界端口（或端口范围）关联扫描结果，以便您查询面向互联网的资源的状况。
	暴露路径	根据输入的资产信息以**树状图**的形式该资产所有面向互联网暴露的路径，展示网络链路前后关联关系。
扫描结果	端口服务	展示扫描发现的互联网端口及服务信息。
	Web服务	展示扫描发现的 Web 服务及组件信息。
	漏洞风险	展示扫描发现的漏洞。
	弱口令风险	展示扫描发现的弱口令。

3. 在云边界分析页面，单击**边界梳理**，即可触发边界的梳理任务。

安全体检

对互联网地址进行扫描，并将结果与互联网边界的资产进行关联。涉及的体检项目：端口风险、风险服务暴露、漏洞风险、弱口令风险。

1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 在云边界分析页面，单击**安全体检**，弹出对话框进行扫描。若需要了解安全体检的详细内容，可访问 文档 。

3. 需要使用到的体检项目：端口风险、风险服务暴露、漏洞风险、弱口令风险。页面默认勾选了这四个选项。请阅读体检许可协议后，勾选两个确认框后，单击**确定**即可发起体检。

支持的云产品实例类型

目前，云边界分析已支持以下云产品，产品分类及名称参考云厂商官网文档。

云厂商	产品分类	产品名称
腾讯云	计算	云服务器
		轻量应用服务器
	网络	负载均衡
		弹性公网 IP
		弹性网卡
		NAT 网关
	CDN 与边缘	内容分发网络 CDN

	安全	Web 应用防火墙
	数据库	云数据库 MySQL
		云数据库 MariaDB
		云数据库 SQL Server
		云数据库 MongoDB
		云数据库 PostgreSQL
		云数据库Redis
	存储	对象存储
	大数据	Elasticsearch Service
阿里云	计算	云服务器 ECS
	网络与 CDN	负载均衡 SLB
		内容分发网络CDN
		弹性公网IP
		弹性网卡 ENI
		NAT 网关
		任播弹性公网IP
	大数据计算	检索分析服务 Elasticsearch 版
	Serverless	函数计算
	数据库	云数据库 RDS
		云数据库 MongoDB 版
		云数据库 Tair（兼容 Redis）
	存储	对象存储 OSS
	安全	Web 应用防火墙

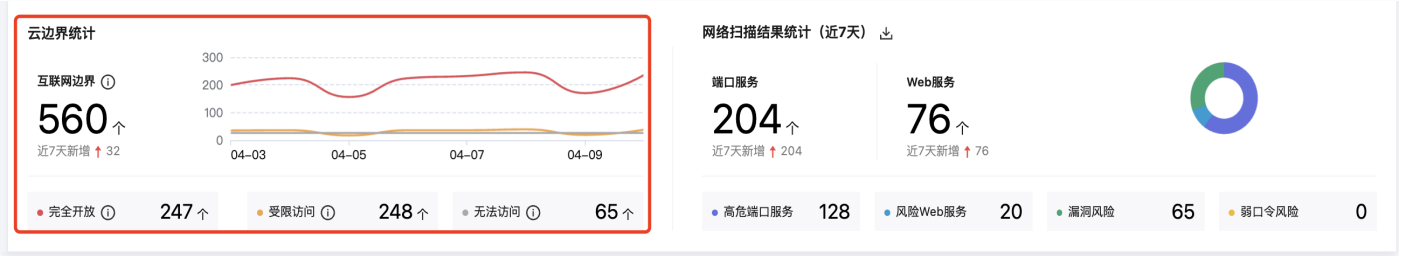
查看统计面板

最近更新时间：2025-04-11 17:39:02

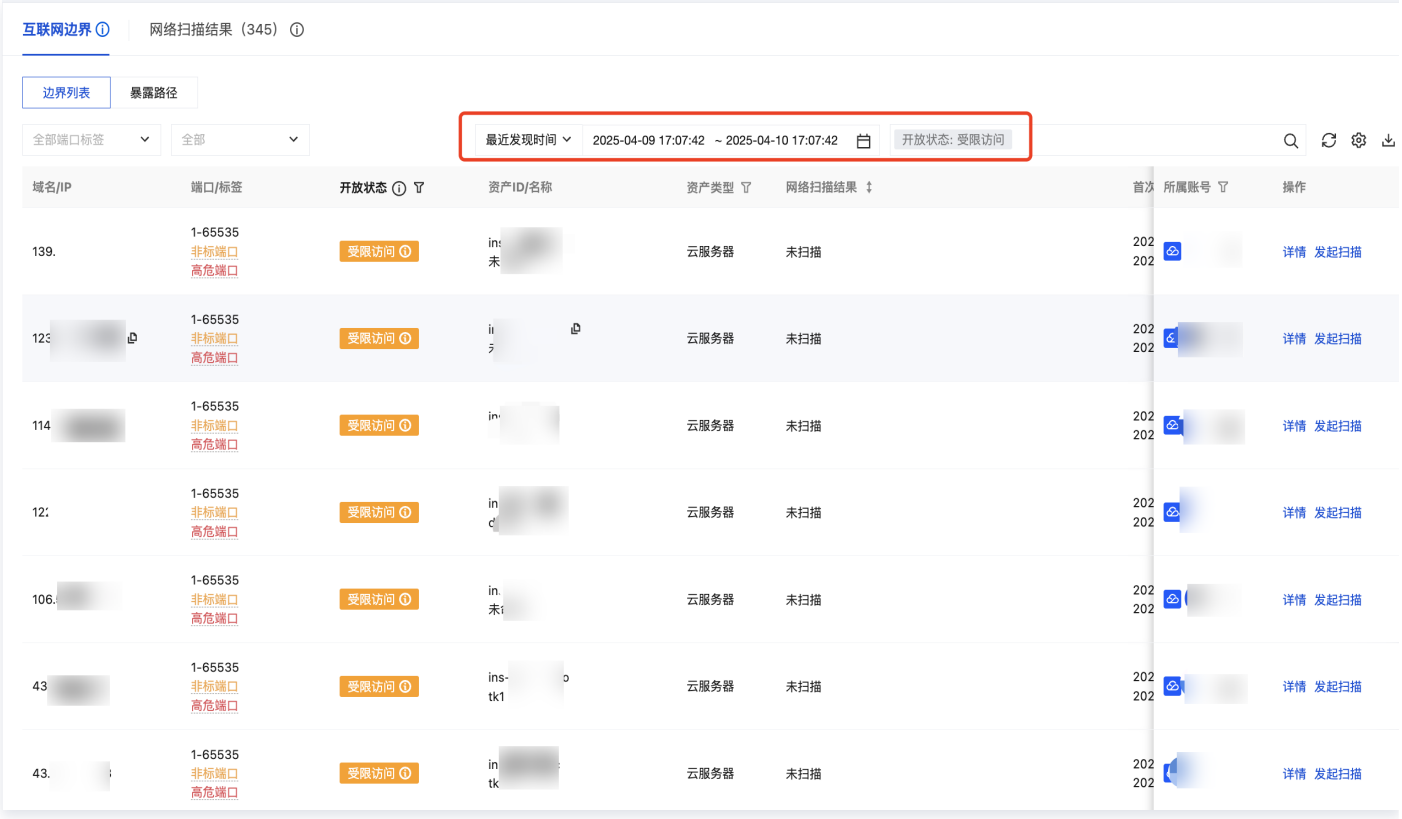
暴露统计

1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 统计面板左侧即**云边界统计**。云边界统计的数据取自最近识别时间在24小时内的互联网端口。云安全中心根据云资源的策略及状态将互联网端口的开放状态分为以下三类：

开放状态	状态说明
完全开放	互联网所有地址均可访问该端口。
受限访问	云资源设置了访问控制，仅白名单里地址可访问该端口。
无法访问	云资源状态异常或关机，因此无法被访问。



3. **功能交互**：单击4个统计数据，将在下方**互联网边界-边界列表**内，展示具体的结果。下图是点击**云边界统计**面板中“**受限访问**”对应数字的展示结果。



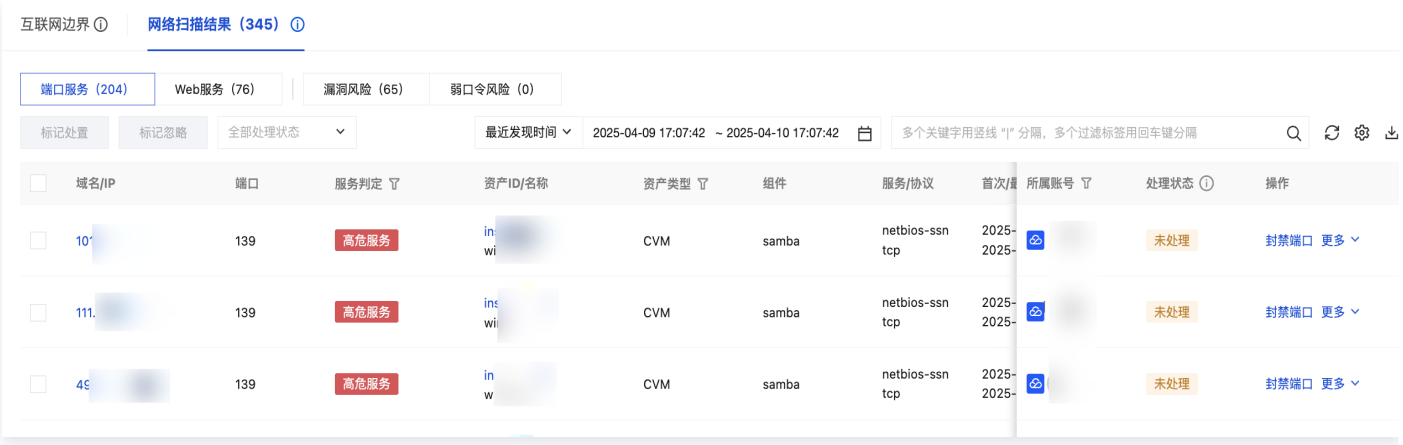
4. **云边界数量趋势图**：展示了近7天边界数量的整体趋势。

扫描结果统计

1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 统计面板右侧即**扫描结果统计**。扫描结果取自安全体检中近7天网络扫描的结果，涉及的体检项为端口风险、风险服务暴露、漏洞风险、弱口令风险。数据统计的性质说明如下表：

统计内容	内容说明
端口服务	通过扫描发现的端口服务。
Web 服务	通过扫描发现的Web服务。
高危端口服务	扫描识别为高危服务的端口服务，如：mysql、redis 等。
风险 Web 服务	扫描识别为高危的 Web 服务，如：Jenkins、phpmyadmin 等。
漏洞风险	扫描发现的漏洞。
弱口令	扫描发现的弱口令，如：ssh 弱口令、Web 后台弱口令。

3. **功能交互**：单击**扫描结果统计面板中的统计数字**，将在下方**扫描结果**的对应 Tab 页面，展示具体的结果。下图是单击“**高危端口服务**”对应数字的展示结果。



4. **功能交互**：单击该导出按钮，可以下载全部扫描结果。

5. 通过调整体检任务，可以查看不通体检任务的结果。综合体检结果即根据所有体检任务的结果进行汇总。体检任务的切换只影响扫描结果，不影响互联网边界的结果。

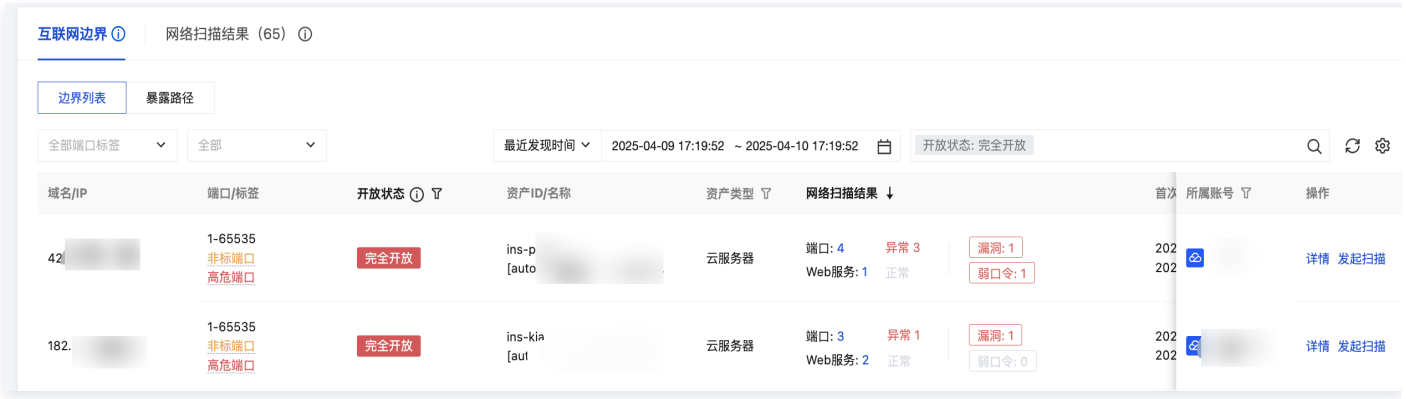

边界梳理
安全体检
综合体检结果
云边界统计
请输入体检报告ID/名称进行搜索
(近7天)
互联网边界
560
近7天新增 32
体检报告ID/名称
体检计划
体检资产
所属账号
周期任务
429
立即体检
425
Web服务
76
近7天新增 76
完全开放
247
128
风险Web服务
20
漏洞风险
65
弱口令风险
0

查看边界列表

最近更新时间：2025-04-11 17:39:02

查询边界列表

1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 在**云边界分析 > 互联网边界 > 边界列表**中，支持查看云上互联网边界的详细列表。



特殊的展示字段说明如下表。

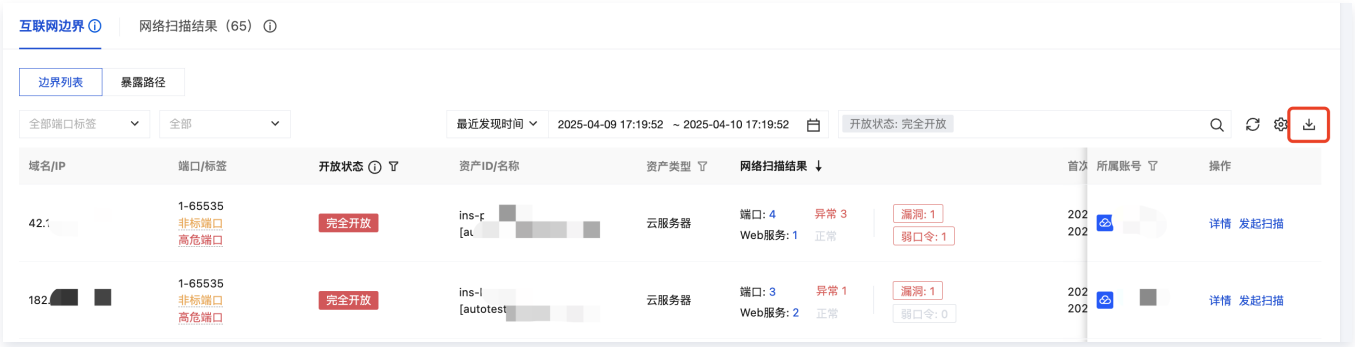
字段名	示例	说明
端口	• 1-65535 • 22	端口是根据云资源的访问控制规则获取，如您的安全组如果配置了1-65535的开放策略，那么1-65535就会被定为一个边界。
端口标签	• 高危端口 • 非标端口	端口标签直接根据端口号进行判定。定义端口标签是为了帮助您更好的规范网络开放端口。 • 高危端口：以下端口将被视为高危端口：22、23、135、137、139、161、1099、1433、1521、3306、3389、5432、8000、9200、27017。 • 非标端口：非 80，443 的端口将被视为非标端口。
开放状态	• 完全开放 • 受限访问 • 无法访问	开放状态是云安全中心根据资产的属性进行判断的接口，代表您网络策略配置的状态，并不是指扫描结果。 • **完全开放**：互联网所有地址均允许访问该端口。 • **受限访问**：云资源设置了访问控制，仅允许白名单里地址访问该端口。 • **无法访问**：云资源状态异常或关机，因此无法被访问。
扫描结果	• 未扫描 • 0	资产经过体检中相关扫描后，即可获取扫描结果。结合扫描结果可以提升治理优先级。 • 0代表扫描未发现端口开放情况。 • 未扫描即该资产未经过扫描，无法获取扫描结果。 • 扫描结果包含：端口服务、Web 服务、漏洞、弱口令。
发现时间	2025-02-28 00:00:00	• 首次发现时间：代表首次记录该互联网边界数据的时间。 • 最近发现时间：代表该互联网边界数据最近被更新的时间。每一次对互联网边界进行统计时，若发现该数据，即更新时间。因此，您可以根据最近发现时间判断该边界是否仍存在。

特殊过滤条件说明如下表：

字段	可选值	使用场景

端口标签	• 高危端口 • 非标端口 • 其他	如果您期望网络开放按一定的规范进行，那么您可以根据筛选不同的端口标签和开放状态来进行网络规范治理。 如：除报备的特殊需求场景外，80,443是唯一允许开放至互联网的端口。那您可以过滤完全开放并且标签为非标端口的边界。
开放状态	• 完全开放 • 受限访问 • 无法访问	
扫描结果	• 端口可访问 • 存在 Web 服务 • 存在高危服务 • 存在风险 Web 页面 • 存在漏洞 • 存在弱口令	选项说明： • 端口可访问：互联网边界端口范围内，扫描发现端口可访问。 • 存在 Web 服务：互联网边界端口范围内，扫描发现 Web 服务。 • 存在高危服务：互联网边界端口范围内，扫描发现高危服务，如 mysql、ssh 等。 • 存在风险 Web 页面：互联网边界端口范围内，扫描发现可能存在风险的 Web 服务，如 jenkins。 • 存在漏洞：互联网边界端口范围内，扫描发现漏洞。 • 存在弱口令：互联网边界端口范围内，扫描发现系统弱口令。如ssh弱口令、网站后台弱口令。 您可以根据不同的风险优先级来推进治理工作。

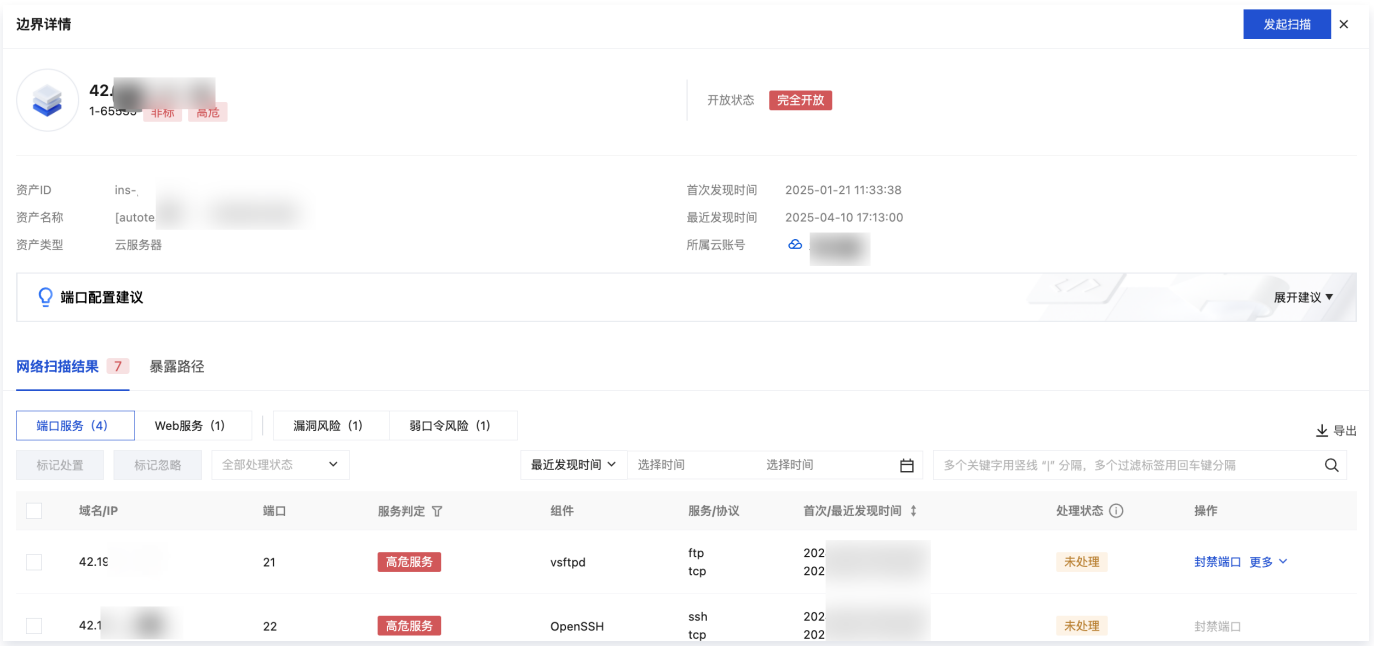
3. 单击后侧的**导出**按钮，可以将数据进行导出，格式是 Excel。



边界详情

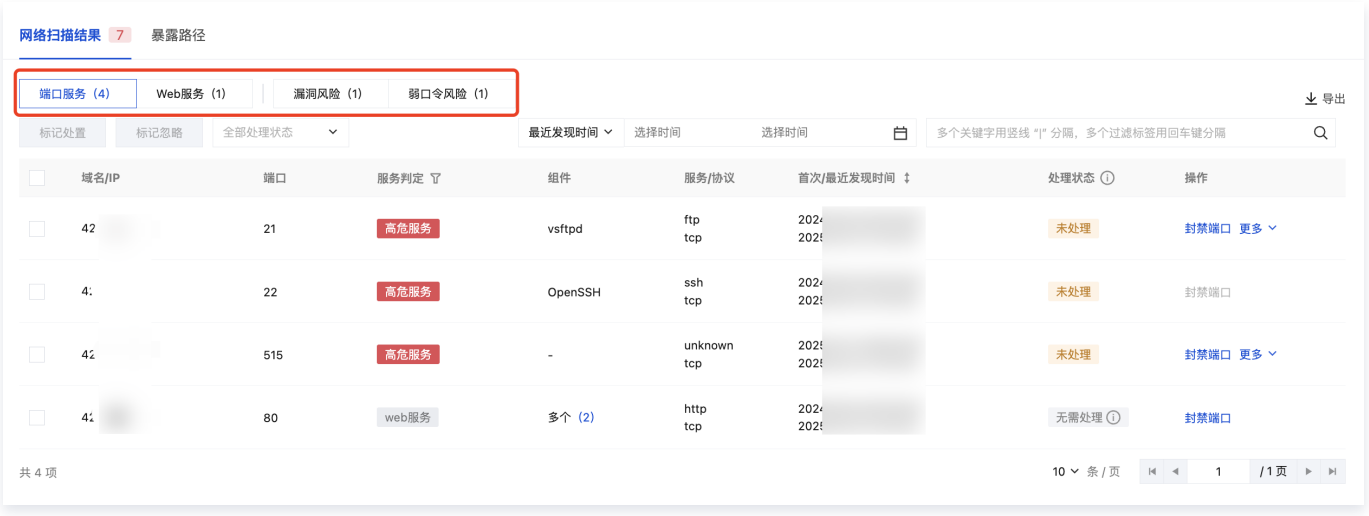
1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 在**云边界分析** > **互联网边界** > **边界列表**中，选择目标数据，单击**详情**。

3. 在边界详情页面上方提供了互联网边界的详情信息、端口配置建议。

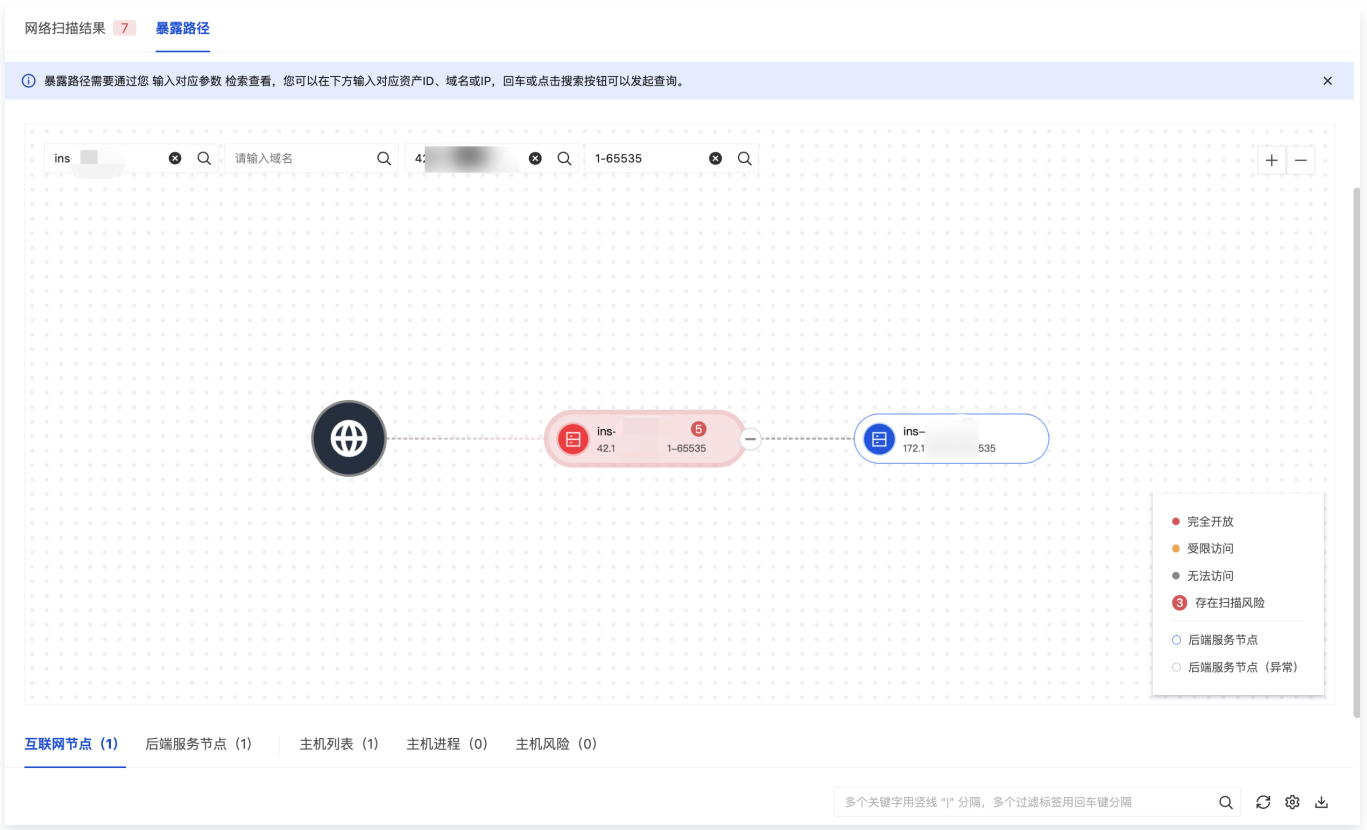


4. 单击**展开建议**，可查看对应的**端口配置建议**。

5. 在边界详情页面，支持通过切换 Tab 页面查看该互联网边界的**扫描结果**。



6. 单击**暴露路径**，可以查看该公网资产的后端资源信息。有关暴露路径功能的详细信息，请参阅 文档 。


网络扫描结果 7
暴露路径
暴露路径需要通过您 输入对应参数 检索查看，您可以在下方输入对应资产ID、域名或IP，回车或点击搜索按钮可以发起查询。
ins
请输入域名
1-65535
ins-
42.1
1-65535
ins-
172.1
535
完全开放
受限访问
无法访问
存在扫描风险
后端服务节点
后端服务节点（异常）
互联网节点（1）
后端服务节点（1）
主机列表（1）
主机进程（0）
主机风险（0）
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

检索暴露路径

最近更新时间：2025-04-11 17:39:02

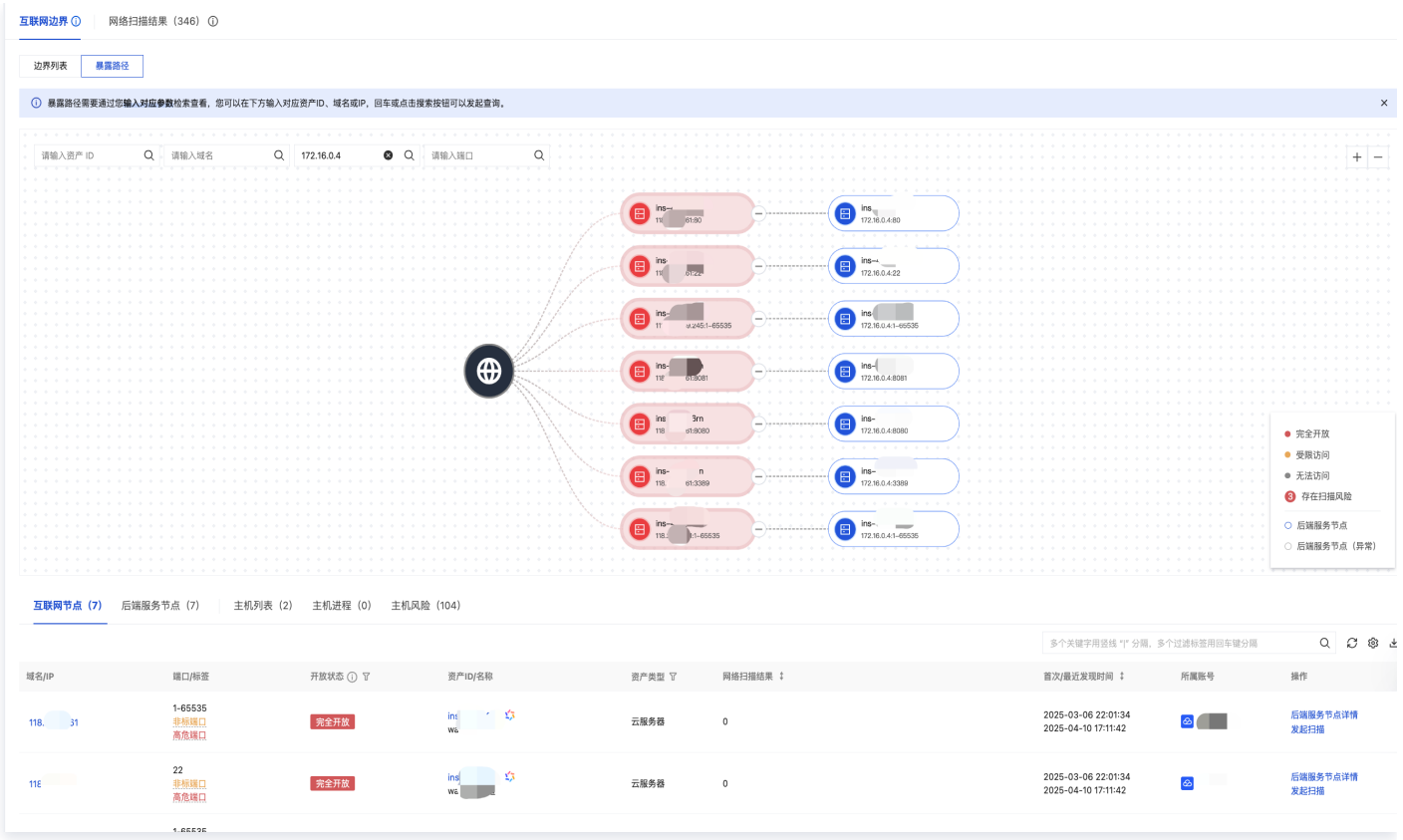
功能介绍

暴露路径提供了基于资产信息来检索资产暴露路径的功能。如果您购买了主机安全产品，还将展示主机对应的进程信息、漏洞信息、高危基线风险信息。通过暴露路径，您可以输入某个**公网资产**，云安全中心将展示该资产后端挂载服务的映射路径，甚至看到具体的端口进程是什么。您也可以输入某个**内网资产**，查看其通过哪些网络设备（如：NAT网关、弹性公网、负载均衡、CDN）等面向互联网开放的过程。

暴露路径检索

1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 在**云边界分析** > **互联网边界** > **暴露路径**中，支持检索资产暴露路径。

3. 输入资产 ID、域名或 IP 的一个或多个，即可开展检索，输入端口可以得到更精确的路径。页面分为**树状图**和**数据详情列表**两个部分。



暴露路径树状图

1. 资产暴露路径将通过树状图的形式进行展示，初始节点为**互联网 Internet**，面向互联网的节点即为**互联网节点**，后续所有资产节点为**后端服务节点**，主机类资产可以关联到**进程端口节点**。若进程存在漏洞或高危基线风险，则会关联**风险节点**。以下是节点的状态说明。

节点类型	颜色区分	说明
互联网节点	• 红色：完全开放 • 橙色：受限访问 • 灰色：无法访问	• **完全开放**：互联网所有地址均允许访问该端口。 • **受限访问**：云资源设置了访问控制，仅允许白名单里地址访问该端口。 • **无法访问**：云资源状态异常或关机，因此无法被访问。
后端服务节点	• 蓝色：正常 • 灰色：异常	• **正常**：资产处于正常运行、激活等状态。 • **异常**：资产处于关机、未激活等异常状态。

2. 在暴露路径中，将鼠标放置于节点上，可以查看节点的详细信息。

数据详情列表

在暴露路径中，云安全中心将根据暴露路径的节点信息提供更详细的数据展示。

- 互联网节点列表：展示面向互联网的节点的数据信息。

- 后端服务节点列表：展示互联网节点后映射的后端服务的数据信息。

- 主机列表：展示通过主机安全采集到的主机进程信息，以便您了解主机上的应用信息、端口监听情况。

- **主机进程列表：展示通过主机安全采集到的主机进程信息，以便您了解主机上的应用信息、端口监听情况。**

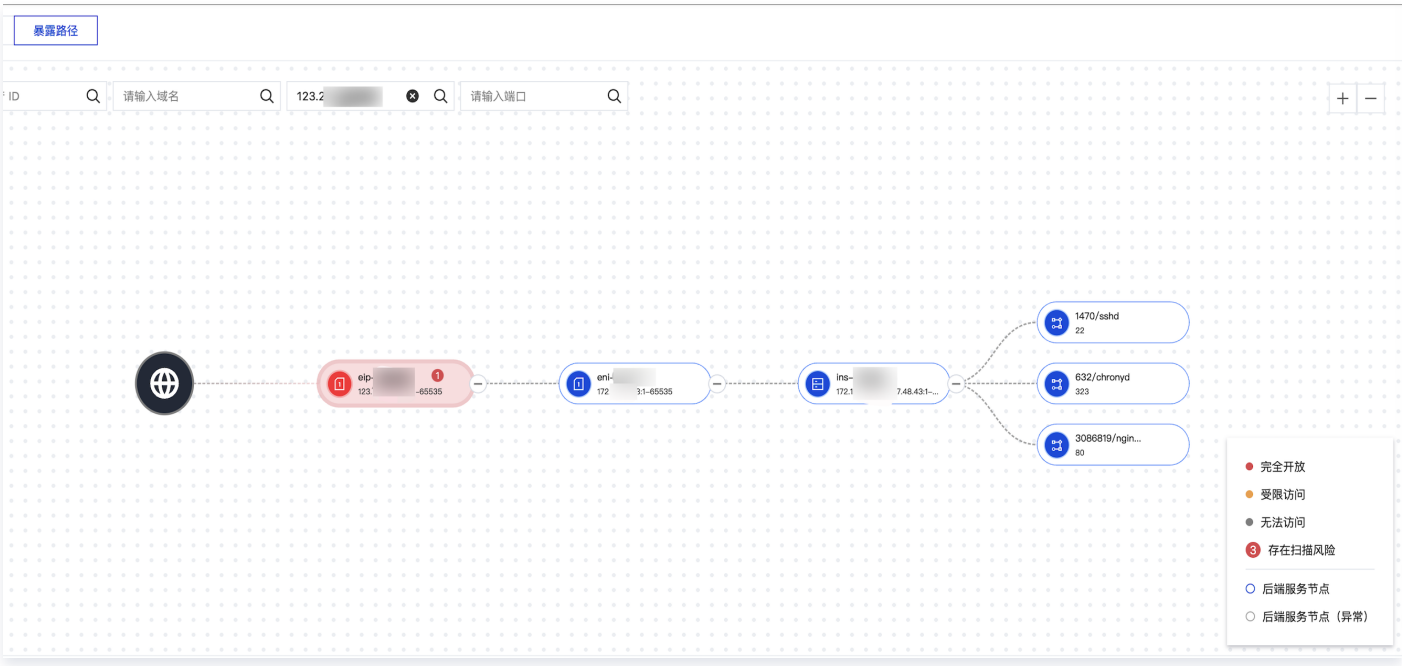
- **主机风险列表：分为主机漏洞、主机高危基线风险。高危基线风险包含弱口令检查、未授权访问等。**

暴露路径示例解读

下图的路径关系如下：

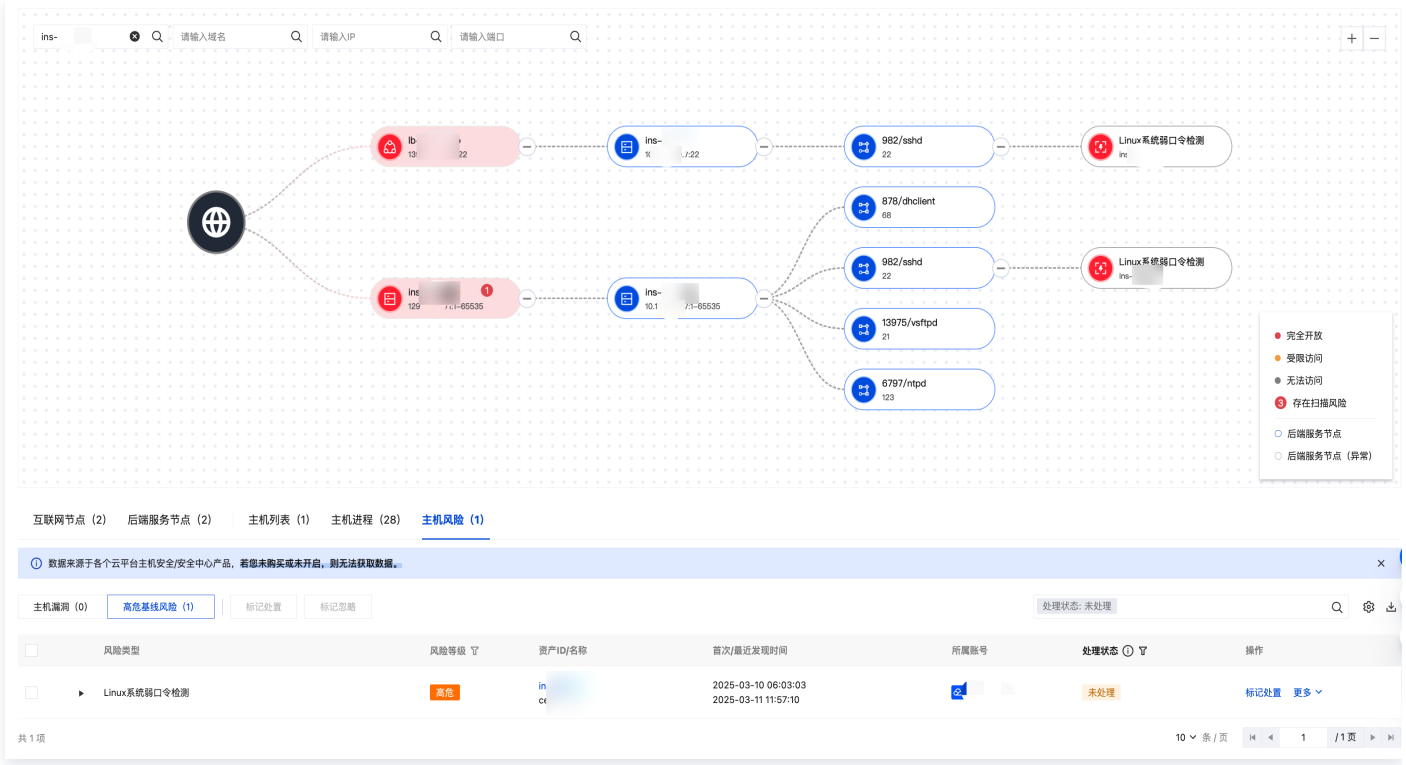
1. 弹性公网 EIP（eip-****, IP:123.***.***.***）绑定了弹性网卡（eni-****）。

2. 弹性网卡（eni-****）绑定了弹性网卡云服务器（ins-***）。
3. 关联主机安全资产，发现云服务器（ins-***）的3个进程监听了22、323、80等三个端口。
4. 由于弹性网卡的安全组策略设定了1-65535端口面向0.0.0.0/0开放，最终导致公网IP（123.***.***.***）面向互联网开放了1-65535端口。实际，可访问的端口是22、323、80。



应用场景示例

1. 当 CVM 实例 ins-ox****出现入侵告警时，需要排查可能的入侵路径。您可以在暴露路径输入该实例 ID，即可展示该资产面向互联网开放的场景。

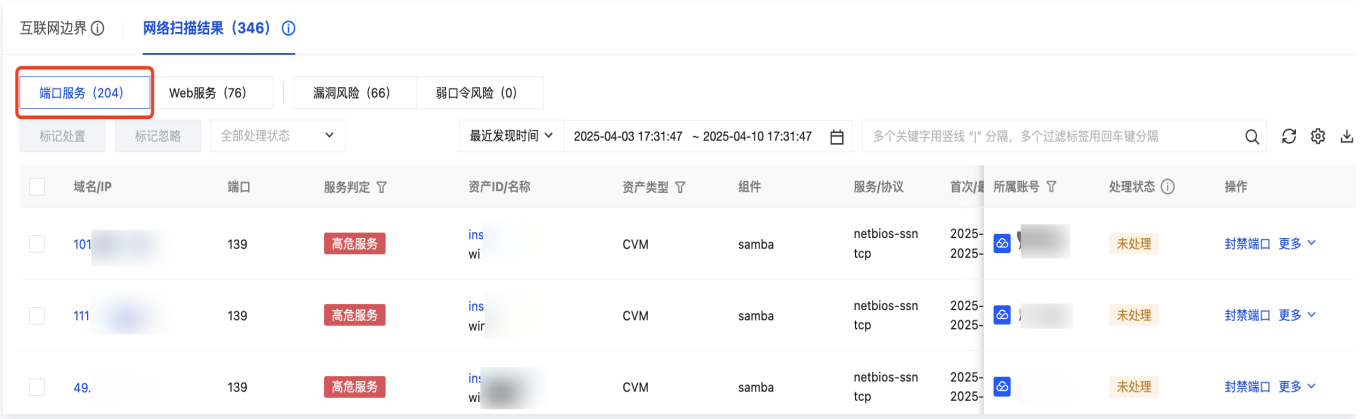


2. 分析可知，资产通过安全组开放了所有端口，并且配置了公网 IP(129.***.***.***)。同时通过负载均衡（139.***.***.***）开放了22端口。资产存在 Linux 系统弱口令，该弱口令可能是入侵的主要原因。可以根据该方向进行排查。

查看扫描结果

最近更新时间：2025-04-11 17:39:02

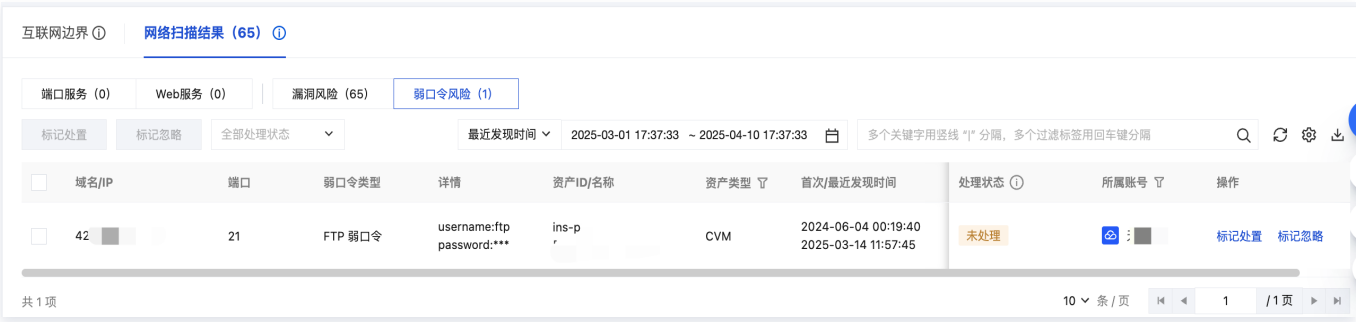
1. 登录 云安全中心控制台，在左侧导览中，单击**云边界分析**。
2. 在**云边界分析 > 扫描结果**中，切换 Tab 选项卡，读取不同的结果数据。
   - **端口服务**：查看扫描发现的互联网端口及对应的组件、服务信息。云安全中心会将高危服务进行标注。



   - **Web 服务**：查看扫描发现的 Web 服务，包括预览页、标题、状态响应码、组件等。云安全中心会将高危 Web 服务进行标注。

   - **漏洞风险**：查看扫描发现的漏洞。您可以通过勾选**仅展示 POC 扫描发现**，来过滤通过 POC 检测的漏洞。

- **弱口令风险**：查看扫描发现的应用弱口令或网站后台弱口令。

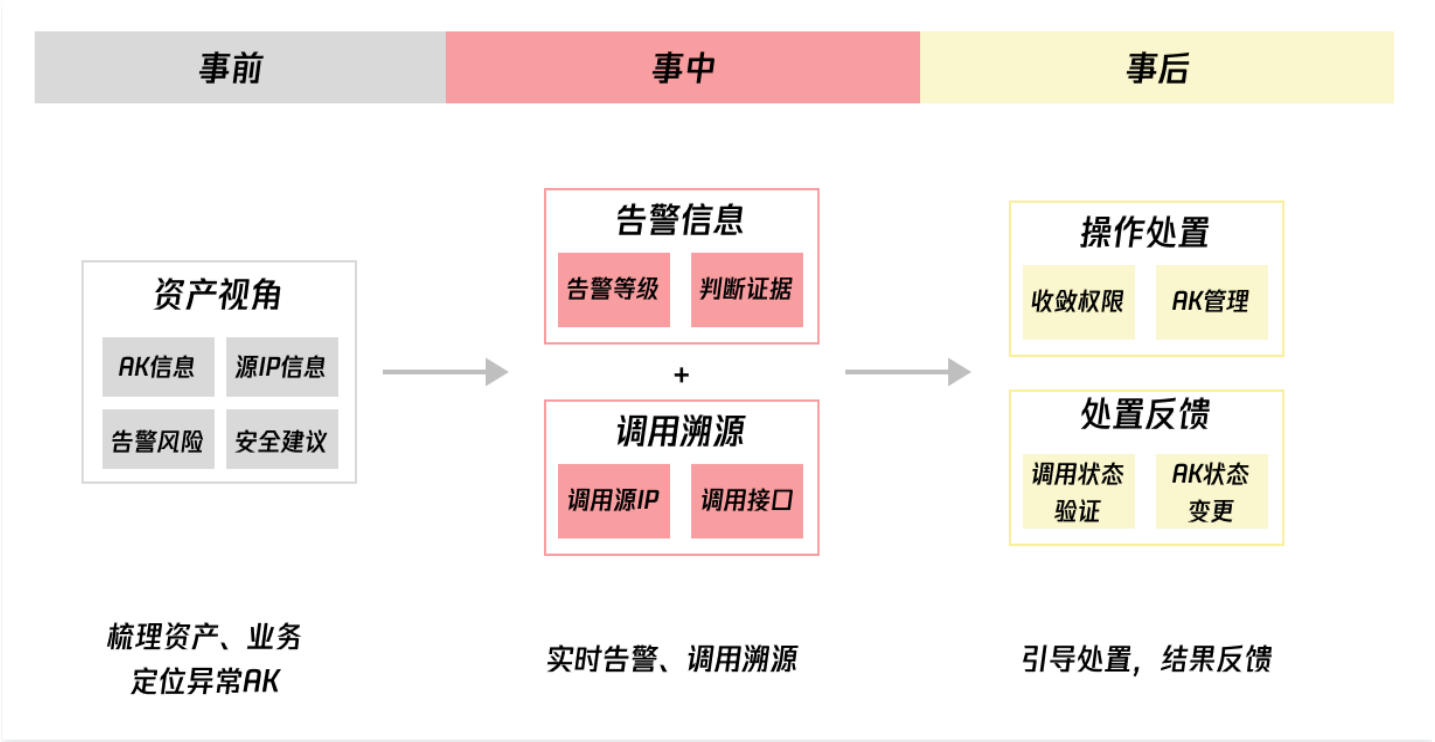


云 API 异常监测
功能简介

最近更新时间：2025-04-22 16:18:12

云安全中心通过实时监测云 API 访问密钥 AccessKey（以下简称：AK）相关信息，梳理 AK 权限配置与调用路径，并基于腾讯云独有的丰富情报识别**泄露事件、异常调用、权限配置风险**，并进行告警。

> **注意：**
> 建议您及时关注 AK 调用情况与异常告警，并按照相关指引修改权限策略，可帮助您解决 AK 的权限失控、配置错误、泄露响应慢、异常调用难溯源等问题，更好地对 AK 进行管理，减少安全隐患，防止威胁扩散，保障云上安全。



功能点梳理

功能板块		功能点	解决问题	操作指引
统计面板 资产概览 & 安全概览		快速了解 AK 资产情况，定位建议关注的异常 AK、待处理告警、待处理风险等。	定位高优问题，了解有多少 AK 需关注，待处理的问题有多少，近期安全运营趋势怎样。	统计面板
资产列表	AK 资产	基于 AK 资产视角，查看 AK 基本信息、安全建议、关联告警与风险、调用记录与关联资产。（永久密钥与临时密钥均支持）	梳理 AK 数量，了解每个 AK 是否在被调用，这把 AK 被多少个 IP 访问了哪些接口，调用是否有异常，相关策略是哪些。	资产列表
	调用源 IP	基于调用源 IP 视角，查看 IP 地域、类型、调用 AK 情况、关联告警、调用记录。	梳理请求了永久 AK 的 IP 数量，IP 是否为内部资产，IP 属地是哪，调用了多少 AK，是否有告警，支持客户备注 IP 所属业务。	

告警列表		实时监控 AK 泄露与异常调用： • 黑客工具/行云管家/ cos-browser 识别。 • github 泄露（github 合作 + IP检查等）。 • 异常 IP 调用敏感接口等。 基于告警规则视角，查看告警内容（泄露、异常调用），关联 AK 与异常调用记录，并提供权限策略配置建议。	• 实时告警泄露事件，全面分析并溯源异常调用； • 了解泄露地址，了解异常调用链路（调用IP、访问服务与接口、相关策略），提供治理建议，引导处置。	告警
风险列表		自动化扫描 AK 权限配置， 检查 AK 是否存在高权限策略，基于风险规则视角，查看配置风险描述与风险判定证据，并提供权限策略配置建议。	支持事前梳理 AK 的高风险策略配置，收敛敏感权限，减少安全隐患。	风险
策略管理	告警策略	管理系统告警策略。	管理需要关注的告警策略，并基于业务需要自定义白名单。	策略管理
	白名单策略	管理告警白名单，可对白名单进行增删改查，基于IP、调用方式、AK、接口等进行加白。		

说明：
由于 AK 异常检测功能比较敏感，提供 API 后可能暴露更多风险 API 接口，暂不提供 API 接口。

云 API 密钥安全使用方案

最近更新时间：2025-04-22 16:18:12

云 API 密钥 AccessKey（以下简称“AK”）是构建腾讯云 API 请求的重要凭证。您的 API 密钥代表您的账号身份和所拥有的权限，使用腾讯云 API 可以操作您名下的所有腾讯云资源。
AK 包含 SecretId 和 SecretKey，用于您调用 腾讯云 API 时生成签名，查看 生成签名算法 。SecretId 作为用户标识，**SecretKey（必须保密）**为验证用户身份的密钥。

> **注意：**
> AK 若泄露且被恶意利用，会给用户的云上资源与相关业务带来很大的安全隐患，进一步造成重大损失。

AK 泄露案例

1. 代码仓库硬编码暴露风险

开发者将 SecretId/SecretKey 直接写入业务代码并上传至 GitHub 等开源平台，攻击者通过关键词（如"SecretKey"、"cos.ap-shanghai"等）搜索即可快速定位敏感凭据。（代码中未使用环境变量或配置中心，凭据以明文形式存在于版本控制历史记录中。）

2. 客户端反编译导致的凭证提取

小程序/APP 开发者将 SecretKey 硬编码在客户端，攻击者通过逆向工程（如反编译 APK、微信小程序源码）提取凭据，直接接管云资源。

3. 技术文档与样例代码泄露

技术文档、内部或公开分享材料中包含测试环境 SecretId/SecretKey，攻击者利用其访问生产资源。

4. 临时密钥滥用

开发者在客户端直接生成临时密钥，攻击者在有效期内劫持并利用其发起恶意请求。

5. 日志与监控系统泄露

云函数（SCF）环境变量、云硬盘快照或操作审计日志中残留 SecretKey 明文，攻击者通过权限枚举获取敏感信息。

6. 服务器内明文配置的 AK 被攻击者获取

攻击者通过漏洞入侵服务器、任意文件读取漏洞，通过环境变量、配置文件等，窃取到明文 AK/SK。

AK 安全实践教程

避免使用主账号 AK

请尽量不要使用主账号 AK 访问腾讯云，更不要将 AK 共享给他人。一般情况下，应该为所有访问腾讯云的用户创建子账号，同时授权该子账号相应的管理权限。相关设置请参见 用户类型 。

请勿在代码中嵌入 AK

嵌入代码中的 AK 凭证容易被人忽视，经验丰富的开发者会将其写入数据库或者独立的文件中，使得其管理起来更方便。
开发者应将 AK 存储在独立加密配置文件或密钥管理系统中（如腾讯云 KMS 白盒密钥），而非直接写入业务代码，降低因代码仓库权限管理疏漏或客户端反编译导致的泄露风险。

定期更新 AK

建议您或 CAM 用户要定期轮换 AK。这样可以让身份凭证泄露情况下的影响时间受限。

删除不需要的权限/AK

- 删除用户不再需要的权限，尽量减少 AK 泄露后带来的安全风险。
- 删除长期不使用的 AK，减少 AK 的暴露面。

遵循最小权限原则申请账户

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限，不要授予更多无关权限。例如，一个用户仅是 COS 服务的使用者，那么不需要将其他服务的资源访问权限（如 CAM 读写权限）授予给该用户。
另外申请用户时，如果只需要 API，仅申请 API 权限用户即可，不要把控制台和 API 的用户混合。

事前 AK 请求情况梳理

在云安全中心 > 云 API 异常监测，实时做好 AK 的资产管理和备注。

- AK 列表：梳理 AK 资产，了解我有多少把 AK，备注每把 AK 是什么业务在用。
- 调用源 IP：梳理调用源 IP，了解每个调用源 IP 属于哪个业务。
- 风险权限收敛：查看 AK 配置检查结果，梳理是否有不需要的高权限接口。
- 应急响应：当提前掌握好上面的情况后，出现 AK 泄露导致异常调用时，可以快速的完成 AK 替换。

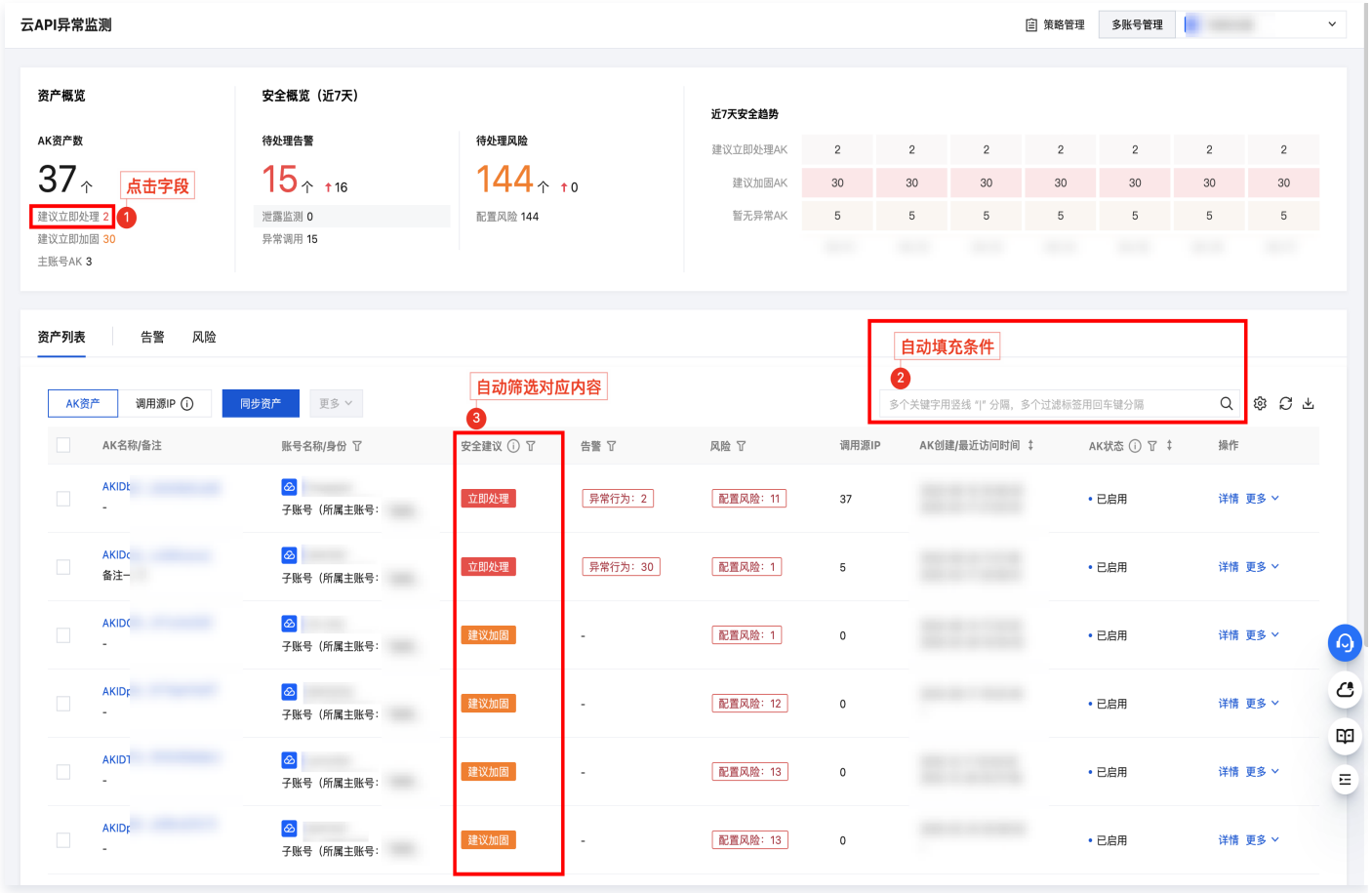
统计面板

最近更新时间：2025-04-22 16:18:12

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. **资产概览：**统计当前腾讯云账号下主账号与子账号全部 AK 数量（包含永久密钥与临时密钥）与不同安全建议的 AK 数量。

安全建议	建议说明
立即处理	该 AK 有异常调用告警/泄露事件，请立即关注并处理。
建议加固	该 AK 权限配置存在风险，建议进行关注并收敛权限，完成加固。
暂无异常	该 AK 暂无异常调用告警、泄露事件，权限配置暂无风险。

3. **安全概览：**统计近7天待处理的告警和风险，与不同类型告警的数量；统计近7天不同安全建议的 AK 变化趋势。
4. 单击“关注的字段”，下方列表搜索框中自动添加条件并筛选出对应内容。



资产列表

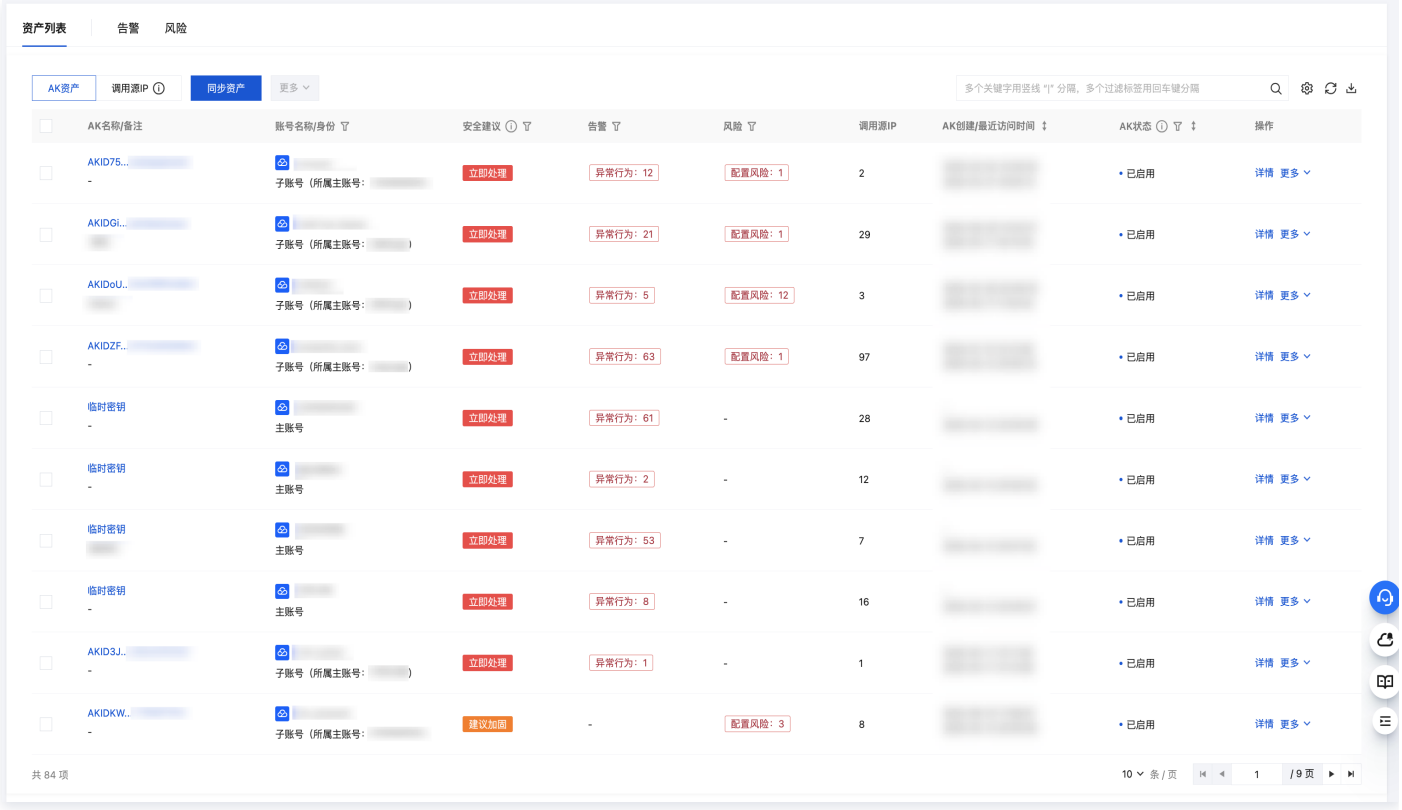
最近更新时间：2025-04-22 16:18:12

AK 资产

AK 资产列表

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在**资产列表 > AK 资产**中，基于 AK 资产视角，查看 AK 基本信息、安全建议、关联告警与风险。

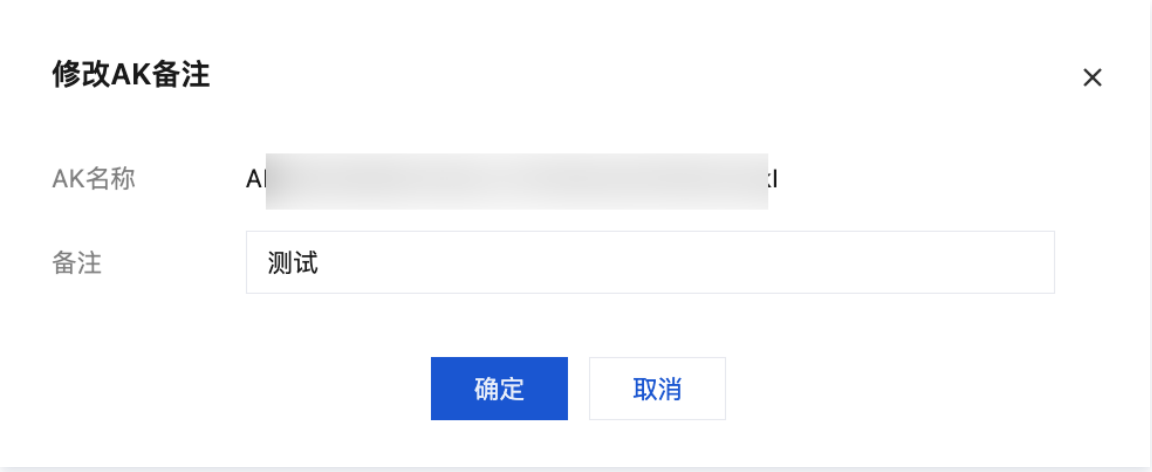
> **说明：**
> 临时密钥由于数量较多，不停变化，所以进行了聚合展示，临时密钥也包含了控制台的临时密钥，AK名称为“临时密钥”



字段名	示例	说明
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 **AK 详情**抽屉。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”。
账号名称/身份	账号 A 主账号/子账号（所属主账号：主账号 B）	• AK 所属云厂商与账号，若为子账号展示所属主账号信息。 • 鼠标悬浮查看账号 ID与 APPID；支持筛选主账号/子账号。

安全建议	• 立即处理 • 建议加固 • 暂无异常	• 基于当前 AK 的告警、风险状态，为您提供综合的安全等级，可以按照推荐的处理等级进行处置。 • 支持筛选不同建议管理的 AK。
告警	• 异常调用：x • 泄露监测：x	• 近期未处理告警，单击拉起 **AK 详情**抽屉，定位到**告警**页签。 • 支持筛选泄露监测/异常行为/无告警
风险	• 权限风险：x	近期未处理风险，单击拉起 **AK 详情**抽屉，定位到**风险**页签。
调用源IP	6	调用该 AK 的 IP 数量。
AK创建/最近访问时间	• 2025-01-01 18:00:00 • 2025-01-12 18:00:00	AK 创建与最近访问时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
AK状态	• 已禁用 • 已启用	展示 AK 禁用/启用状态。 支持筛选已禁用/已启用。

3. 在 AK 资产中，支持进行如下操作：
   - 详情：单击**详情**，拉起 **AK 详情**抽屉。
   - 更多：单击**更多**，支持选择检测、API 密钥管理、修改 AK 备注、添加白名单策略。
     - 检测：检查对应 AK 的配置风险。
     - API 密钥管理：跳转至**访问管理** > **访问密钥** > **API 密钥管理**页面。
     - 修改 AK 备注：修改备注信息，单击**确定**。

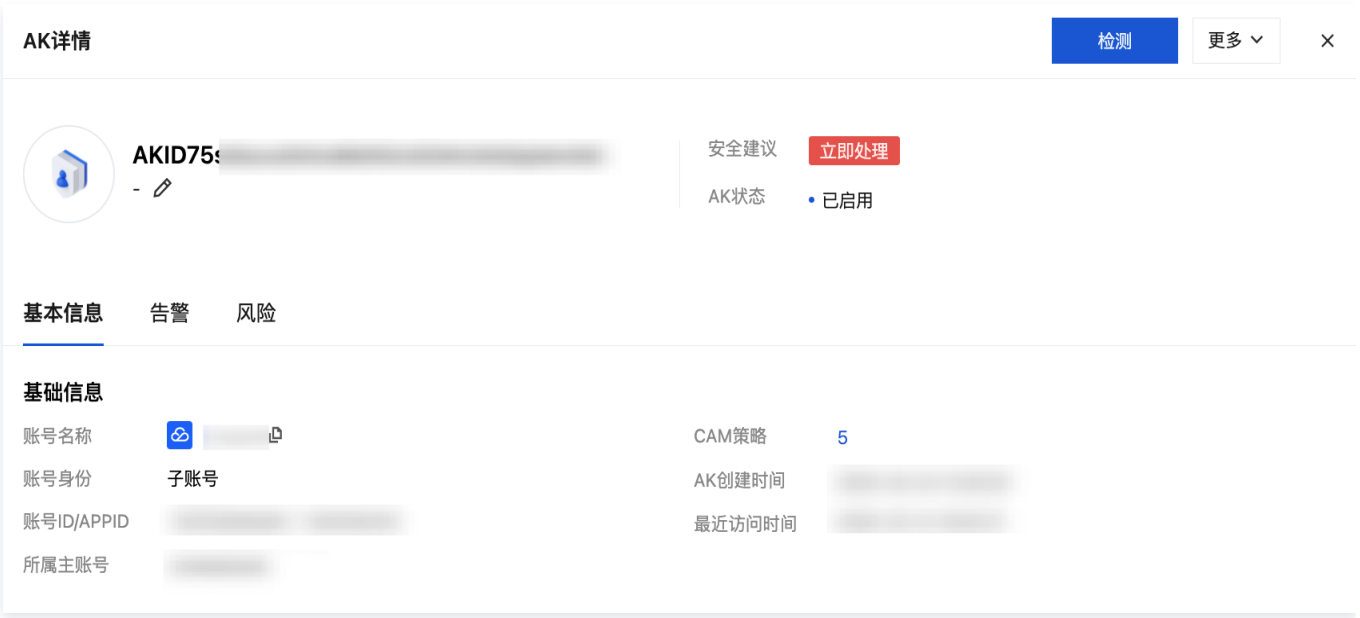


     - 添加白名单策略：进入添加白名单策略页面，并填充对应 AK。

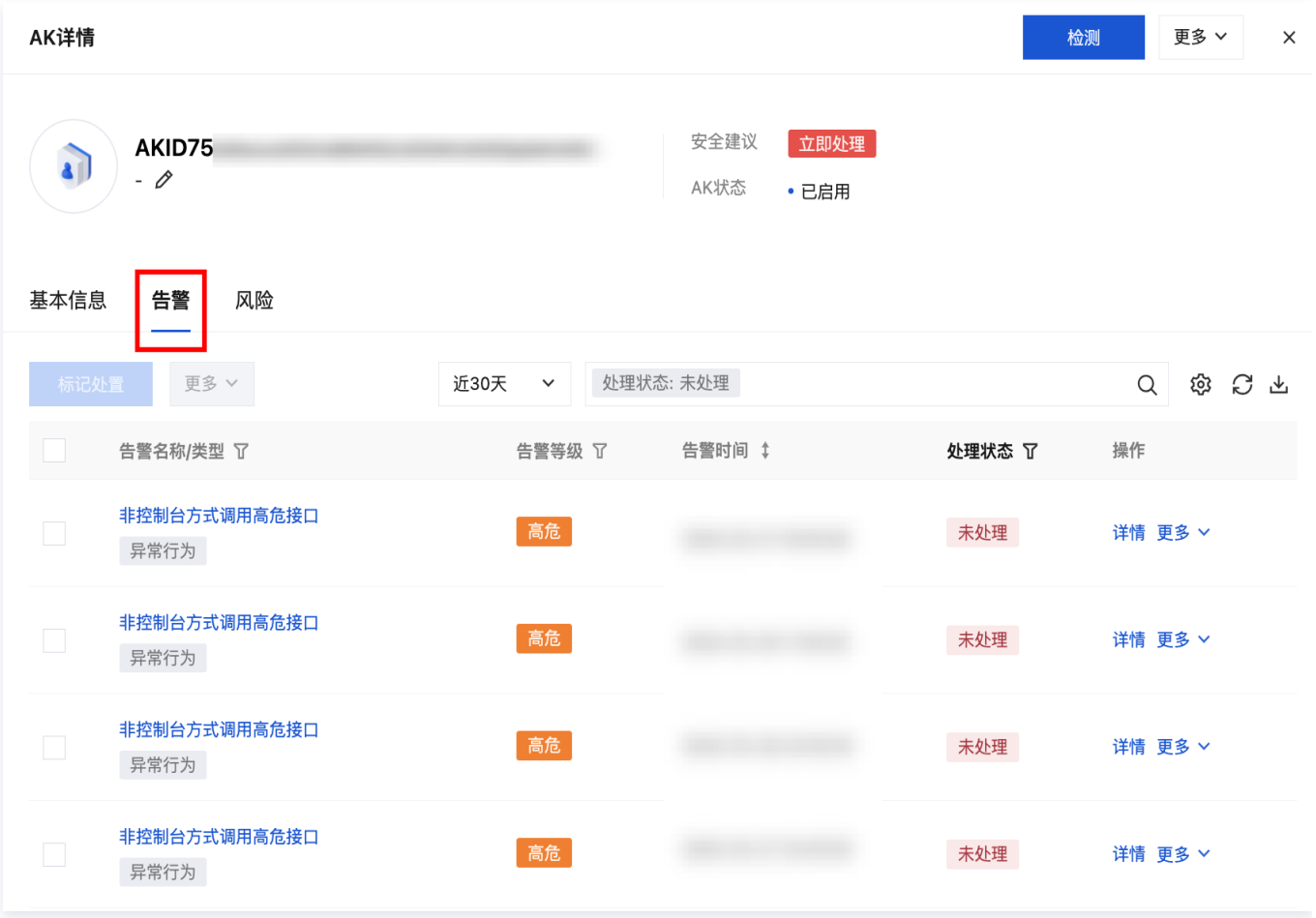
AK 详情

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在**资产列表** > **AK 资产**中，选择所需资产，单击**详情**。

3. 在 AK 详情页面，查看 AK 信息关联告警与风险、调用记录与关联资产。
   - 查看 AK 信息



   - 查看 AK 告警信息，默认展示未处理告警，单击**详情**拉起**告警详情抽屉**，字段解释请参见 告警 。



- 查看 AK 风险信息，默认展示未处理风险，单击**详情**拉起**风险详情抽屉**，字段解释请参见 风险 。

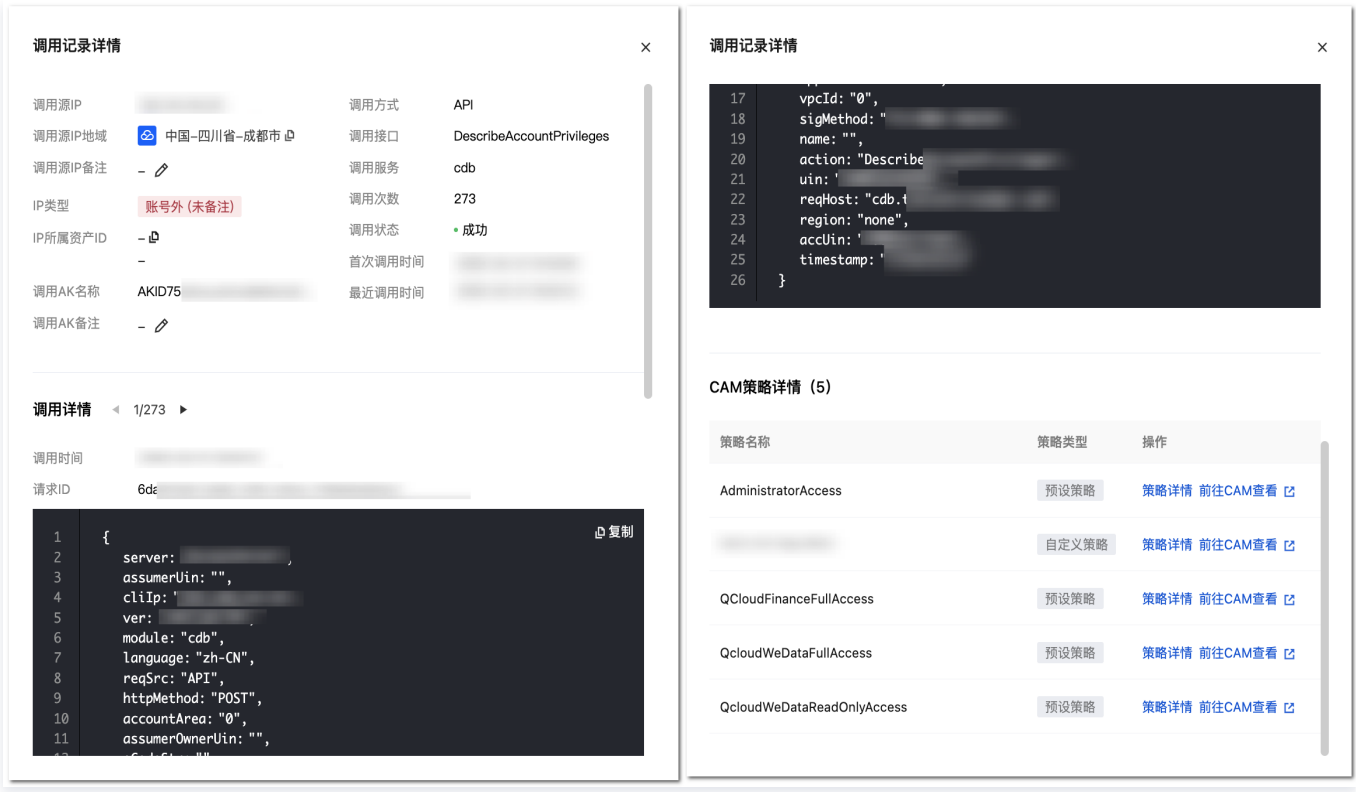
- 查看调用记录，查看调用该 AK 的 IP、IP 类型、用什么方式调用了什么服务、调用成功和失败分别的次数、首次/最近调用时间，以及相关的 CAM 策略。

字段名	示例	说明

调用源 IP/地域/备注	1.1.1.1 中国-北京 | 部门1AK	调用源 IP、所属地域与自定义备注。 • IP 内容支持一键复制。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”。
IP类型	• 账号外（未备注） • 账号内（未备注） • 账号外 • 账号内	• 账号内：在云安全中心 IP 资产列表中识别到的调用源 IP，有备注。 • 账号内（未备注）：在云安全中心 IP 资产列表中识别到的调用源 IP，无备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 账号外：非账号内 IP 但有备注。
调用方式	• API • 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。
调用接口/服务	DescribeAccountPrivileges cdb	调用的接口与接口所属服务。
CAM 策略	AdministratorAccess	该 AK 关联的 CAM 策略，多个时显示数字，单击打开 CAM 策略详情弹窗。
调用状态/次数	• 成功（x次） • 失败（x次）	调用该 AK 成功/失败状态及次数。
首次/最近调用时间	• 2025-01-01 18:00:00 • 2025-01-12 18:00:00	首次与最近调用时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
IP所属资产（ID/名称）	ins-xxx 机器1号	展示 AK 所属资产。

4. 在 **AK 详情 > 基本信息 > 调用记录**页面，选择所需调用源 IP，单击**详情/更多**。

- **详情**
  - 展示调用信息，调用详情（包含时间、请求 ID、请求体；支持翻页），CAM 策略详情。



- 单击**策略详情**，展示其策略代码，支持复制；单击**前往 CAM 查看**，跳转至定位**访问管理 > 策略 > 具体策略详情**。

- 更多
  - 添加白名单策略：在添加白名单策略页面，填充对应 IP、调用方式、AK、接口、返回码，单击**保存**。
  - 管理白名单策略：在策略管理页面，定位至**白名单策略**。

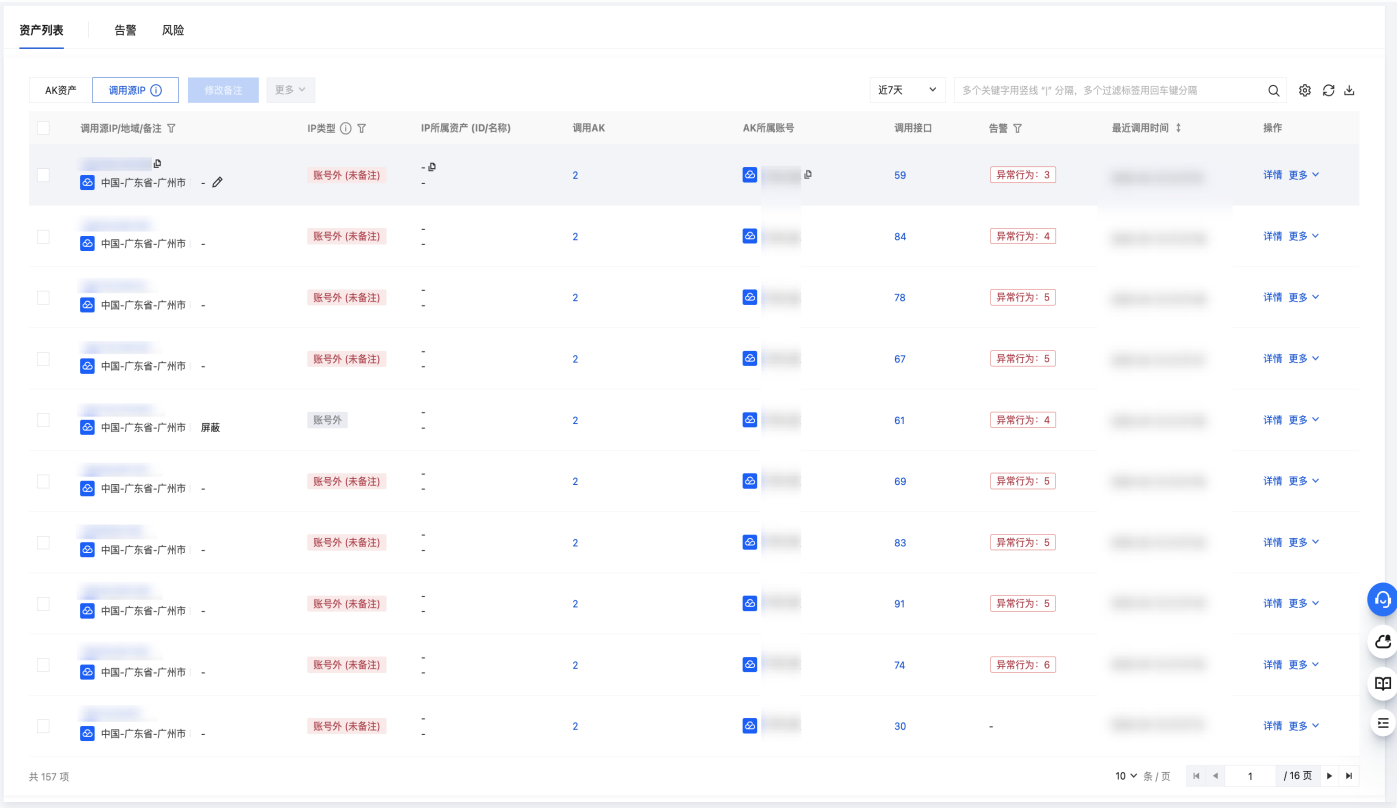
调用源 IP

调用源 IP 列表

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在**资产列表** > **调用源 IP** 中，基于调用源 IP 视角，查看调用源 IP 信息、安全建议、关联告警与风险、调用的 AK 与接口。

说明：

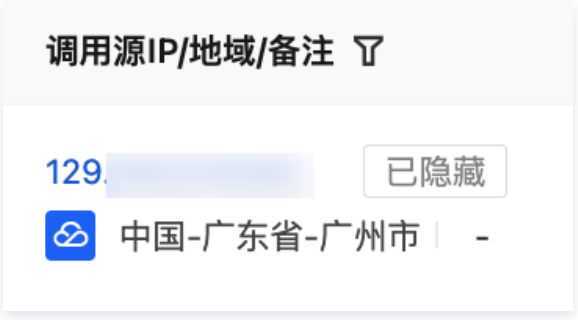
- 列表数据聚合逻辑：一天内同一 IP 调用同一账号下的 AK。
- 仅展示永久密钥的 API 请求。



字段名	示例	说明
调用源 IP/地域/备注	• 已隐藏 • 未隐藏	调用源 IP、所属地域与自定义备注；支持隐藏，可通过字段旁边筛选展示已隐藏/未隐藏IP。 • IP内容支持一键复制。 • 备注可自定义编辑，不超过20字符，若备注为空显示“–”。
IP类型	• 账号外（未备注） • 账号内（未备注） • 账号外 • 账号内	• 账号内：在云安全中心IP资产列表中识别到的调用源 IP，有备注。 • 账号内（未备注）：在云安全中心IP资产列表中识别到的调用源 IP，无备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 账号外：非账号内 IP 但有备注。
IP 所属资产（ID/名称）	ins-xxx 机器1号	展示 AK 所属资产。
调用 AK	AKXXX	多个时显示数字，单击**数字**展示具体 AK 及其所属账号。
AK 所属账号	账号 A	调用 AK 所属的主账号。
调用接口	7	多个时显示数字，单**数字**击打开**调用源 IP 详情**抽屉。
告警	• 异常调用：x	• 近期未处理告警，单击拉起**调用源 IP 详情**抽屉，定位到告警页签。

	• 泄露监测：x	• 支持筛选泄露监测/异常行为/无告警。
最近调用时间	2025-01-01 18:00:00	最近调用时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。

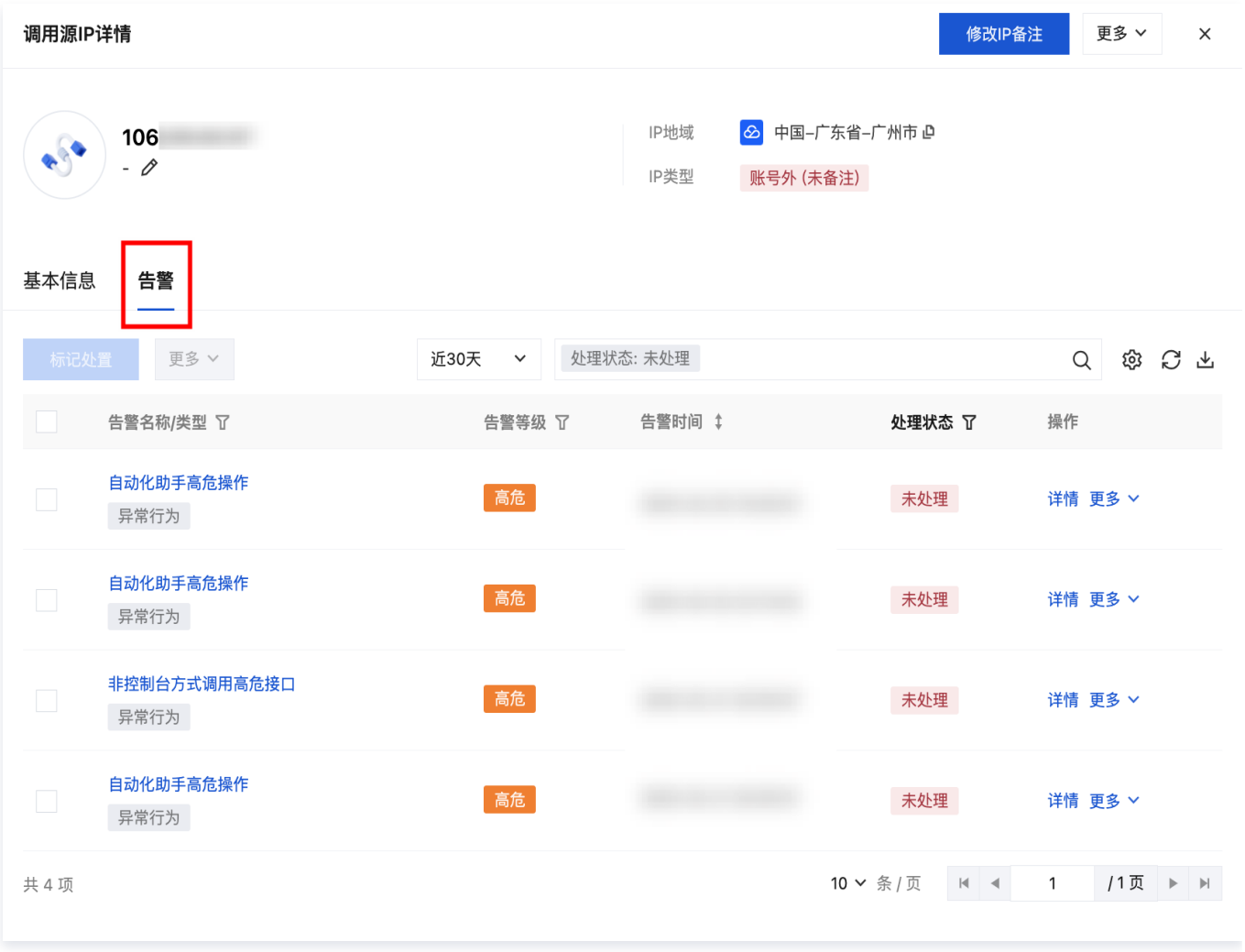
3. 在调用源 IP 中，选择所需调用源 IP，单击**详情/更多**。

操作类型		说明
详情		单击拉起**调用源 IP 详情**抽屉。
更多	修改 IP 备注	修改源 IP 备注，单击**确定**。
	添加白名单策略	单击拉起**添加白名单策略**抽屉，并填充对应 IP。
	管理白名单策略	单击跳转至**策略管理 > 白名单策略**。
	隐藏该 IP	单击隐藏该 IP的调用记录，隐藏该调用源 IP 后，后续新增 IP 的调用记录同步隐藏。隐藏后可通过字段旁边筛选展示已隐藏/未隐藏 IP，隐藏 IP 旁边通过标签标识。 

调用源 IP 详情

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在**资产列表 > 调用源 IP** 中，选择所需调用源 IP，单击**详情**。
3. 在调用源 IP 详情页面，查看 IP 信息关联告警、调用记录。
   - 查看 IP 信息

○ 查看该 IP 相关告警信息，默认展示未处理告警，单击**详情**拉起**告警详情抽屉**，字段解释请参见 告警 。



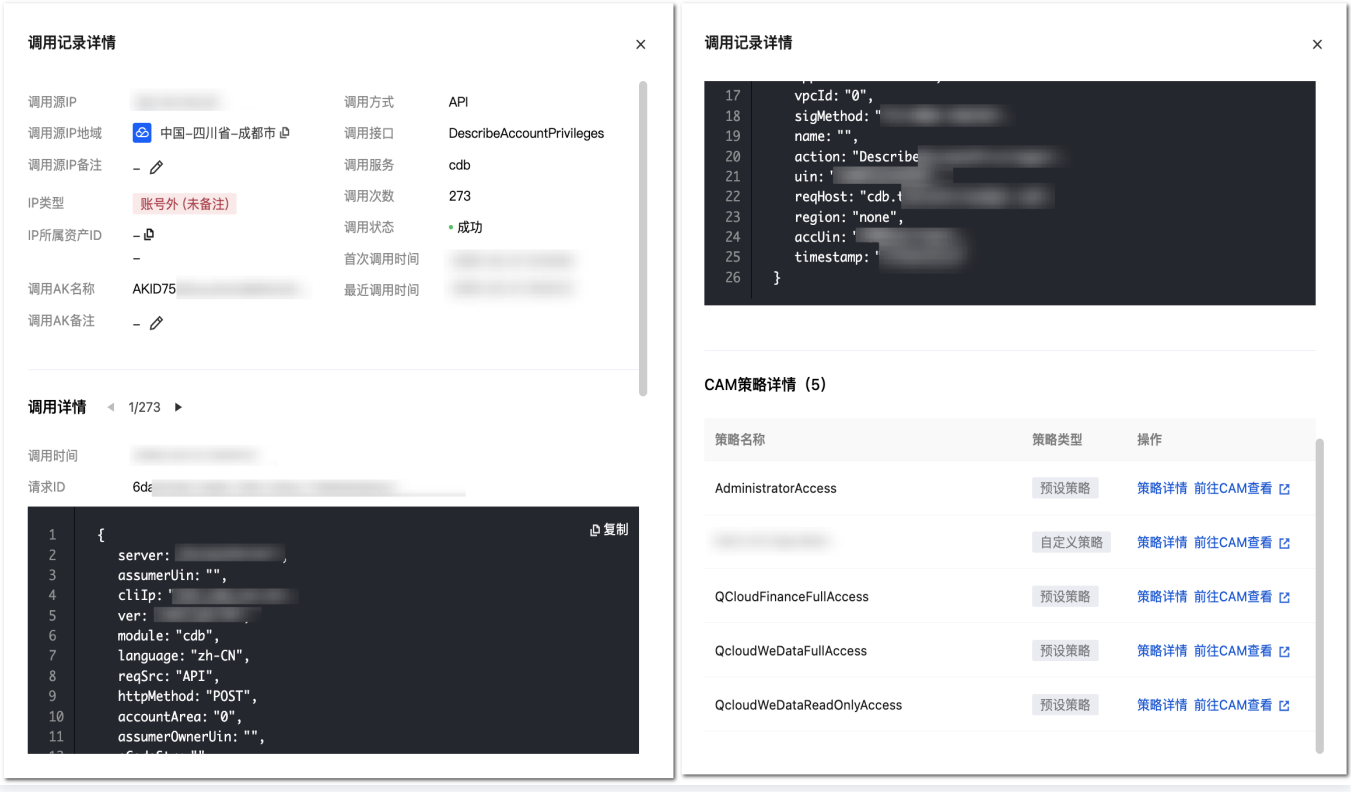
- 查看调用记录，查看调用该 AK 的 IP、IP 类型、用什么方式调用了什么服务、调用成功和失败分别的次数、首次/最近调用时间，以及相关的 CAM 策略。

字段名	示例	说明
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK保留前6位与后11位，中间省略，支持一键复制；单击拉起 AK 详情抽屉。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”
调用方式	• API • 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。
调用接口/服务	DescribeAccountPrivileges cdb	调用的接口与接口所属服务。
CAM策略	AdministratorAccess	该 AK 关联的 CAM 策略，多个时显示数字，单击打开 CAM 策略详情弹窗。
调用状态/次数	• 成功（x次） • 失败	调用该 AK 成功/失败状态及次数。

	（x次）	
最近调用时间	2025-01-01 18:00:00	最近调用时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
IP 所属资产（ID/名称）	ins-xxx 机器1号	展示 AK 所属资产。

4. 在基本信息页面，选择所需 AK，单击**详情/更多**。

- **详情：**
  - **展示调用信息，调用详情（包含时间、请求 ID、请求体；支持翻页），CAM 策略详情。**



  - **单击策略详情，展示其策略代码，支持复制；单击前往 CAM 查看，跳转至访问管理 > 策略 > 具体策略详情。**

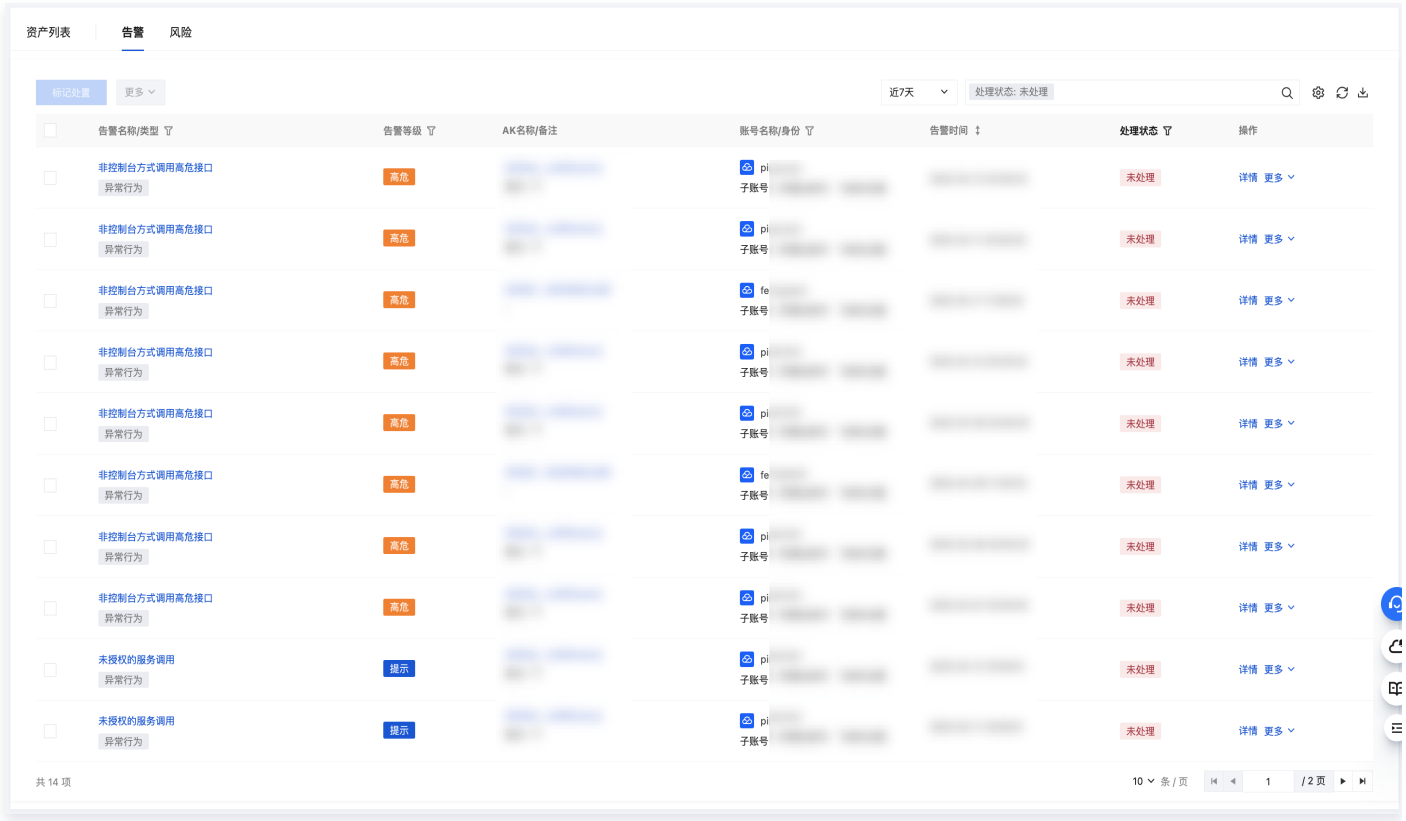
- 更多
  - 添加白名单策略：在添加白名单策略页面，填充对应 IP、调用方式、AK、接口、返回码，单击**保存**。
  - 管理白名单策略：在策略管理页面，定位至**白名单策略**。

告警

最近更新时间：2025-04-22 16:18:12

告警列表

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在告警列表中，基于告警规则视角，查看告警内容（泄露、异常调用），关联 AK 与异常调用记录，并提供权限策略配置建议。



字段名	示例	说明
告警名称/类型	• 异常行为 • 泄露监测	单击拉起**告警详情**抽屉。
告警等级	• 严重 • 高危 • 中危 • 低危 • 提示 • 无效	基于腾讯云安全实践评定告警等级。
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 **AK 详情**抽屉。 • 备注可自定义编辑，不超过20字符，若备注为空显示“–”。
账号名称/身份	账号A	• AK 所属云厂商与账号，若为子账号展示所属主账号信息。 • 鼠标悬浮查看账号 ID 与 APPID；支持筛选主账号/子账号。

	主账号/子账号（所属主账号：主账号B）	
告警时间	2025-01-12 18:00:00	告警发生时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
处理状态	• 未处理 • 已处置 • 已忽略	展示告警处理状态，手动完成标记，处理状态支持筛选。

3. 在告警列表中，选择所需告警，单击**详情/更多**。

操作类型		说明
详情		单击拉起**告警详情**抽屉。
更多	标记处置	单击后处理状态变为“已处置”。
	标记忽略	单击后处理状态变为“已忽略”
	添加白名单策略	单击拉起**添加白名单策略**抽屉，并填充对应 AK。
	API 密钥管理	单击跳转至**访问管理** > **访问密钥** > API 密钥管理。

规则说明

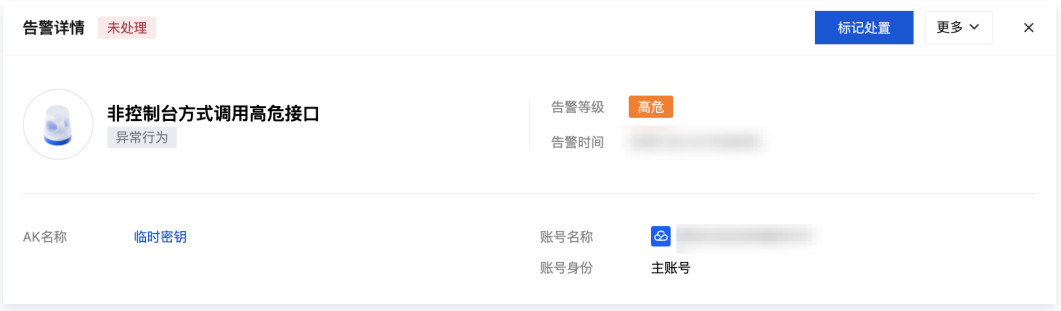
实时监控 AK 泄露与异常调用，监测分为三类：黑客工具/行云管家/cos-browser 识别、github 泄露（github 合作 + IP检查等）、异常 IP 调用敏感接口等，具体规则见下表：

规则名称	规则说明
根密钥调用高危接口	主账号访问密钥调用高危接口。 高危接口包含cam、sts、tat、scf、tke、cdb、cvm、cbs 等20+类服务的30+接口，相关示例：cam.ListAccessKeys、cam.DeleteUser...
非控制台方式调用高危接口	使用非控制台方式(主要是通过 sdk 调用云 API)，调用高危接口。
未授权的服务调用	通过 API 调用未授权的服务，需要收敛该账号/角色的权限。

创建密钥操作	有新的密钥被创建。
权限提升行为	通过调用 sts、cam 的部分接口，该用户权限得到提升。
非正常时间段敏感行为	在晚上10点至凌晨6点时间段内，通过控制台或者 API 执行一些敏感操作，例如删除资源等操作。
新增用户调用高危接口	1天内创建的用户调用了高危 API，需要注意。
github密钥确认请求	检查请求是否来源于 GithubAK 回调的出口 IP。 如果命中，代表该 ak 存在于 github 公库/私有库。
黑客工具检测	检查同一个 ak 的行为是否与黑客工具相似。
长期未使用的访问密钥出现调用	在过去一个月内未曾使用的访问密钥出现了 API 调用，需要注意。
通过cos-browser调用云API	通过 cos-browser 调用云 API，部分攻击者会使用 cos-browser 进行文件下载，需要判断是否正常使用。
通过api创建云资源	通过腾讯云 API，创建云资源，例如创建云服务器（CVM）、云数据库（CDB）等。
行云管家行为	这部分调用来源于行云管家的调用，需要关注。 行云管家是一个多云管理平台,可以可视化的管理云上 CVM、网络、镜像等，部分攻击者也会使用。需要梳理运维人员是否使用行云管家。
自动化助手高危操作	通过调用 tat 的部分接口，直接对机器执行命令。

告警详情

1. 在告警列表中，选择所需告警，单击**详情**。
2. 在告警详情页面， 查看告警信息与异常调用记录。
   - 查看告警信息

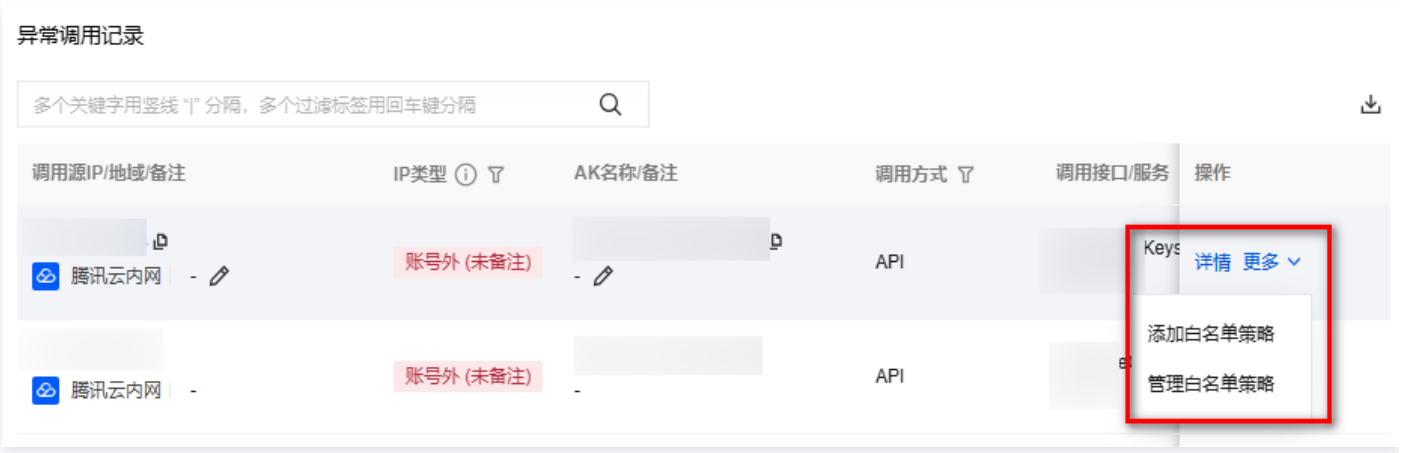


   - 查看异常调用记录，查看命中该告警的是哪个 IP、IP 类型、用什么方式使用了哪个 AK 调用了什么服务、调用成功和失败分别的次数、首次/最近调用时间，以及相关的 CAM 策略；根据 AK 权限策略配置对 AK 进行处置。

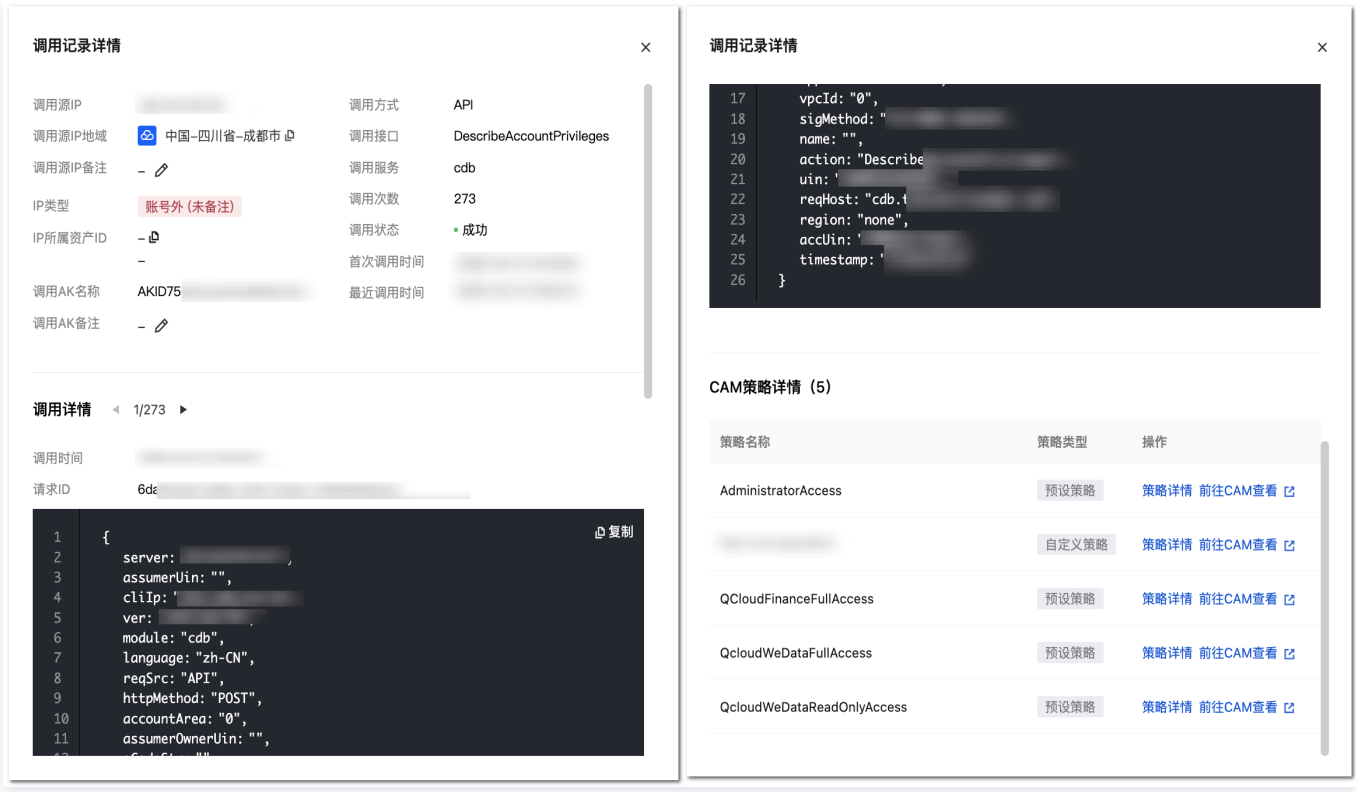
字段名	示例	说明
调用源IP/地域/备注	1.1.1.1 中国-北京 | 部门1AK	调用源 IP、所属地域与自定义备注。 • IP 内容支持一键复制。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”。
IP类型	• 账号外（未备注） • 账号内（未备注） • 账号外 • 账号内	• 账号内：在云安全中心 IP 资产列表中识别到的调用源 IP，有备注。 • 账号内（未备注）：在云安全中心 IP 资产列表中识别到的调用源IP，无备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 账号外：非账号内 IP 但有备注。
AK名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 AK 详情抽屉。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”。
调用方式	• API • 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。

调用接口/服务	DescribeAccountPrivileges cdb	调用的接口与接口所属服务。
用户角色/策略	角色：CSIG_Security 策略：1	该 AK 关联的角色与 CAM 策略，多个时显示数字，单击打开 CAM 策略详情弹窗。
调用状态/次数	• 成功（x次） • 失败（x次）	调用该 AK 成功/失败状态及次数。
首次/最近调用时间	• 2025-01-01 18:00:00 • 2025-01-12 18:00:00	首次与最近调用时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
IP 所属资产（ID/名称）	ins-xxx 机器1号	展示 AK 所属资产。

3. 在告警详情页面，选择所需调用源 IP，单击**详情/更多**。



- 详情
  - 展示调用信息，调用详情（包含时间、请求 ID、请求体；支持翻页），CAM 策略详情。



- 单击**策略详情**，展示其策略代码，支持复制；单击**前往 CAM 查看**，跳转至**访问管理 > 策略 > 具体策略详情**。


调用记录详情
17 vpcId: "0",
18 sigMethod: "
19 name: "",
20 action: "Describ
21 uin: "
22 reqHost: "cdb.
CAM策略详情
复制
{
statement: [
{
action: "*",
effect: "allow",
resource: "*"
},
],
version: "2.0"
}
QCloudFinanceFullAccess
预设策略
策略详情 前往CAM查看
QcloudWeDataFullAccess
预设策略
策略详情 前往CAM查看
QcloudWeDataReadOnlyAccess
预设策略
策略详情 前往CAM查看

- 更多

- 添加白名单策略：输入对应 IP、调用方式、AK、接口、返回码，填写说明请参见 策略管理 。

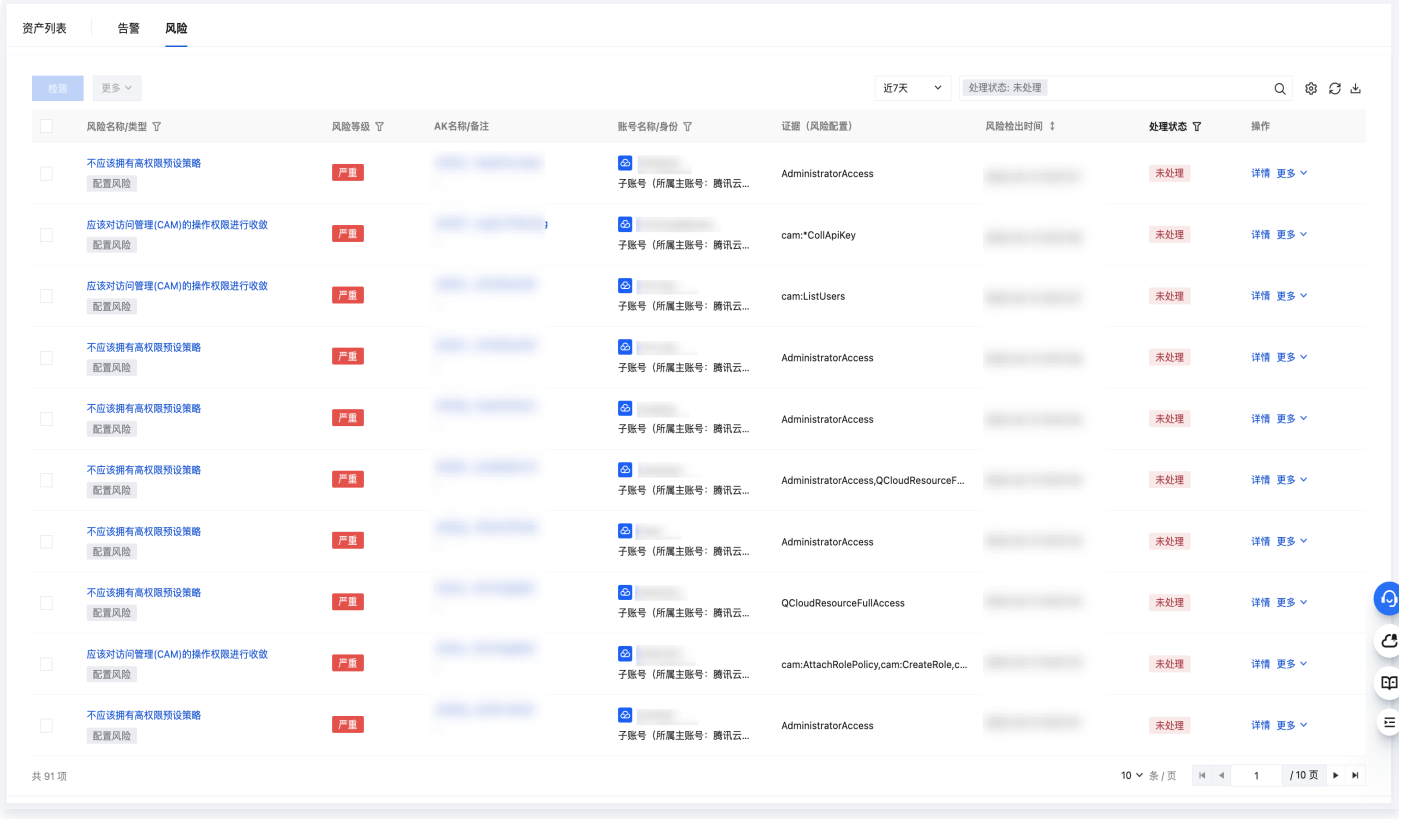
- 管理白名单策略：单击拉起**策略管理**抽屉，跳转至**策略管理 > 白名单策略**。

风险

最近更新时间：2025-04-22 16:18:12

风险列表

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在风险列表中，自动化扫描 AK 权限配置， 检查 AK 是否存在高权限策略，基于风险规则视角，查看配置风险描述与风险判定证据，并提供权限策略配置建议。



字段名	示例	说明
风险名称/类型	配置风险	单击拉起**风险详情**抽屉。
风险等级	• 严重 • 高危 • 中危 • 低危 • 提示 • 无效	基于腾讯云安全实践评定风险等级。
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 **AK 详情**抽屉。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”。
账号名称/身份	账号A 主账号/子账号（所属主账号：主账号 B）	• AK 所属云厂商与账号，若为子账号展示所属主账号信息。 鼠标悬浮查看账号 ID 与 APPID；支持筛选主账号/子账号。

风险检出时间	2025-01-12 18:00:00	风险检出时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
处理状态	• 未处理 • 已处置 • 已忽略	展示风险处理状态，手动完成标记，处理状态支持筛选。

3. 在风险列表中，选择所需风险，单击**详情/更多**。

操作类型		说明
详情		单击拉起**告警详情**抽屉，查看风险描述与判定证据。查看风险检测内容以及 AK 对应的配置内容，根据 AK 权限策略配置对 AK 进行加固。
更多	检测	单击后重新检测该规则。
	标记忽略	单击后处理状态变为“已忽略”。
	API 密钥管理	单击跳转至**访问管理** > **访问密钥** > API 密钥管理。

规则说明

实时监控 AK 泄露与异常调用，监测分为三类：黑客工具识别、github 泄露（github 合作 + IP检查等）、异常 IP 调用敏感接口等，具体规则见下表：

规则名称	规则说明
应该对私有网络(VPC)的操作权限进行收敛	应该对私有网络(VPC)的操作权限进行收敛，不应拥有如下敏感接口权限：CreateCcnRouteTables, CreateNatGatewayDestinationIpPortTranslationNatRule, CreateNatGatewaySourceIpTranslationNatRule, CreateSecurityGroup, CreateSecurityGroupWithPolicies, CreateVpcEndPoint, CreateVpcPeeringConnection
应该对向量数据库的操作权限进行收敛	应该向量数据库的操作权限进行收敛，不应拥有如下敏感接口权限：ModifyAccessKey
应该对容器服务的操作权限进行收敛	应该容器服务的操作权限进行收敛，不应拥有如下敏感接口权限：CreateClusterEndpoint, DeleteEKSCluster, DeleteEKSContainerInstances, DescribeClusterKubeconfig, DescribeClusterSecurity, DescribeEKSClusterCredential

应该对高性能计算平台的操作权限进行收敛	应该高性能计算平台的操作权限进行收敛，不应拥有如下敏感接口权限：ModifyInitNodeScripts
应该对云开发服务的操作权限进行收敛	应该对云开发服务的操作权限进行收敛，不应拥有如下敏感接口权限：CreateCloudUser, DescribeEnvs
应该对腾讯云自动化助手的操作权限进行收敛	应该对腾讯云自动化助手的操作权限进行收敛，不应拥有如下敏感接口权限：CreateCommand, CreateInvoker, EnableInvoker, InvokeCommand, RunCommand
应该对安全凭证服务的操作权限进行收敛	应该对安全凭证服务的操作权限进行收敛，不应拥有如下敏感接口权限：AssumeRole, GetFederationToken
应该对云函数的操作权限进行收敛	应该对云函数的操作权限进行收敛，不应拥有如下敏感接口权限：CreateFunction, Invoke
应该对云数据库(Redis)的操作权限进行收敛	应该对云数据库(Redis)的操作权限进行收敛，不应拥有如下敏感接口权限：ClearInstance, KillMasterGroup, ModifyInstanceAccount, ResetPassword
应该对云数据库(PostgreSQL)的操作权限进行收敛	应该对云数据库(PostgreSQL)的操作权限进行收敛，不应拥有如下敏感接口权限：ResetAccountPassword
应该对集团账号管理的操作权限进行收敛	应该对集团账号管理的操作权限进行收敛，不应拥有如下敏感接口权限：AddUserToGroup, CreateUserSyncProvisioning
应该对轻量应用服务器的操作权限进行收敛	应该对轻量应用服务器的操作权限进行收敛，不应拥有如下敏感接口权限：CreateKeyPair, ImportKeyPair, ResetInstancesPassword
应该对域名注册的操作权限进行收敛	应该对域名注册的操作权限进行收敛，不应拥有如下敏感接口权限：CreateDomainBatch, RegisterDomain, RenewAgentPay
应该对云解析(DNS)的操作权限进行收敛	应该对云解析(DNS)的操作权限进行收敛，不应拥有如下敏感接口权限：CreateDomainBatch, CreateShareDomains
应该对容器安全服务(TCSS)的操作权限进行收敛	应该对容器安全服务(TCSS)的操作权限进行收敛，不应拥有如下敏感接口权限：DeleteMachine
应该对主机安全(CWP)的操作权限进行收敛	应该对主机安全(CWP)的操作权限进行收敛，不应拥有如下敏感接口权限：DeleteMachine
应该对操作审计(CloudAudit)的操作权限进行收敛	应该对操作审计(CloudAudit)的操作权限进行收敛，不应拥有如下敏感接口权限：DeleteAudit, DeleteAuditTrack
应该对云数据库(MySQL)的操作权限进行收敛	应该对云数据库(MySQL)的操作权限进行收敛，不应拥有如下敏感接口权限：CloseWanService, CreateAccounts, CreateRoInstanceIp, DescribeAccounts, DescribeBackups, DescribeBinlogs, ModifyAccountPassword, ModifyDBInstanceSecurityGroups, OpenWanService
应该对访问管理(CAM)的操作权限进行收敛	应该对访问管理(CAM)的操作权限进行收敛，不应拥有如下敏感接口权限：AddUser, AddUserToGroup, AttachRolePolicy, AttachUserPolicy, CreateAccessKey, CreateApiKey, CreateCollApiKey, CreateOIDCConfig, CreateRole, CreateSAMLProvider, CreateServiceLinkedRole, CreateUserOIDCConfig, CreateUserSAMLConfig, EnableApiKey, GetProjectKey, ListAccessKeys, ListUsers, UpdateAccessKey, UpdateCollPassword, UpdateUser
应该对黑石物理服务器(BM)的操作权限进行收敛	应该对黑石物理服务器(BM)的操作权限进行收敛，不应拥有如下敏感接口权限：BuyDevices, CreateSpotDevice, ReloadDeviceOs, ResetDevicePassword, ShutdownDevices

应该对云服务器(CVM)的操作权限进行收敛	应该对云服务器(CVM)的操作权限进行收敛，不应拥有如下敏感接口权限：CreateKeyPair, ExportImages, ImportKeyPair, InquirePriceCreateInstances, InquiryPriceRunInstances, ModifyImageSharePermission, ModifySecurityGroupPolicys, ResetInstancesPassword, RunInstances, Adduser, UpdateUser
应该删除长期未使用AK密钥	应该删除长期未使用AK密钥，即使AK被禁用了也应该删除
不应该拥有高权限预设策略	AK不应该有AdministratorAccess、QCloudResourceFullAccess、QcloudCamFullAccess、QCloudFinanceFullAccess高权限预设策略

策略管理

最近更新时间：2025-04-22 16:18:12

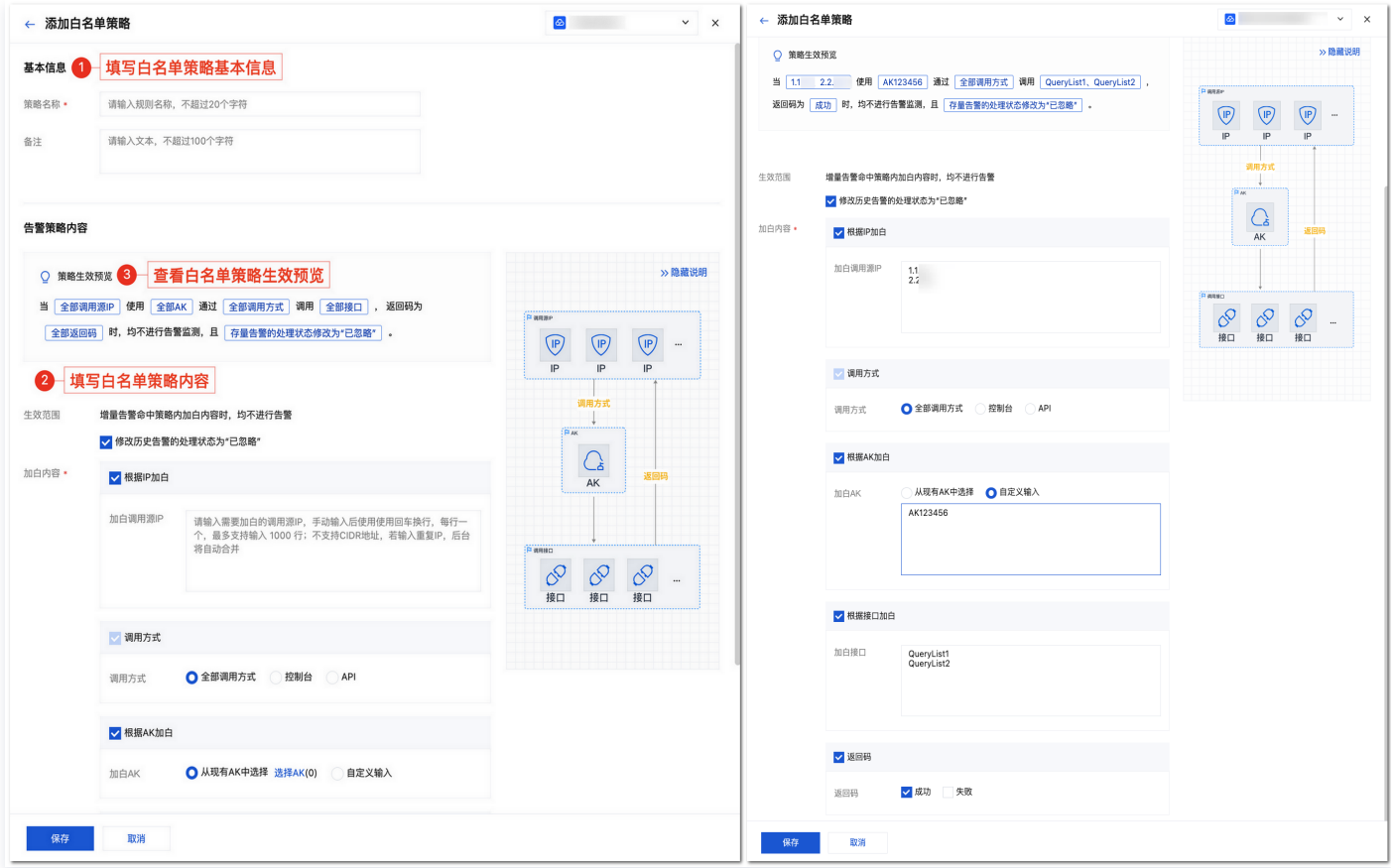
告警策略

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 单击右上角的**策略管理**，进入告警策略页面，对告警策略进行管理，目前支持开启/关闭具体的告警策略、快速定位命中策略的告警。

白名单策略

1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 单击右上角的**策略管理** > **白名单策略**，对白名单策略进行管理，支持基于调用源 IP、调用方式、AK、接口、返回码进行加白，并指定生效范围。

3. 单击**添加策略**，配置相关参数，单击**保存**。



内容名称	说明	示例

生效范围	• 默认为增量告警命中策略内加白内容时，均不进行告警。 • 可选择是否修改历史告警的处理状态为“已忽略”。	-
根据 IP 加白	勾选该文本框后，自定义需加白的调用源 IP；不勾选默认全部 IP；填写规则： • 多个 IP 换行隔开，每行一个。 • 最多支持输入1000行；不支持 CIDR 地址，若输入重复 IP，后台将自动合并。	1.1.1.1 2.2.2.2
调用方式	勾选该文本框后，选择需加白的调用方式；不勾选默认全部 IP。 • 全部调用方式。 • 控制台。 • API。	-
根据 AK 加白	勾选该文本框后，选择或自定义需加白的 AK；不勾选默认全部 AK；填写规则： • 多个 AK 换行隔开，每行一个。 • 最多支持输入 1000 行。	AK1 AK2
根据接口加白	勾选该文本框后，自定义需加白的接口；不勾选默认全部接口；填写规则： • 多个接口换行隔开，每行一个。 • 最多支持输入1000 行。	QueryList1 QueryList2
返回码	勾选该文本框后，选择需加白的返回码；不勾选默认全部。 • 成功。 • 失败。	-

DNS 威胁监测
功能简介

最近更新时间：2025-05-27 09:24:11

云安全中心基于腾讯云内网 VPC DNS 公网递归解析（腾讯云默认183.60.83.19/183.60.82.98的 DNS 服务器），对域名请求行为进行实时威胁监控，基于腾讯云独有的丰富情报识别**恶意或异常请求行为**，并进行告警。
建议您及时关注账号内主机**请求情况与相关告警**，可帮助您识别**矿池挖掘、恶意 C2、远程桌面工具、偏离基线行为**等，减少安全隐患，保障云上安全。

核心能力

- **海量情报精准匹配：**基于腾讯安全大数据挖掘能力和攻防经验模型化，提供专业威胁情报库，精准匹配百万情报，为您进行异常请求匹配，获取威胁信息。
- **恶意请求实时监控：**免部署一键接入，接入后将默认同步您的腾讯云内网 VPC DNS 公网递归解析日志信息，为您进行实时安全监控，更好了解 DNS 威胁。
- **异常行为基线监测：**重保、护网期间，支持对核心机器设定 DNS 解析行为基线，监测基线外异常行为。

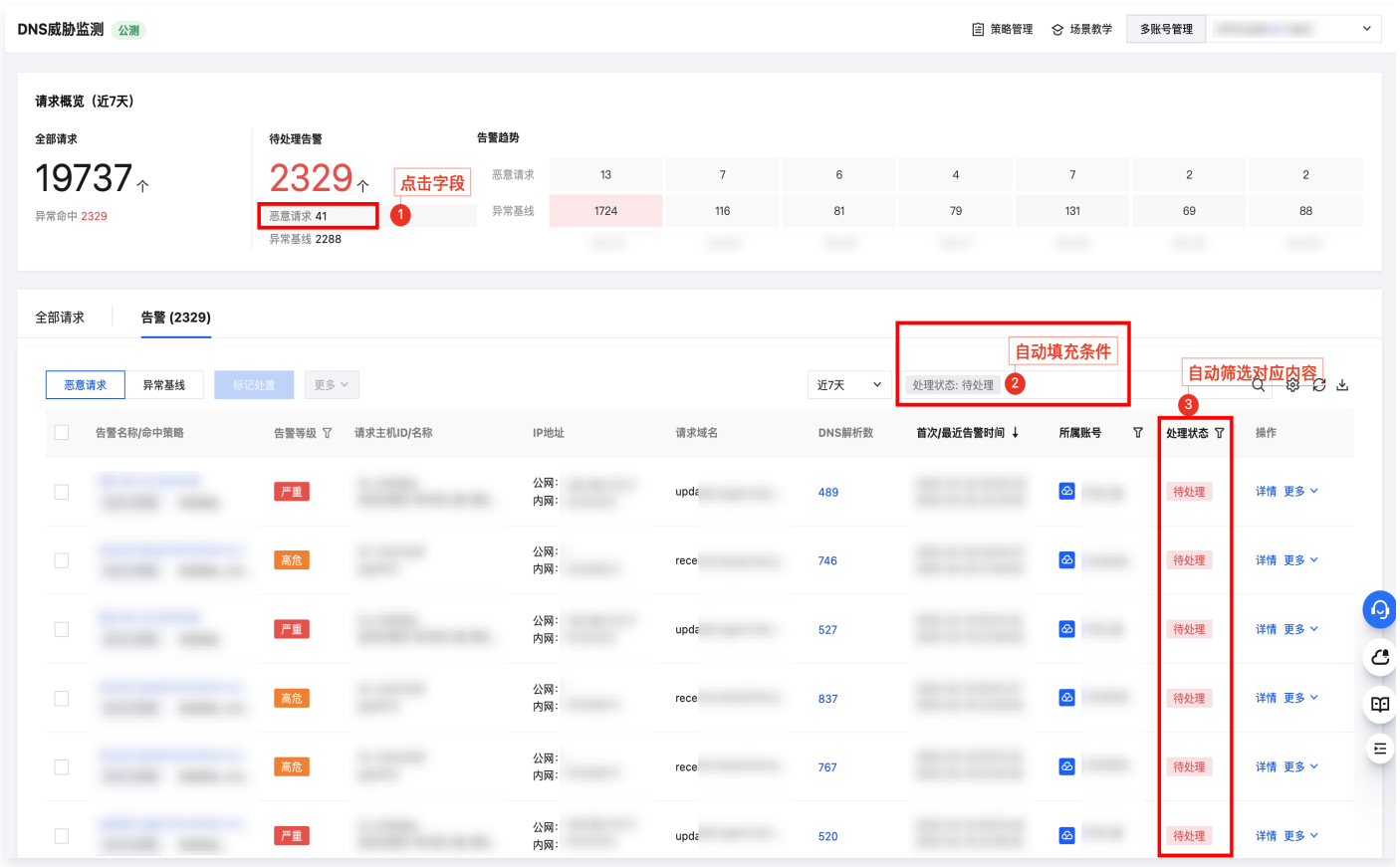
功能点梳理

功能板块		功能点	解决问题	操作指引
统计面板-请求概览		快速了解请求情况、待处理的恶意请求与异常基线告警等。	了解请求情况与异常占比，待处理的问题有多少，近期安全运营趋势怎样。	统计面板
全部请求		查看全部域名请求情况、关联异常分析。	梳理有多少主机请求了哪些域名，是否有命中异常。 关键时期可以进行历史全量域名请求记录的回溯，协助进行溯源排查。	全部请求
告警列表	恶意请求	实时监控恶意域名请求，基于系统与自定义告警规则视角，查看告警内容、机器详细信息，并提供说明&修复方案。	识别矿池挖掘、远控木马、恶意 C2、远程桌面工具等，配合主机/容器安全定位进程，引导处置	恶意请求
	异常基线	支持设定行为基线策略，编辑监测的主机与域名范围。当发生行为基线范围外的请求时，产生异常告警。可查看告警内容、机器详细信息。	对核心机器设定 DNS 解析行为基线，监测基线外异常行为。	异常基线
策略管理	告警策略	管理系统告警策略。	管理需要关注的告警策略，并基于业务需要自定义白名单。	策略管理
	白名单策略	管理告警白名单，可对白名单进行增删改查，基于主机、域名进行加白。		

统计面板

最近更新时间：2025-04-24 15:11:02

1. 登录 云安全中心控制台，在左侧导览中，单击 **DNS 威胁监测**。
2. 在 DNS 威胁监测页面，请求概览模块分为以下三种：
   - **全部请求：**统计近7天，当前腾讯云账号下主账号与子账号全部请求。
   - **待处理：**统计近7天，当前腾讯云账号下主账号与子账号中处理状态为“待处理”的恶意请求&异常基线数量。
   - **告警趋势：**统计近7天，每天新增的恶意请求&异常基线数量。
3. 在 DNS 威胁监测页面，单击**关注的字段**，下方列表搜索框中自动添加条件并筛选出对应内容。



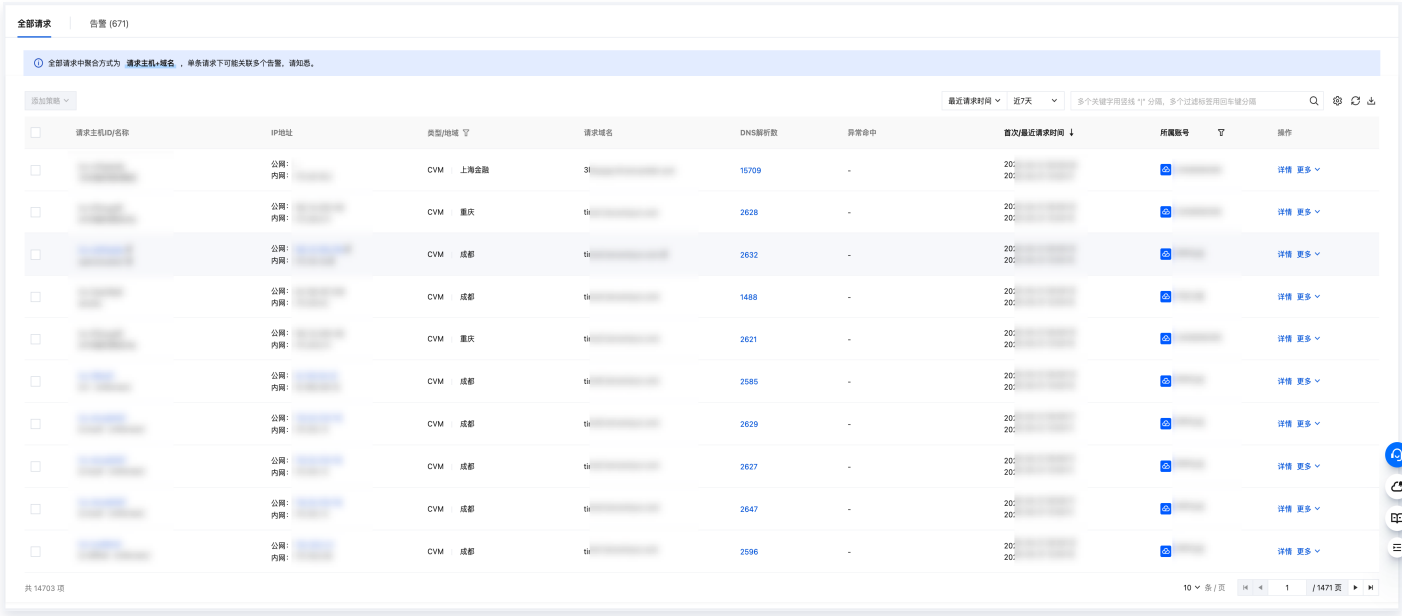
全部请求

最近更新时间：2025-04-24 15:11:02

全部请求列表

1. 登录 云安全中心控制台，在左侧导览中，单击 **DNS 威胁监测**。
2. 在 **DNS 威胁监测 > 全部请求列表**中，查看请求内容（主机信息、请求域名）、异常命中判定等。

> **说明：**
> 列表数据聚合逻辑：一天内同一账号下，同一主机请求同一域名聚合为一条数据。



字段名	示例	说明
请求主机 ID/名称	ins-xxx 主机 A	发起请求的主机，单击新开页面进入**主机资产详情**
IP 地址	公网：x.x.x.x 内网：x.x.x.x	发起请求主机的公网与内网 IP 地址
类型/地域	CVM | 地域 A	发起请求主机的类型与所属地域，当前仅支持 CVM
请求域名	xxx.com	主机请求的域名
DNS 解析数	-	单击跳转**日志分析**，筛选对应日志
异常命中	异常基线 恶意请求	该请求是否有命中相关
首次/最近请求时间	2025-01-01 18:00:00 2025-01-12 18:00:00	• 格式：YYYY-MM-DD HH:MM:SS • 支持排序

3. 在全部请求列表中，选择所需请求，单击**详情/更多**。

操作类型		说明
详情		单击拉起 请求详情 抽屉。
更多	添加恶意请求策略	单击打开**添加恶意请求策略**弹窗，并填充对应内容。添加后若命中该策略将产生恶意请求告警。
	加入行为基线策略	单击打开**加入行为基线策略**弹窗，并填充对应内容。加入后当发生行为基线策略范围外的请求时，产生异常基线告警。

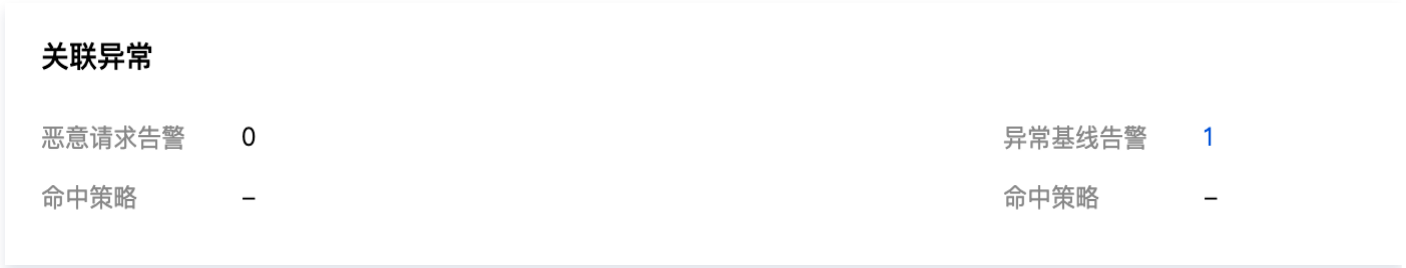
请求详情

在请求详情抽屉页面，查看请求信息、请求详情与关联异常情况。

- 查看请求基本信息

- 查看请求详情：查看哪些主机访问了指定域名，并提供主机的详细信息。要获取进程、命令行、MD5等更多信息，请升级至主机安全 专业版或旗舰版。

- **查看关联异常：查看恶意请求、异常基线的告警关联情况及其命中策略。**



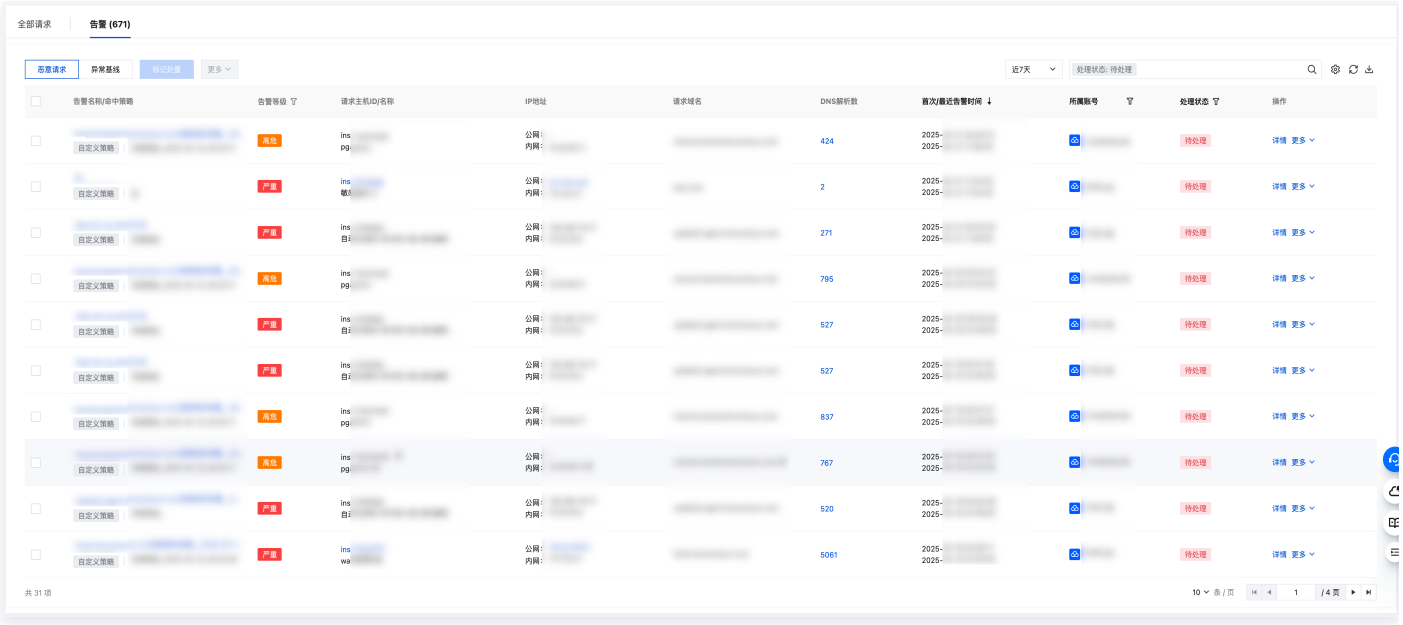
恶意请求

最近更新时间：2025-04-24 15:11:02

恶意请求列表

1. 登录 云安全中心控制台，在左侧导览中，单击 **DNS 威胁监测**。
2. 在 **DNS 威胁监测 > 告警列表 > 恶意请求**中，查看告警内容（名称、等级），请求内容（主机信息、请求域名）处理状态等。

> **说明：**
> 列表数据聚合逻辑：一天内同一账号下，同一告警。



字段名	示例	说明
告警名称/命中策略	• 系统策略 • 自定义策略	单击拉起**告警详情**抽屉
告警等级	• 严重 • 高危 • 中危 • 低危 • 提示 • 无效	基于腾讯云安全实践评定告警等级
请求主机ID/名称	ins-xxx 主机 A	发起请求的主机，单击新开页面进入**主机资产详情**
IP地址	公网：x.x.x.x 内网：x.x.x.x	发起请求主机的公网与内网 IP 地址
请求域名	xxx.com	主机请求的域名
DNS解析数	-	单击跳转**日志分析**，筛选对应日志

首次/最近告警时间	2025-01-01 18:00:00 2025-01-12 18:00:00	• 格式：YYYY-MM-DD HH:MM:SS • 支持排序
处理状态	• 未处理 • 已处置 • 已忽略	展示告警处理状态，手动完成标记，处理状态支持筛选

3. 在恶意请求列表中，选择所需请求，单击**详情/更多**。

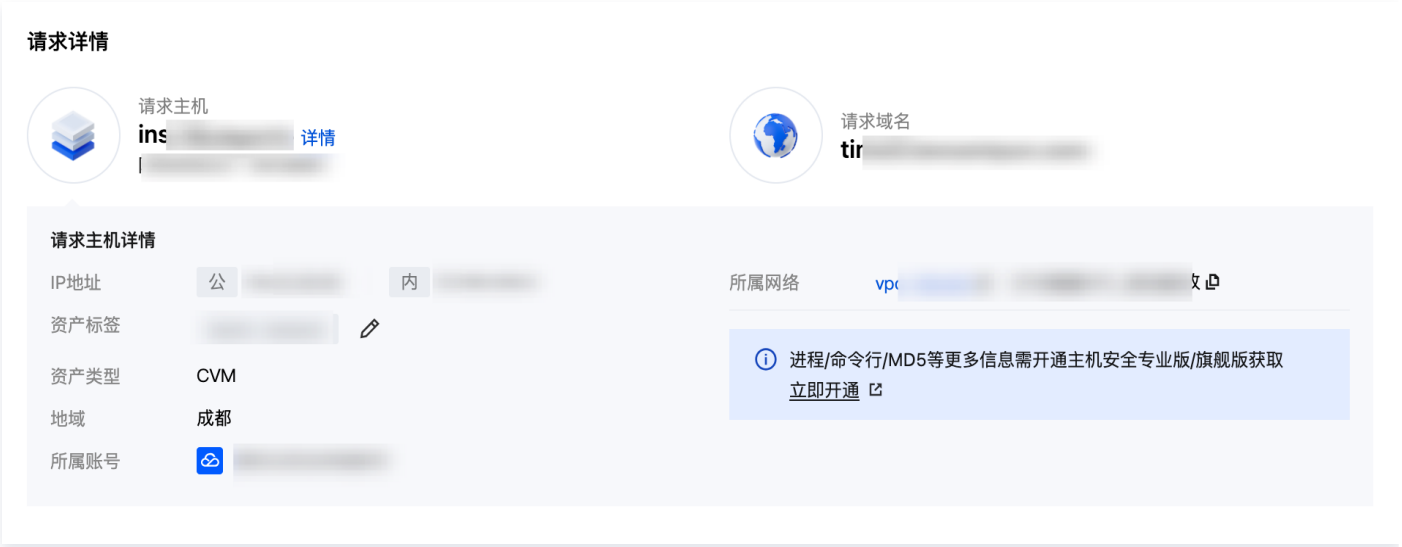
操作类型		说明
详情		单击拉起 告警详情 抽屉。
更多	标记处置	单击后处理状态变为“已处置”。
	标记忽略	单击后处理状态变为“已忽略”。
	添加白名单策略	单击拉起**添加白名单策略**抽屉，并填充对应 AK。

恶意请求详情

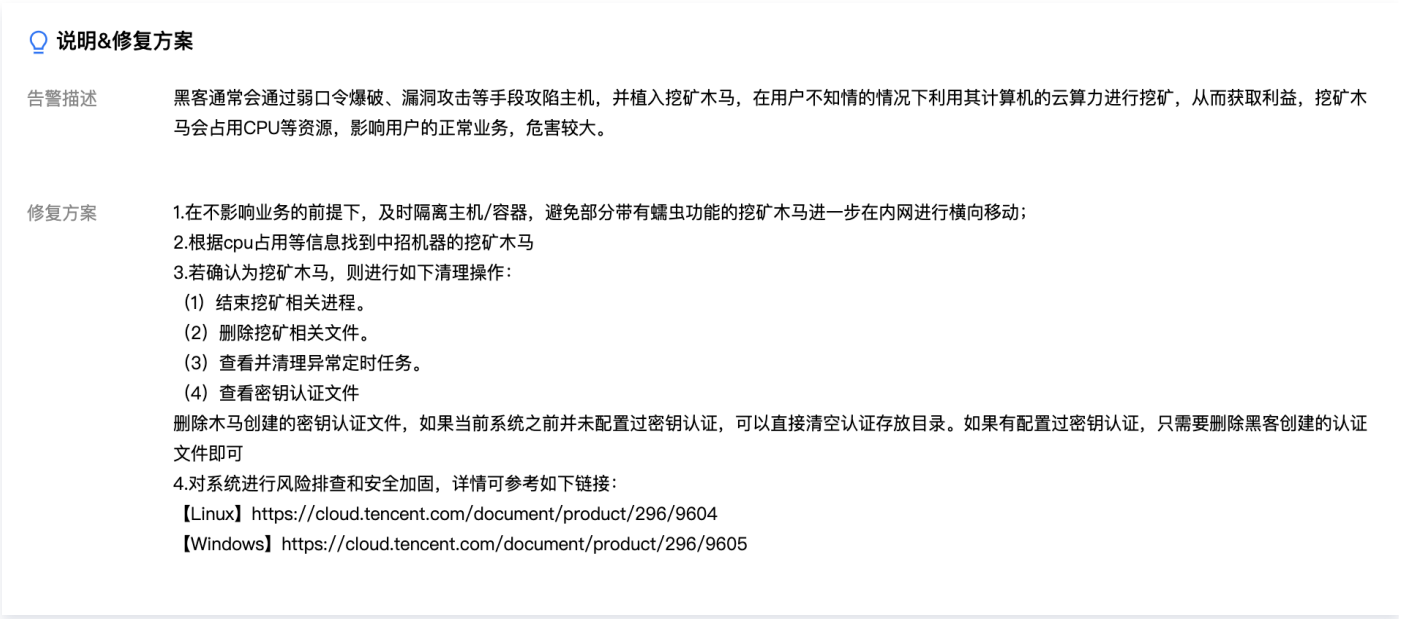
在告警详情抽屉页面，查看告警信息、请求详情与说明&修复方案。

- 查看告警基本信息。

- **查看请求详情：查看哪些主机访问了指定域名，并提供主机的详细信息。要获取进程、命令行、MD5等更多信息，请升级至主机安全 专业版或旗舰版。**



- **查看说明&修复方案：按照指引处置告警。**



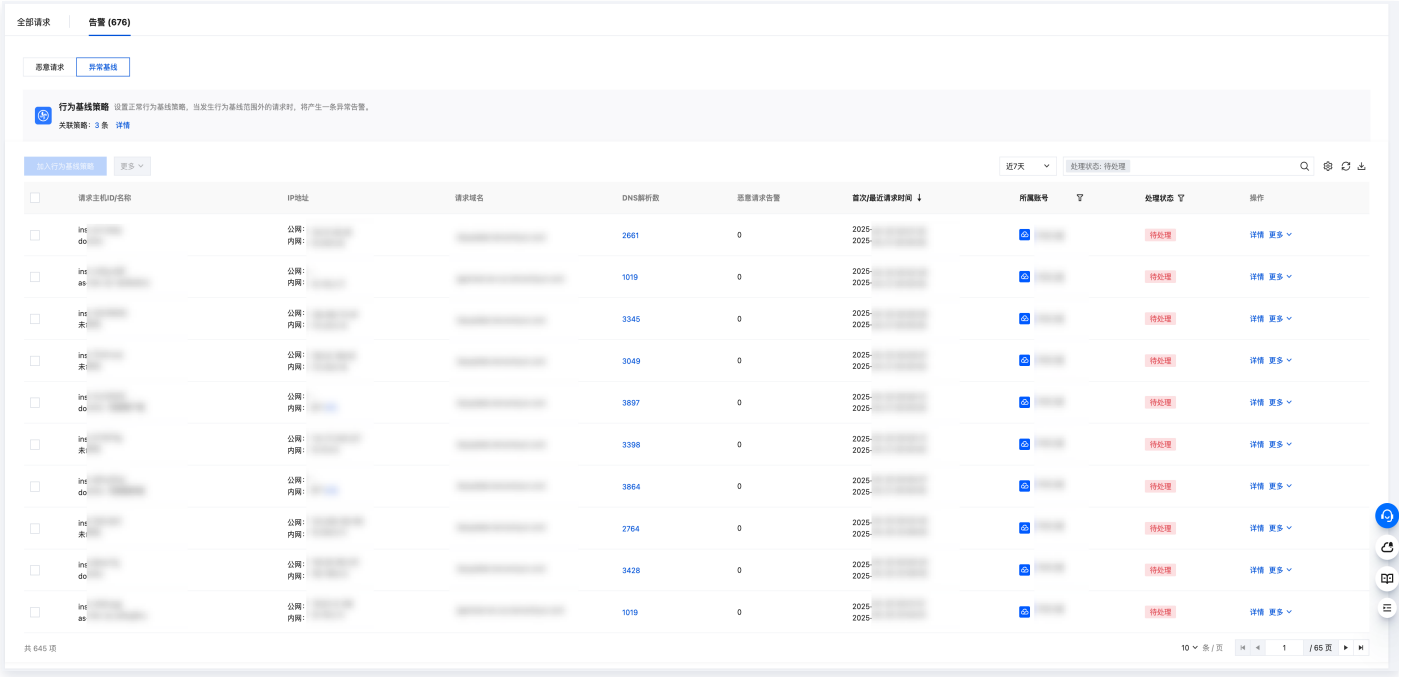
异常基线

最近更新时间：2025-04-24 15:11:02

异常基线列表

1. 登录 云安全中心控制台，在左侧导览中，单击 **DNS 威胁监测**。
2. 在 **DNS 威胁监测 > 告警列表 > 异常基线**中，查看偏离基线的请求行为（请求内容：主机信息、请求域名），处理状态等。

> **说明：**
> 列表数据聚合逻辑：一天内同一账号下，同一主机请求同一域名聚合为一条数据。



字段名	示例	说明
请求主机 ID/名称	ins-xxx 主机 A	发起请求的主机，单击新开页面进入**主机资产详情**
IP 地址	公网：x.x.x.x 内网：x.x.x.x	发起请求主机的公网与内网 IP 地址
请求域名	xxx.com	主机请求的域名
DNS 解析数	-	单击跳转**日志分析**，筛选对应日志
恶意请求告警	-	该偏离基线行为是否命中情报
首次/最近请求时间	2025-01-01 18:00:00 2025-01-12 18:00:00	• 格式：YYYY-MM-DD HH:MM:SS • 支持排序
处理状态	• 未处理 • 已处置 • 已忽略	展示告警处理状态，手动完成标记，处理状态支持筛选

3. 在异常基线列表中，选择所需请求，单击**详情/更多**。

操作类型		说明
详情		单击拉起 告警详情 抽屉。
更多	加入行为基线策略	单击打开**加入行为基线策略**弹窗，并填充对应内容。加入后当发生行为基线策略范围外的请求时，产生异常基线告警。
	标记处置	单击后处理状态变为“已处置”。
	标记忽略	单击后处理状态变为“已忽略”。
	创建告警策略	单击拉起**添加策略--恶意请求**抽屉，并填充生效主机、生效域名。添加后若命中该策略将产生恶意请求告警。

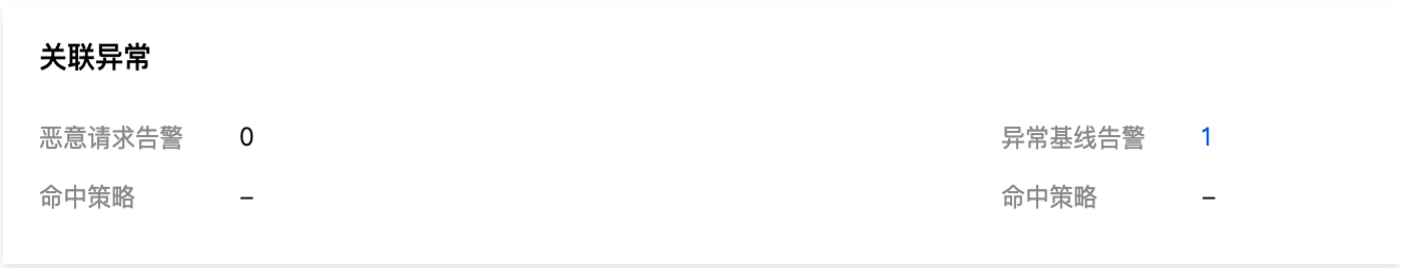
异常基线详情

在请求详情抽屉页面，查看请求信息、请求详情与关联异常情况。

- 查看请求基本信息。

- 查看请求详情：查看哪些主机访问了指定域名，并提供主机的详细信息。要获取进程、命令行、MD5等更多信息，请升级至主机安全 专业版或旗舰版。

- **查看关联异常：查看恶意请求、异常基线的告警关联情况及其命中策略。**



策略管理

最近更新时间：2025-04-24 15:11:02

恶意请求

1. 登录 云安全中心控制台，在左侧导览中，单击 DNS 威胁监测。
2. 在 DNS 威胁监测页面，单击右上角的策略管理。
3. 在恶意请求页签，可以对告警策略进行管理，目前支持开启/关闭具体的告警策略、自定义策略、快速定位命中策略的告警。

4. 在恶意请求页签，单击添加策略，配置相关参数，单击保存。

异常基线

1. 登录 云安全中心控制台，在左侧导览中，单击 **DNS 威胁监测**。
2. 在 DNS 威胁监测页面，单击右上角的**策略管理**。
3. 在异常基线页签，对行为基线策略进行管理，目前支持开启/关闭具体的策略、编辑策略。

> **说明：**
> 策略说明：一个账号仅支持配置1条行为基线策略，在策略中添加您判定为正常的请求主机及域名，策略生效后进行非白即黑判定，对所有基线策略外产生的请求生成告警。

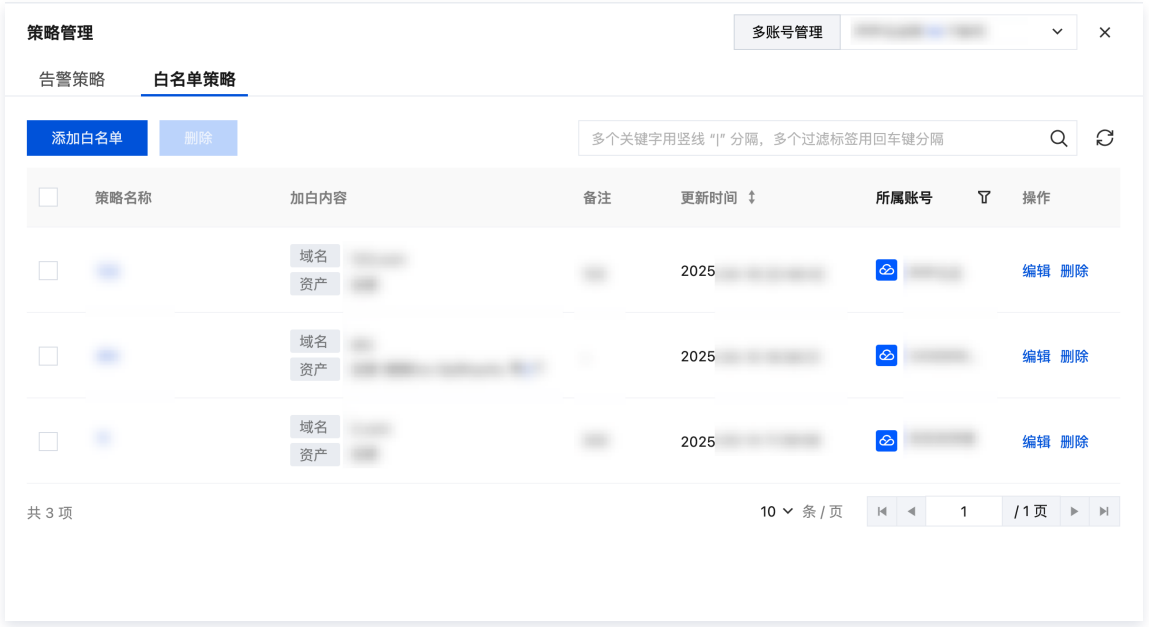
4. 在异常基线页签，单击行为基线策略的 ，修改生效主机/域名，单击**保存**。

说明：

- 选择生效主机：建议选择核心机器设定 DNS 解析行为基线，监测基线外异常行为。
- 选择生效域名：展示在 X 天内请求过的域名，选择需要加入行为基线的域名。建议选择全部未命中情报的域名（命中情报：命中腾讯云主机安全恶意域名库的域名）。

白名单策略

1. 录 云安全中心控制台，在左侧导览中，单击 **DNS 威胁监测**。
2. 在 DNS 威胁监测页面，单击右上角的**策略管理 > 白名单策略**。
3. 在白名单策略页面，对白名单策略进行管理，支持基于资产、域名进行加白。



4. 在白名单策略页面，单击添加白名单，配置相关参数，单击**保存**。

用户行为分析（UEBA）

最近更新时间：2025-05-28 18:07:11

用户行为分析（UEBA）功能提供了对云用户操作行为和云 API 调用的可视化审计与监控，能够针对 AKSK 异常调用、高风险接口调用、用户高风险操作、未授权服务使用、权限提升等风险行为进行检测和告警，识别因用户异常行为和风险 API 调用等引起的安全风险。

> **模块可见范围说明：**
> 用户行为分析（UEBA）功能仅供存量用户使用，新用户如需相关能力，可以使用 云 API 异常监测 功能，相关文档：云 API 异常监测-功能简介 。

功能特性

- 审计日志接入：通过多云多账户功能模块，可以获取云账户对应的用户列表和云外用户信息。通过操作审计日志，可以获取所有云用户的行为记录，并识别用户行为字段。此外，还能对云用户的操作行为和云 API 调用日志进行可视化监控和实时审计。
- 风险检测：对 AKSK 异常调用、高危接口调用、用户高危操作、未授权服务使用、权限提升等风险行为进行检测和告警。同时，支持用户自定义启用或禁用检测规则，并自定义添加检测策略。
- 安全可视化：从异常行为和异常账号等方面展示近7天内检测到的风险数据，客户可以通过对比数据快速了解风险趋势，并及时进行风险管理。

用户概况

1. 登录 云安全中心控制台 ，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在用户行为分析（UEBA）页面，支持对您所有用户的行为分析，用户包括您的主账号、子账号、协作者。

3. 单击**配置自定义用户**，您可以通过选择一个日志类型来识别第三方日志中的用户信息。

> **注意：**
> 此操作需要 配置日志接入 才能进行。

4. 在自定义用户对话框中，配置日志类型、用户 ID 等参数。

参数名称	说明
日志类型	在完成 配置日志接入 后，用户可以在此部分选择要为其添加策略的自定义用户，以审计所需的日志类型。 日志类型包括云防火墙的访问控制日志、操作日志、流量日志、入侵防御日志、零信任防护日志，Web 应用防火墙的攻击日志、访问日志，主机安全的客户端上报日志、云安全中心的内容风险日志、风险服务暴露日志、弱口令风险日志、配置风险日志、漏洞风险日志，SaaS 化堡垒机的资产登录日志、产品登录日志，或其他的自定义日志。
用户 ID	选择代表用户 ID 的字段。
用户名称	选择代表用户名称的字段，可不选。
操作对象	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的对象，建议选择服务、产品、资源、实例、接口等信息，允许为空。
操作方式	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的方式，建议选择密钥、AKSK 等信息，允许为空。 配置完成之后，自定义用户部分的用户数据会根据配置信息进行刷新。

5. 单击**确定**，配置完成之后，自定义用户部分的用户数据会根据配置信息进行刷新。

行为概况

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在行为概况模块中，使用功能之前，需先接入日志，单击**立即接入**。

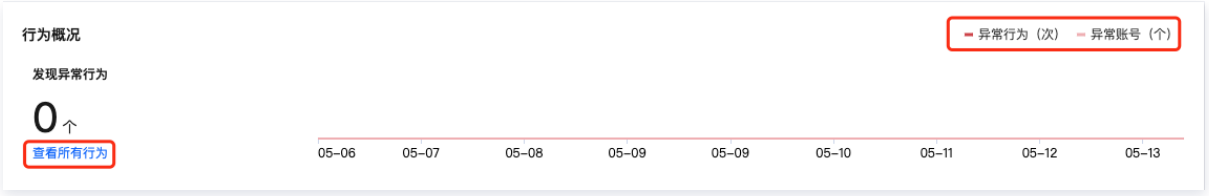
3. 在接入日志源对话框中，日志来源可选择操作o和自定义日志来源。

> **说明：**
> 如果在日志分析已经已经接入了这两类日志，则在用户行为分析（UEBA）功能模块可免去此部分的配置工作，直接添加策略。

日志来源	参数名称	说明
云审计	存储时长	默认为180天，可选择7天、30天、60天、90天或180天。

	接入方式	默认为通过跟踪集接入。
	跟踪集	仅展示可用且存储到 COS 的跟踪集，如已关闭，请先前往 COS 产品开启。
自定义日志来源	日志来源名称	需自定义日志来源名称。
	存储时长	可选择7天、30天、60天、90天或180天。
	接入方式	默认为通过自有 COS 桶接入。
	COS 存储桶	将所需接入的日志写入所选的 COS 存储桶，并配置权限，允许云安全中心服务角色进行读取。云安全中心将自动定时读取日志文件。还可以通过 提交工单 来定制读取方式，或前往 COS 产品页面创建一个新的存储桶。
	存储目录	为提升读取性能，建议在选定的目录下，进一步按照 yyyy/mm/dd 的格式组织日志文件路径，我们会根据日历自动读取对应自然日的文件； 日志格式支持 J格式，用‘/n’分割行，支持 gzip 压缩。
	日志样例	建议您输入日志样例供系统参考。系统会根据输入的样例进行字段解析，您可以进一步查看并选择指定字段及排序操作，这将提升日志的读取性能及解析的正确性。
	时间戳	选择日志样例及其对应的时间戳格式。

4. 单击**确定**后，系统将完成日志接入。接下来，系统策略和用户自定义策略会根据实时接入的日志，对异常行为和异常账号进行审计。如果发现异常行为，将更新下图中的异常行为数据和趋势图。单击**查看所有行为**，可跳转至日志分析查看日志详情。



查看策略

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在用户行为分析（UEBA）列表中，提供系统策略来检测异常行为和异常账号，可针对 AKSK 异常调用、高危接口调用、用户高危操作、未授权服务使用、权限提升等风险行为进行检测告警。

参数名称	说明
策略 ID	系统默认生成。
策略名称	系统策略由产品后台定义；用户自定义策略由用户定义。
策略类型	包括系统策略和自定义策略。

告警等级	包括严重、高危、中危、低危和提示。
策略内容	解释策略的检测内容。
开关	用户可自定义开启或关闭此条策略。
命中次数	统计近7天的策略命中纪录。单击可跳转告警中心查看告警详情，告警来源为用户行为分析（UEBA）。
操作	系统策略不允许编辑和删除。用户自定义策略可编辑或删除策略。

添加策略

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在用户行为分析（UEBA）页面，单击**添加策略**，可自定义用户行为分析策略。
3. 在自定义策略页面，配置相关参数，单击**确定**。

参数名称	说明
策略名称	用户自定义策略名称，不超过20个字符。
用户类型	云账号或自定义用户。 • 选择云账号时，可选择的日志类型包括云审计读操作日志和云审计写操作日志。 • 选择自定义用户时，可选择的日志类型即自定义用户中配置的日志类型。
发生时间	选项包括每10分钟、每小时、每天、每周、每月。
发生事件	可按语句检索或过滤检索进行配置。
告警名称	可选用户异常行为。

告警等级	包括严重、高危、中危、低危和提示。
操作者	请在当前的日志字段中，选择最多3个字段用于体现操作者的信息，建议选择 IP、账号、用户相关字段，不允许为空。
操作对象	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的对象，建议选择服务、产品、资源、实例、接口等信息，允许为空。
操作方式	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的方式，建议选择密钥、AKSK 等信息，允许为空。

大模型态势管理

最近更新时间：2025-04-01 10:13:13

大模型态势管理为您提供大模型组件资产识别、大模型组件风险识别、网络攻击预警等能力。您可以通过本页面查看云账号下存在的大模型组件，并了解其可能存在的安全风险及可能正在遭受的网络攻击。资产与风险识别来源于云安全中心体检能力及主机安全的检测能力，网络攻击数据来源于主机安全。云安全中心将在您购买了主机安全的情况下，读取相关数据。

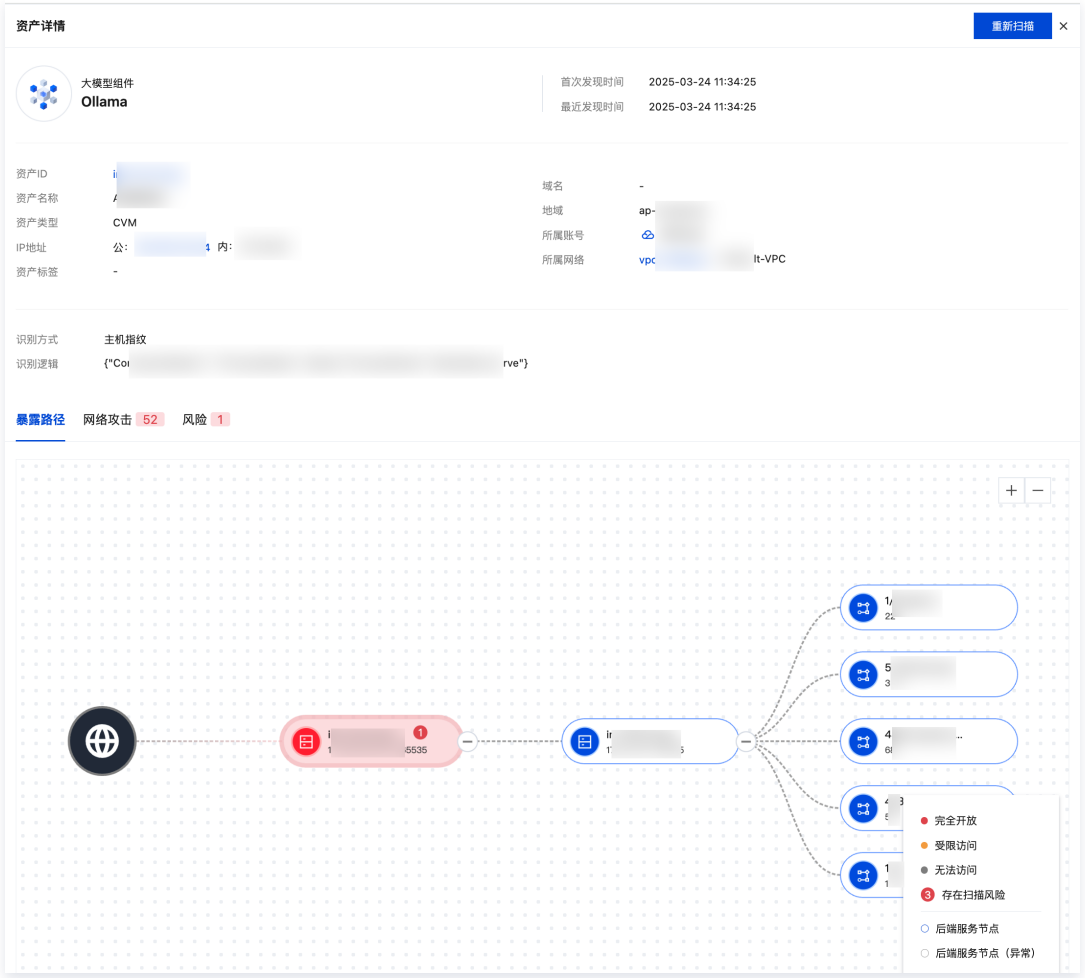
前提条件

已购买 云安全中心高级版 。

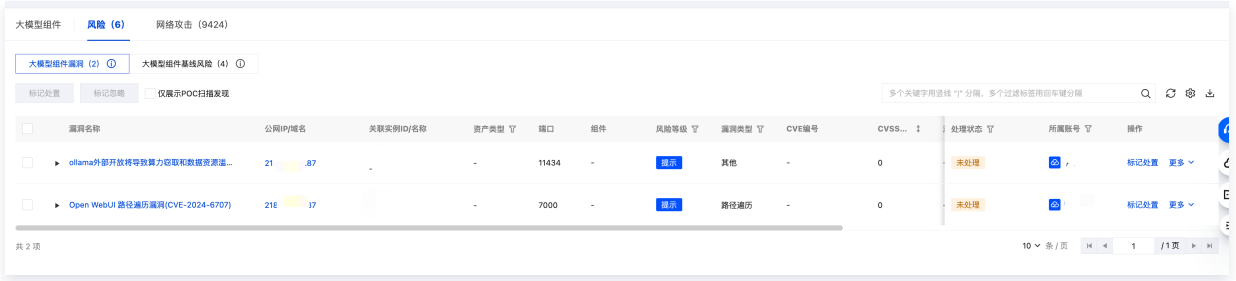
查看功能

1. 登录 云安全中心控制台 ，在左侧导览中，单击**大模型态势管理**。
2. 在大模型态势管理页面，支持查看**大模型组件资产**、**大模型组件风险**、**网络攻击**。

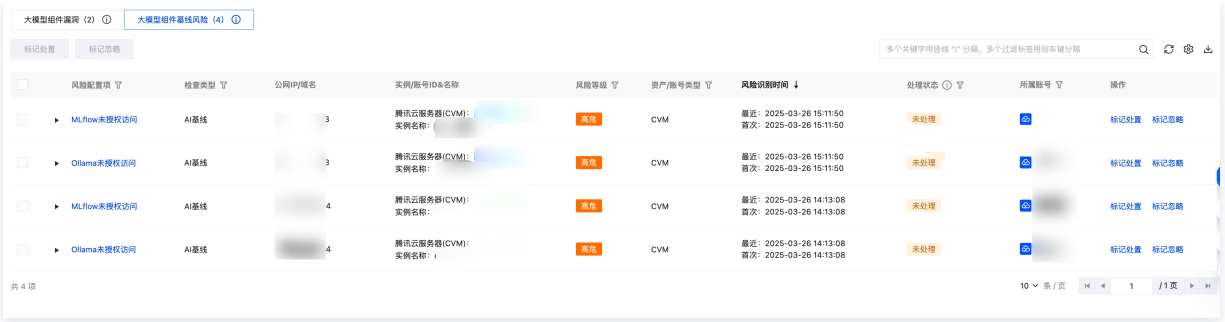
3. 在**大模型资产**列表中，您可以查看已识别的组件信息、资产实例信息、识别方式等。选择您关心的数据，单击**详情**可查看具体的组件识别原因、暴露路径 、网络攻击、风险等。



4. 切换至**风险**标签页，您可以查看识别的大模型组件相关风险，风险包含**漏洞风险**、**基线风险**。
   - **漏洞风险**：包含网络扫描和主机安全识别的大模型组件相关漏洞。



   - 切换至**基线风险**，可查看通过主机基线检测发现的风险，基线风险是指通过主机安全检测的大模型组件配置不当等风险。



5. 切换至**网络攻击**标签页，您可以查看资产正在遭受 AI 类漏洞攻击的详情。选择目标的数据，单击**详情**，可以查看网络攻击的详细数据。


大模型资产
风险（152）
网络攻击（9157）
攻击详情
未处理
标记处置
标记忽略
网络攻击告警
攻击状态
尝试攻击
最近攻击时间
2025-03-24 05:24:45
攻击次数
1次
攻击源IP
攻击源地址
中国 江苏省 南京市
漏洞名称
dirk1983/chatgpt 服务器端请求伪造 (SSRF) 漏洞(CVE-2024-27564)
漏洞CVE编号
CVE-2024-27564
漏洞全网攻击热度
服务进程
异常行为
-
攻击数据包
影响主机
大模型资产
Ollama
资产类型
CVM
域名
-
IP地址
资产标签
-
地域
广州
所属账号
所属网络
危害描述
发现主机上存在网络攻击行为，您的主机可能有入侵失陷风险。
网络攻击行为通常是通过从网络侧开放端口机器上，利用漏洞进行入侵，攻击成功后可能进一步进行提权、反弹shell等行为。
解决方案
1.建议相关应用部署WAF防护/云防火墙防护/开启漏洞防御
2.如果端口应用不需要对外，通过云防火墙或者安全组限制端口对公网暴露
3.若该告警为自行扫描，则可通过添加来源IP到白名单来过滤告警

日志投递（支持多账号多产品多日志）

最近更新时间：2024-08-05 14:26:42

功能背景

将接入云安全中心的多款产品日志集中并归一化后通过控制台投递至消息队列，便于存储数据或联合其它系统消费数据，助力挖掘日志数据价值，满足用户日志运维诉求。启用日志投递后，将采集到的日志投递至对应的消息队列。

应用场景

日志存储

根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》等相关法律法规的规定，企业需要对网络安全事件进行记录和存储，并且日志存储时长不少于6个月。这是为了保障企业的信息安全和网络安全，防止安全事件的发生和滋生。

离线分析

将日志投递至 Kafka/CLS 后，企业可以接入其他系统进行离线分析，进一步管控原始日志，协助企业对安全事件进行深入分析和研究，发现安全事件的根本原因和漏洞，提高安全事件的处理能力和水平。

日志投递至Kafka

在日志分析页面，您可配置云安全中心接入的不同日志类型分别投递到指定 Ckafka 实例的不同 Topic 中。

> **前提条件：**
> 为了将日志投递至消息队列，需要先购买云安全中心旗舰版，并将相关产品的日志接入云安全中心。如果需要使用 Ckafka 公网域名或 Ckafka 支撑环境接入两种网络接入方式之一，需要先前往创建腾讯云消息队列 CKafka 实例 。

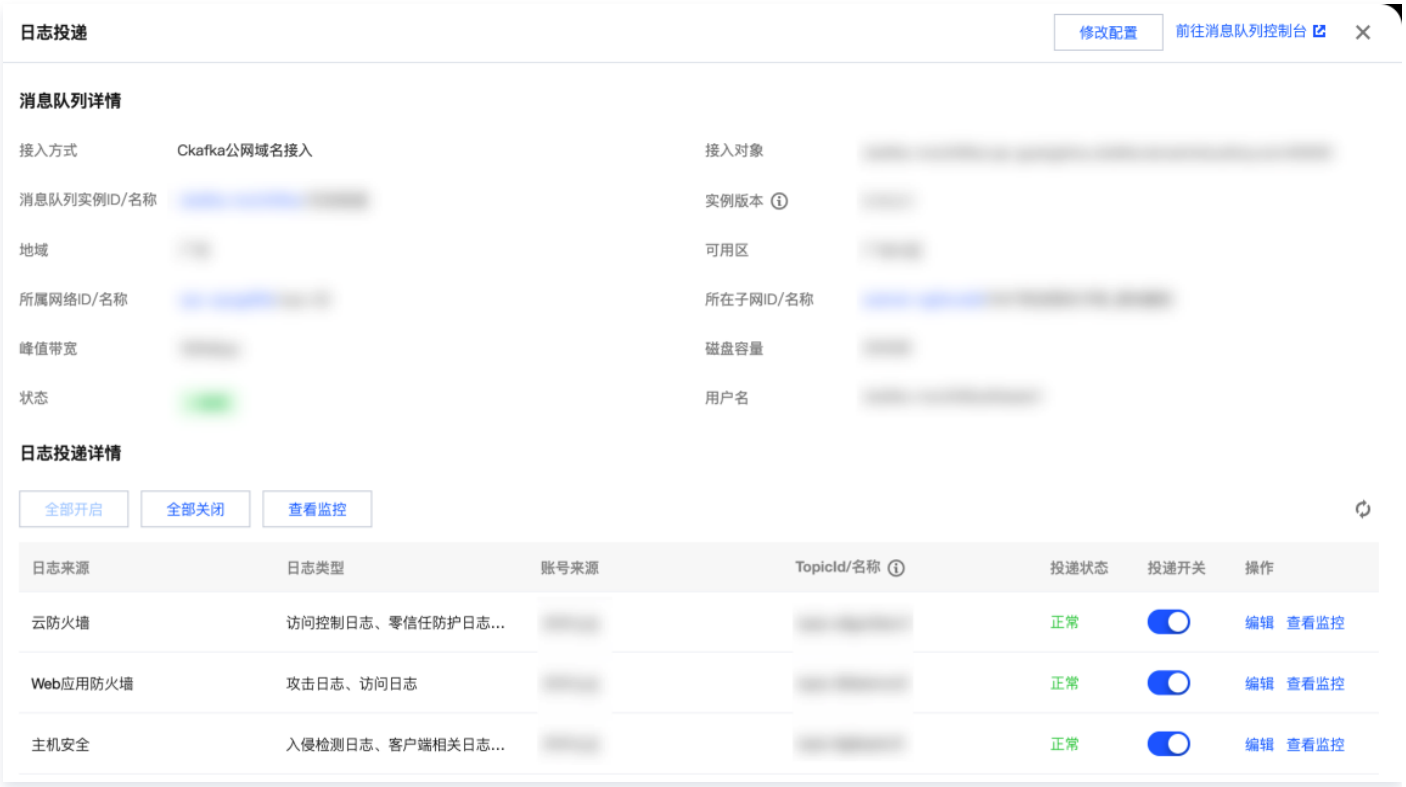
Ckafka 公网域名接入

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击**日志投递 > 投递至 kafka**。
3. 在投递至 kafka页面，云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、已接入云安全中心的日志来源，选择 **Ckafka 公网域名接入**，配置相关参数。

参数名称	说明
网络接入方式	Ckafka 公网域名接入。
TLS 加密	选择是否开启 TLS 加密。
消息队列所属账号	投递目标所属账号。
消息队列实例	云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、选择所需消息队列实例。
公网域名接入	选择所需公网域名。
用户名	请输入所选消息队列实例的用户名。
密码	请输入所选消息队列实例的密码。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
Topic ID/名称	选择所需 Topic。

操作	• 新增：单击**新增日志投递配置**，支持新增多个日志来源。 • 删除：单击目标日志操作列的**删除**，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。 • 编辑：如非首次配置日志投递，则支持在日志投递页面，单击**修改配置**，修改相关日志投递。

4. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的消息队列。
5. 在日志投递页面，支持查看同步接入方式、接入对象、消息队列状态、用户名等消息队列详情，以及日志来源、日志类型、账号来源（多账号下）、Topic ID/名称、Topic 投递状态、投递开关等信息，允许修改消息队列、Topic 配置等信息，查看消息队列和各 Topic 状态。

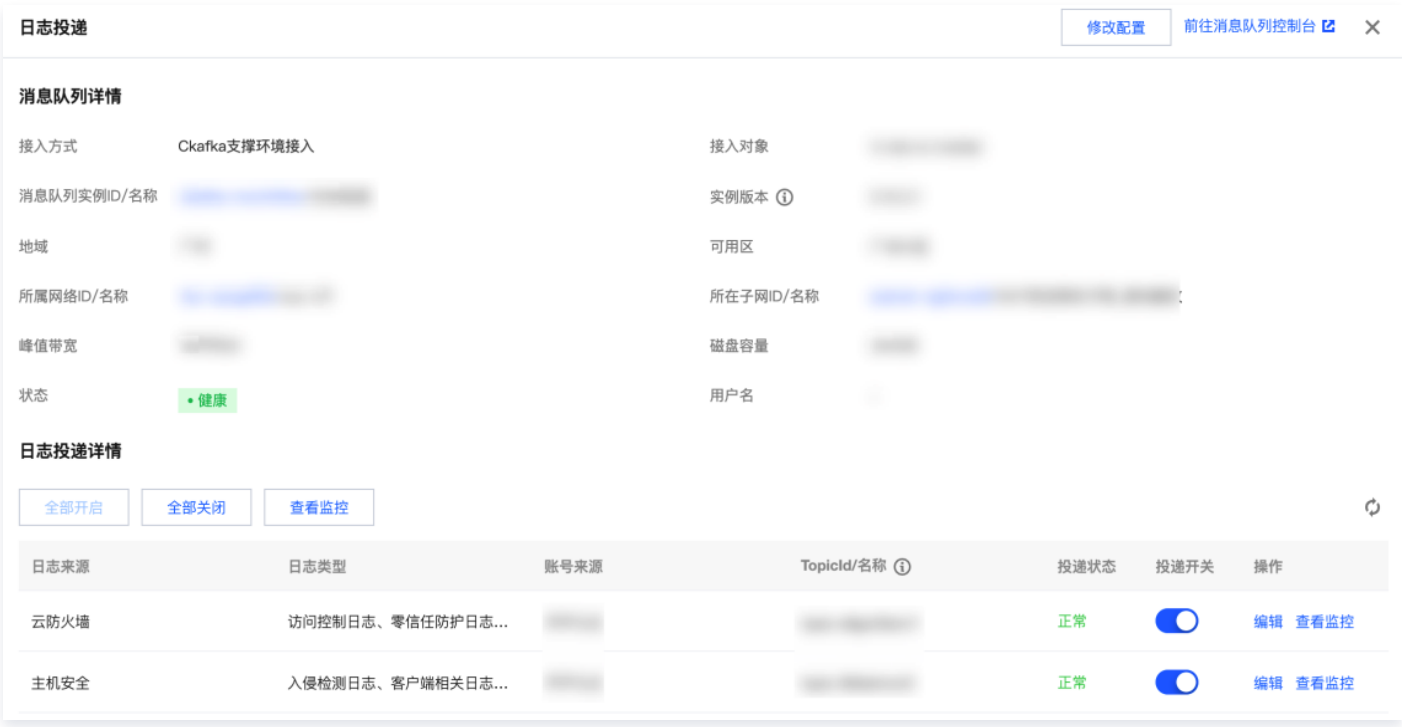


Ckafka 支撑环境接入

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击**日志投递 > 投递至 kafka**。
3. 在投递至 kafka 页面，云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、已接入云安全中心的日志来源，选择 **Ckafka 支撑环境接入**，配置相关参数。

参数名称	说明
网络接入方式	Ckafka 支撑环境接入。
TLS 加密	选择是否开启 TLS 加密。
消息队列所属账号	投递目标所属账号。
消息队列实例	云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、选择所需消息队列实例。
支撑环境接入	选择所需支撑环境。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
Topic ID/名称	选择所需 Topic。
操作	• 新增：单击**新增日志投递配置**，支持新增多个日志来源。 • 删除：单击目标日志操作列的**删除**，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。 • 编辑：如非首次配置日志投递，则支持在日志投递页面，单击**修改配置**，修改相关日志投递。

4. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的消息队列。
5. 在日志投递页面，支持查看同步接入方式、接入对象、消息队列状态、用户名等消息队列详情，以及日志来源、日志类型、账号来源（多账号下）、Topic ID/名称、Topic 投递状态、投递开关等信息，允许修改消息队列、Topic 配置等信息，查看消息队列和各 Topic 状态。



其他 Kafka 公网接入

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击**日志投递** > **投递至 kafka**。
3. 在投递至 kafka 页面，选择**其他 Kafka 公网接入**，配置相关参数。

参数名称	说明
网络接入方式	其他 Kafka 公网接入。
TLS 加密	选择是否开启 TLS 加密。
公网接入	根据实际需求填写公网信息。
用户名	请输入所选消息队列实例的用户名。
密码	请输入所选消息队列实例的密码。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。

Topic 名称	输入所需 Topic 名称。
操作	• 新增：单击**新增日志投递配置**，支持新增多个日志来源。 • 删除：单击目标日志操作列的**删除**，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。 • 编辑：如非首次配置日志投递，则支持在日志投递页面，单击**修改配置**，修改相关日志投递。

4. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的消息队列。
5. 在日志投递页面，支持查看同步接入方式、接入对象、消息队列状态、用户名等消息队列详情，以及日志来源、日志类型、账号来源（多账号下）、Topic 名称、Topic 投递状态、投递开关等信息，并且允许修改消息队列、Topic 配置等信息。

日志投递至 CLS

在日志分析页面，您可配置云安全中心接入的不同日志类型分别投递到指定 CLS 的不同日志主题中。

1. 单击左上角的**日志投递**，打开日志投递配置弹窗，首次若未开通 CLS 服务，须先单击 前往授权，同意服务授权且创建服务角色后才可进行更多日志投递配置。

> **说明：**
> 云安全中心支持将日志投递到CLS，实现日志采集、日志存储到日志检索等全方位的日志服务。当前账号授权访问CLS服务和开启日志投递到CLS后，将为您自动 在CLS服务中创建后付费的存储空间，同时也会生成后付费账单。详情请参见 CLS计费详情 。

2. 完成上述授权后，可对要进行投递的日志配置不同的日志主题（不进行投递的日志类型，可以不进行配置）。

参数名称	说明
投递所属账号	投递目标所属账号。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
日志来源账号	选择的日志源对应的多账号名称。
目标地域	请输入将要投递的目标地域。

日志集操作	选择投递至已有日志集还是新建日志集进行投递。
日志集	输入新建日志集名称/选择已有日志集。
日志主题操作	选择投递至已有日志主题还是新建日志主题进行投递。CLS 仅支持投递到在云安全中心创建的日志主题。
日志主题	输入新建日志主题名称/选择已有日志主题。

3. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的日志主题。
4. 在日志投递页面，支持查看账号名称/ID、所属部门，以及日志来源、日志类型、来源账号（多账号下）、日志主题、投递状态、投递开关等信息，并且允许编辑已投递任务、（批量）删除任务、（批量）开启/关闭任务、（批量）刷新、日志检索。

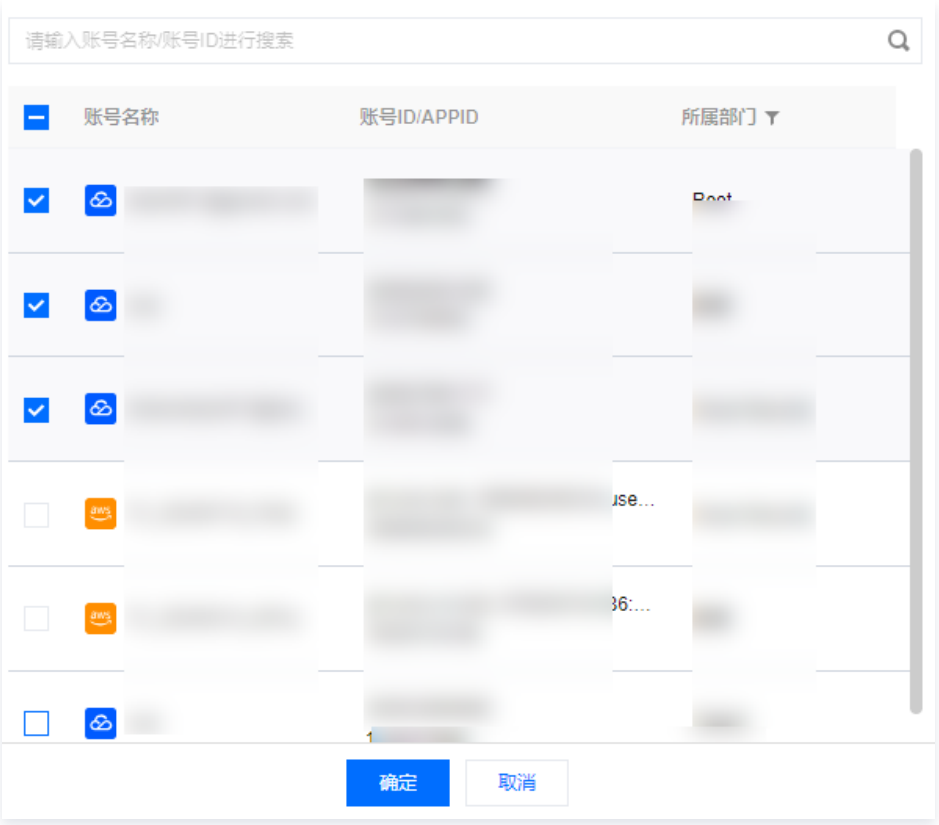
投递及被投递对象

多账号管理

开通 多账号管理 功能后，支持多账号多产品日志投递。

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击右上角的**多账号管理**。

3. 在多账号管理页面，选择所需账号，单击**确定**。



场景说明	未配置	配置完成
管理员/委派管理员将全部账号多产品日志统一投递到同一个 Kafka 中。	右上角选中全部账号后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取**管理员**的 Ckafka，可选所需腾讯云消息队列。	展示管理员的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、账号来源、投递状态等日志投递详情。
管理员/委派管理员管理其他账号日志，即配置其他账号多产品日志投递。	右上角选中其他账号后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取**其他账号**的 Ckafka，可选所需腾讯云消息队列。	展示其他账号的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。
管理员/委派管理员管理当前账号（管理员/委派管理员）日志，即配置当前账号多产品日志投递。	右上角选中当前账号（管理员/委派管理员）后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取**当前账号（管理员/委派管理员）**的 Ckafka，可选所需腾讯云消息队列。	展示当前账号（管理员/委派管理员）的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。

单账号管理

仅支持对当前账号进行多产品日志投递。

- 未配置：在配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取当前账号的 Ckafka，可选所需腾讯云消息队列。

> ⚠ **注意：**
> 若当前账号被管理员/委派管理员管理，则管理员/委派管理员可能编辑当前账号的日志投递配置。

- 配置完成：展示当前账号的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。

常见问题

日志投递如何收费?

日志投递为云安全中心旗舰版专属，可 前往购买日志投递 。

公网日志投递出口 IP 白名单

```
106.55.200.0/24
106.55.201.0/24
106.55.202.0/24
81.71.5.0/24
134.175.239.0/24
193.112.130.0/24
193.112.164.0/24
193.112.221.0/24
111.230.173.0/24
111.230.181.0/24
129.204.232.0/24
193.112.129.0/24
193.112.153.0/24
106.52.11.0/24
106.55.52.0/24
118.89.20.0/24
193.112.32.0/24
193.112.60.0/24
106.52.106.0/24
106.52.67.0/24
106.55.254.0/24
42.194.128.0/24
42.194.133.0/24
106.52.69.0/24
118.89.64.0/24
129.204.249.0/24
182.254.171.0/24
193.112.170.0/24
106.55.207.0/24
119.28.101.0/24
150.109.12.0/24
```

日志投递支持哪些产品哪些日志类型?

产品	日志类型	日志类型
云防火墙	访问控制日志	云防火墙基于用户在互联网边界防火墙、NAT 边界防火墙、VPC 间防火墙和企业安全组间配置的访问控制规则所生成的规则命中记录日志。
	零信任防护日志	云防火墙中用户远程运维登录、Web 服务访问、数据库访问三个模块的零信任防护日志，包括登录与访问服务详情。
	入侵防御日志	云防火墙基于“观察模式”和“拦截模式”所产生和记录的所有安全事件，有“外部入侵，主机失陷，横向移动，网络蜜罐”四个列表，分别查看入站和出站的安全事件详细情况。
	流量日志	云防火墙中互联网边界防火墙和 NAT 边界防火墙基于出站和入站所产生的南北向流量以及 VPC 间的东西向流量情况。
	操作日志	云防火墙中基于该账号内，用户针对安全策略以及开关页所进行的所有操作行为以及操作详情。

Web 应用防火墙	攻击日志	Web 应用防火墙提供攻击日志，记录攻击产生的时间、攻击源 IP、攻击类型及攻击详情等信息。
	访问日志	Web 应用防火墙防护记录域名的访问日志信息。
主机安全	入侵检测日志	主机安全提供木马、高危命令、本地提权及所有登录行为事件等多维度入侵检测的安全日志。
	漏洞管理日志	主机安全中漏洞安全事件详细情况的安全日志。
	高级防御日志	主机安全中基于Java 内存马、攻击检测等高级防御的日志。
	客户端相关日志	主机安全检测到客户端异常离线且长达24小时以上未重新上线、客户端被卸载（仅针对 Linux 系统的服务器）的日志。

多云多账号管理
多云接入

最近更新时间：2025-08-15 17:12:22

功能简介

当用户业务同时部署在腾讯云和第三方云厂商时，支持通过腾讯云云安全中心集中管理多云资源（目前支持阿里云、亚马逊云 AWS、微软云 Azure）。通过接入多云账号，实现多云安全管理上的透明化与可视化，实时掌握第三方云上业务的安全防护状态、风险等信息。

操作步骤

1. 登录 云安全中心控制台，在左侧导览中，单击**多云多账号管理**。
2. 在多云多账号管理页面，单击**接入多云账号**。

3. 在配置多云、云外、混合云账号页面，选择账号类型为 阿里云账号 、 Azure 账号 或 AWS 账号，并配置相关参数，单击**确定**。

阿里云账号

1. 登录阿里云控制台后，前往 RAM 访问控制–创建权限策略，选择**脚本编辑**。

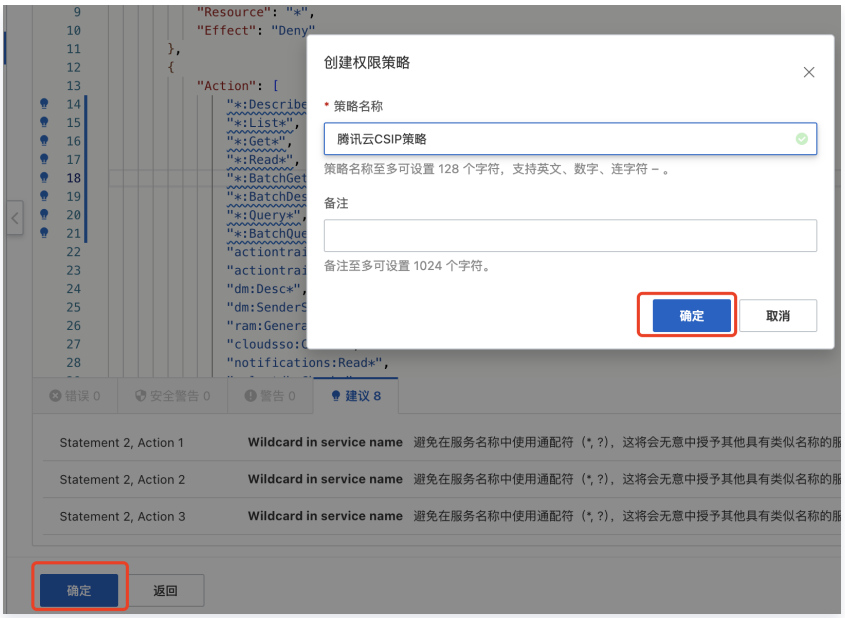
2. 在策略脚本编辑框中，填写下方内容，可访问 文档 了解所需权限的具体原因及参考的系统策略。

```
{
  "Version": "1",
  "Statement": [
      {
```

```
            "Action": [
                "bss:*",
                "bssapi:*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        },
        {
            "Action": [
                "*:Describe*",
                "*:List*",
                "*:Get*",
                "*:Read*",
                "*:BatchGet*",
                "*:BatchDescribe*",
                "*:Query*",
                "*:BatchQuery*",
                "actiontrail:Lookup*",
                "actiontrail:Check*",
                "dm:Desc*",
                "dm:SenderStatistics*",
                "ram:GenerateCredentialReport",
                "cloudsso:Check*",
                "notifications:Read*",
                "selectdb:Check*",
                "hbr:Search*",
                "hbr:BrowseFiles",
                "hbr:BatchCountTables",
                "hbr:CheckRole",
                "hbr:PreCheckSourceGroup",
                "nis:Count*",
                "nis:Check*",
                "nis:Is*",
                "sr:HasRole",
                "resourcecenter:Search*",
                "resourcecenter:ExecuteSQLQuery",
                "resourcecenter:ExecuteMultiAccountSQLQuery",
                "clickhouse:Check*",
                "yundun-waf:*",
                "yundun-cloudfirewall:*",
                "sasti:Get*",
                "sasti:Describe*",
                "sasti:Query*",
                "sasti:List*",
                "sasti:Grant*",
                "ecs:CreateSecurityGroup",
                "ecs:ModifySecurityGroupPolicy",
                "ecs:ModifySecurityGroupAttribute",
                "ecs:DeleteSecurityGroup",
                "ecs:AuthorizeSecurityGroup",
                "ecs:ModifySecurityGroupRule",
                "ecs:RevokeSecurityGroup",
                "ecs:AuthorizeSecurityGroupEgress",
                "ecs:ModifySecurityGroupEgressRule",
                "ecs:RevokeSecurityGroupEgress",
                "ecs:JoinSecurityGroup",
```

```
                "ecs:LeaveSecurityGroup"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "mq:OnsRegionList",
                "mq:OnsInstanceInServiceList",
                "ons:OnsRegionList",
                "ons:OnsInstanceInServiceList"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "yundun-sas:*",
                "yundun-aegis:*",
                "sasti:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "sas.aliyuncs.com",
                        "cloudsiem.sas.aliyuncs.com",
                        "cspm.sas.aliyuncs.com"
                    ]
                }
            }
        }
    ]
}
```

3. 单击**确定**，填写**策略名称**后，再单击**确定**。推荐命名为“腾讯云CSIP策略”，便于理解使用场景。

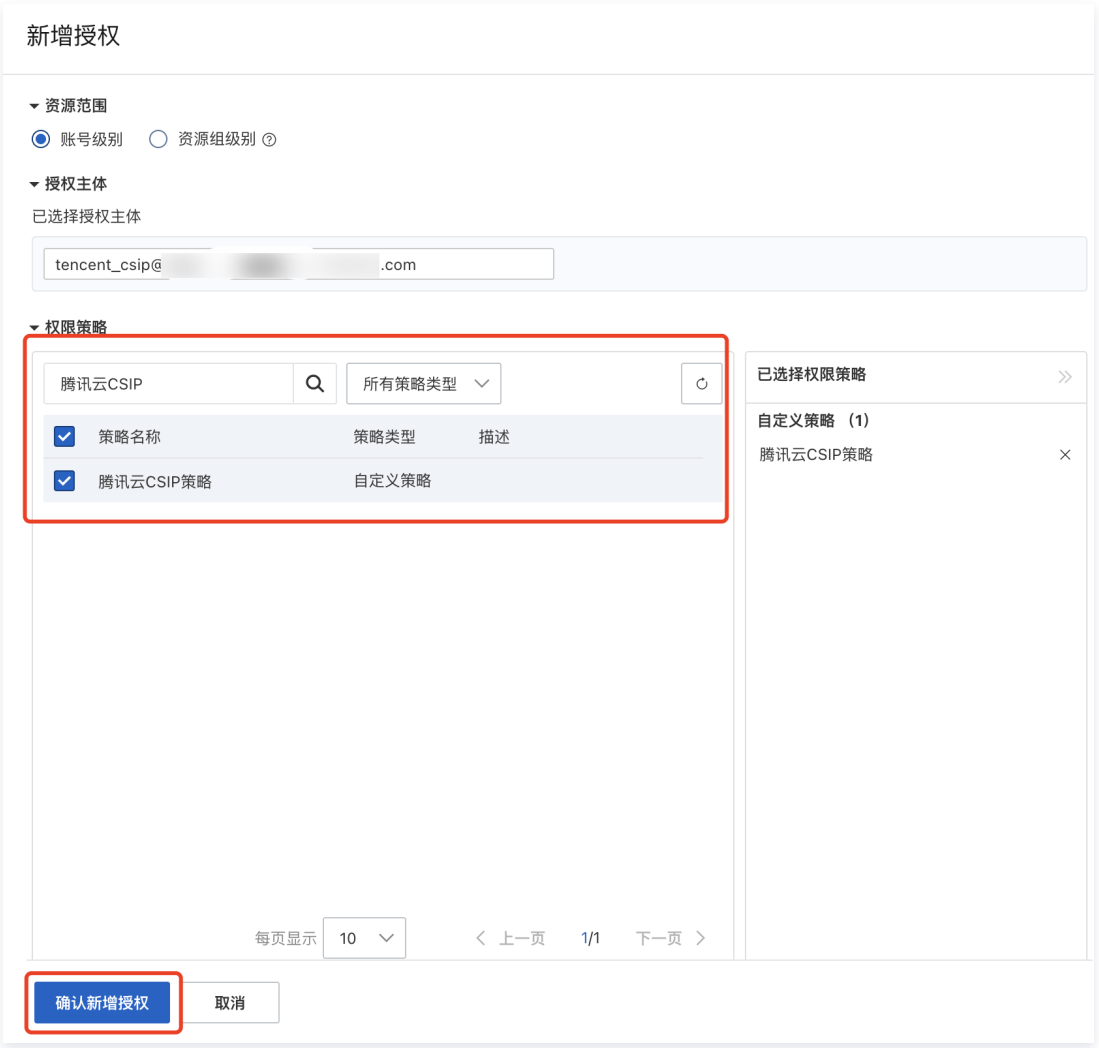


4. 登录阿里云控制台后前往 RAM 访问控制-创建用户 ，选择**使用永久 AccessKey 访问**，推荐使用 tencent_csip 作为名称，便于理解账号用途。

5. 复制或下载 AccessKey ID 和 AccessKey Secret。

6. 勾选账号，单击**添加权限**。

7. 搜索前面步骤创建的策略“**腾讯云CSIP策略**”，勾选并单击**确认新增授权**。

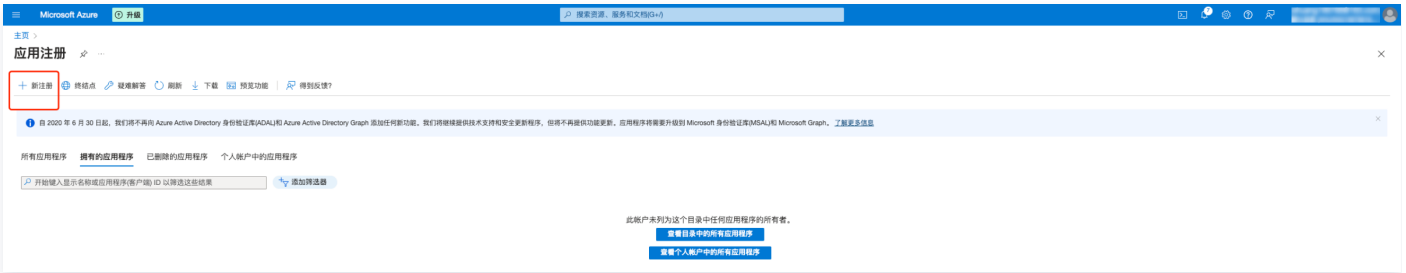


8. 在 多云多账号管理 **的配置页面**，将 AccessKey ID和AccessKey Secret 填写至子账号 SecretID、子账号 SecretKey，并注明账号名称，单击**确定**。

Azure 账号

步骤1：应用注册

1. 登录 Azure 后前往应用注册页面，单击**新注册**（如果已有应用注册，跳到第二步）。

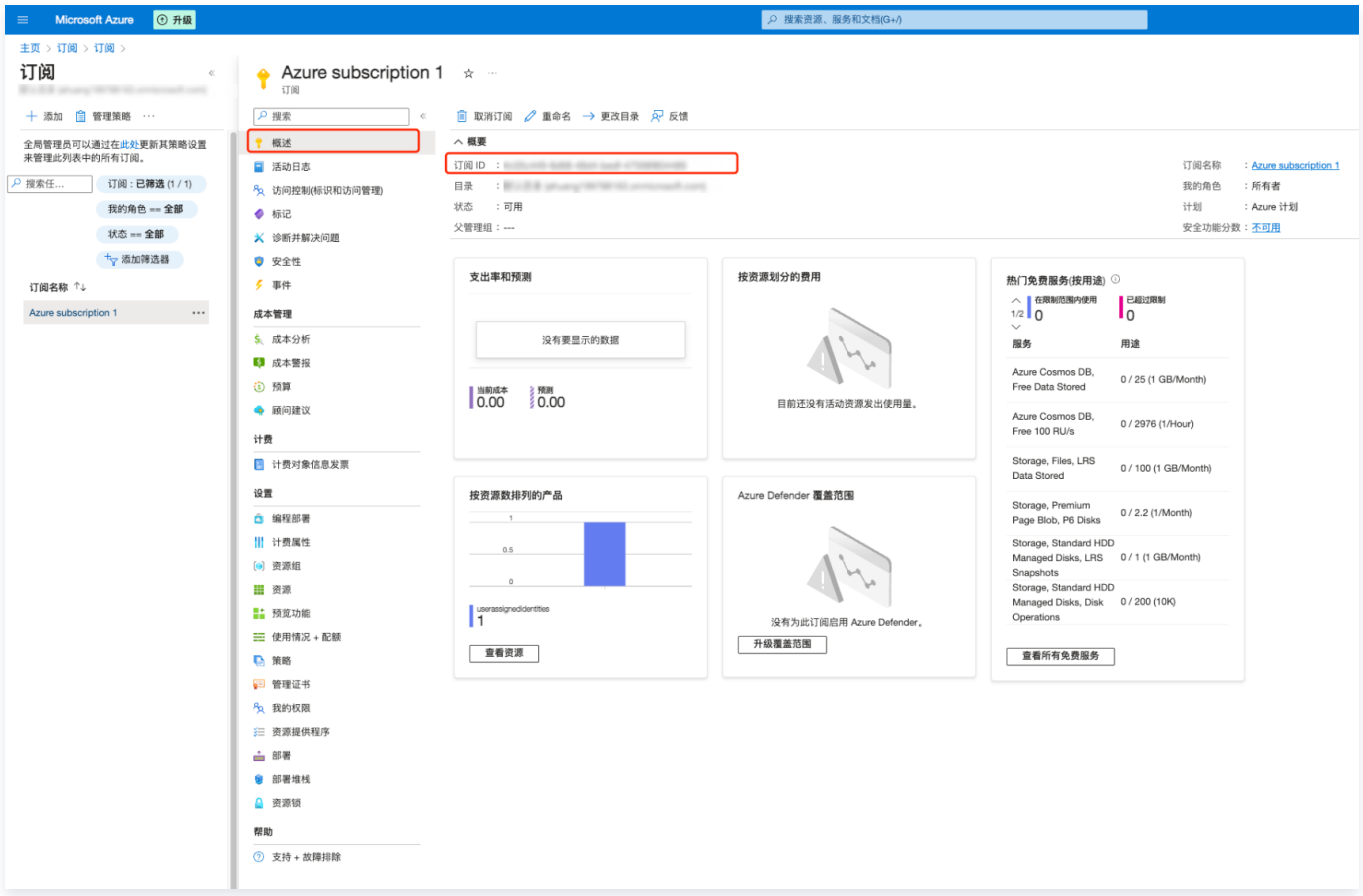


2. 在注册应用程序页面，填写应用程序“名称”，并根据实际需要选择“受支持的账户类型”，单击**注册**。

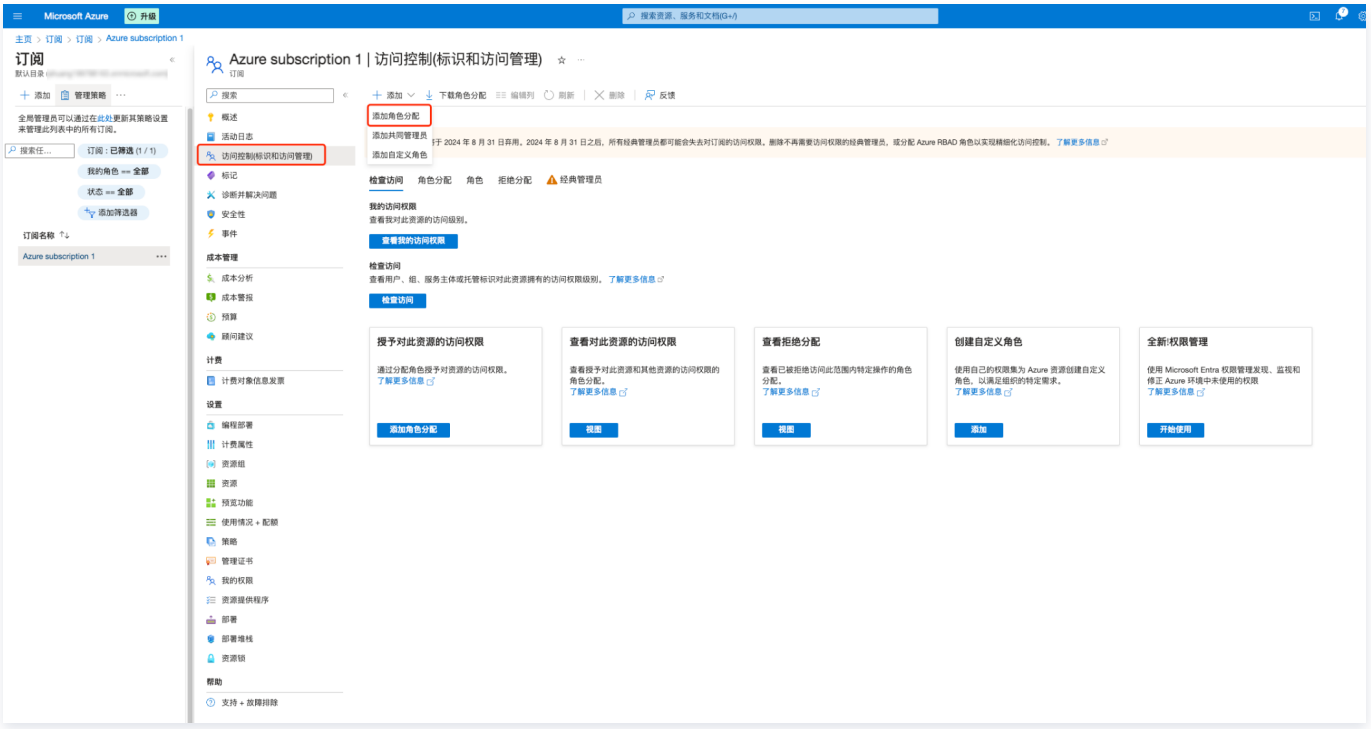
步骤2：获取订阅 ID

1. 在订阅列表页面，选择将要接入的订阅（应用注册可以绑定多个订阅），单击**订阅名称**。

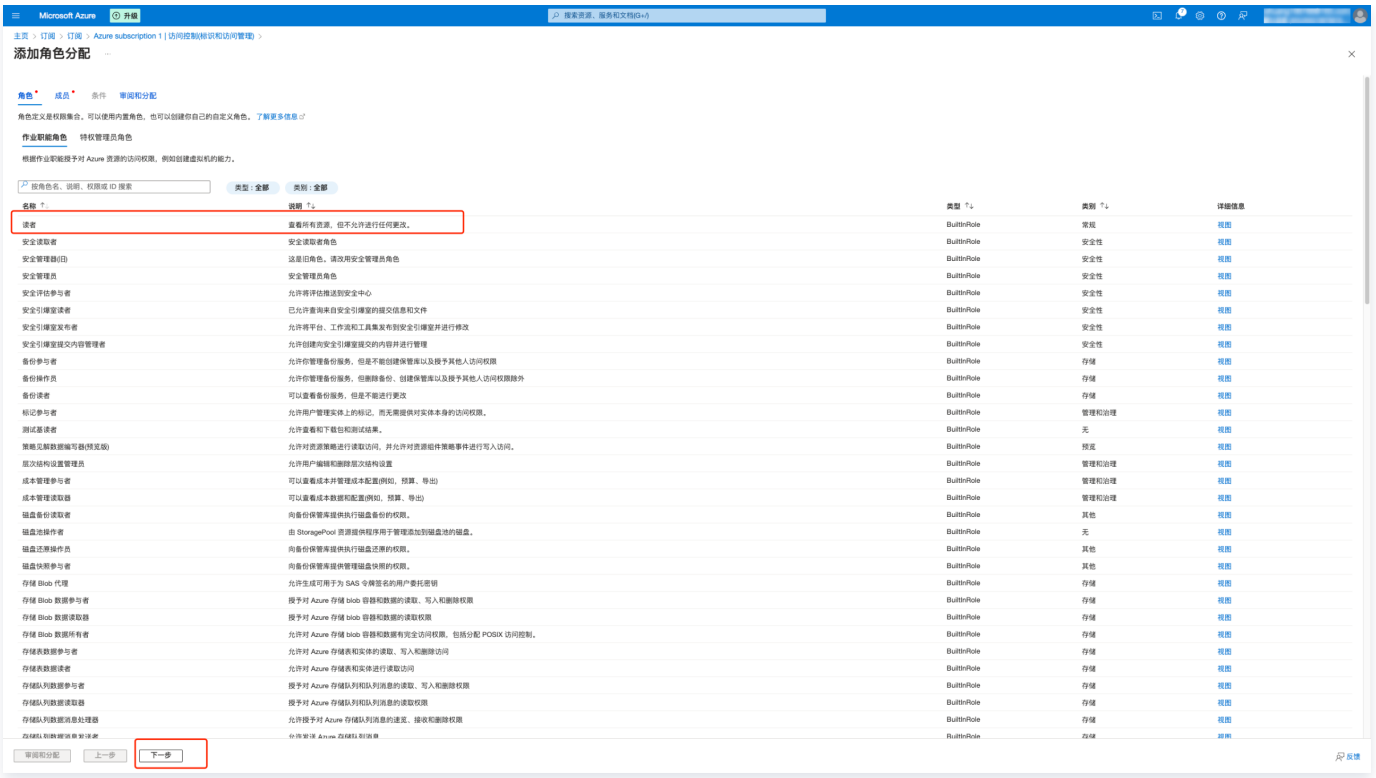
2. 在订阅详情页面，单击**概述**，获取**订阅 ID**。



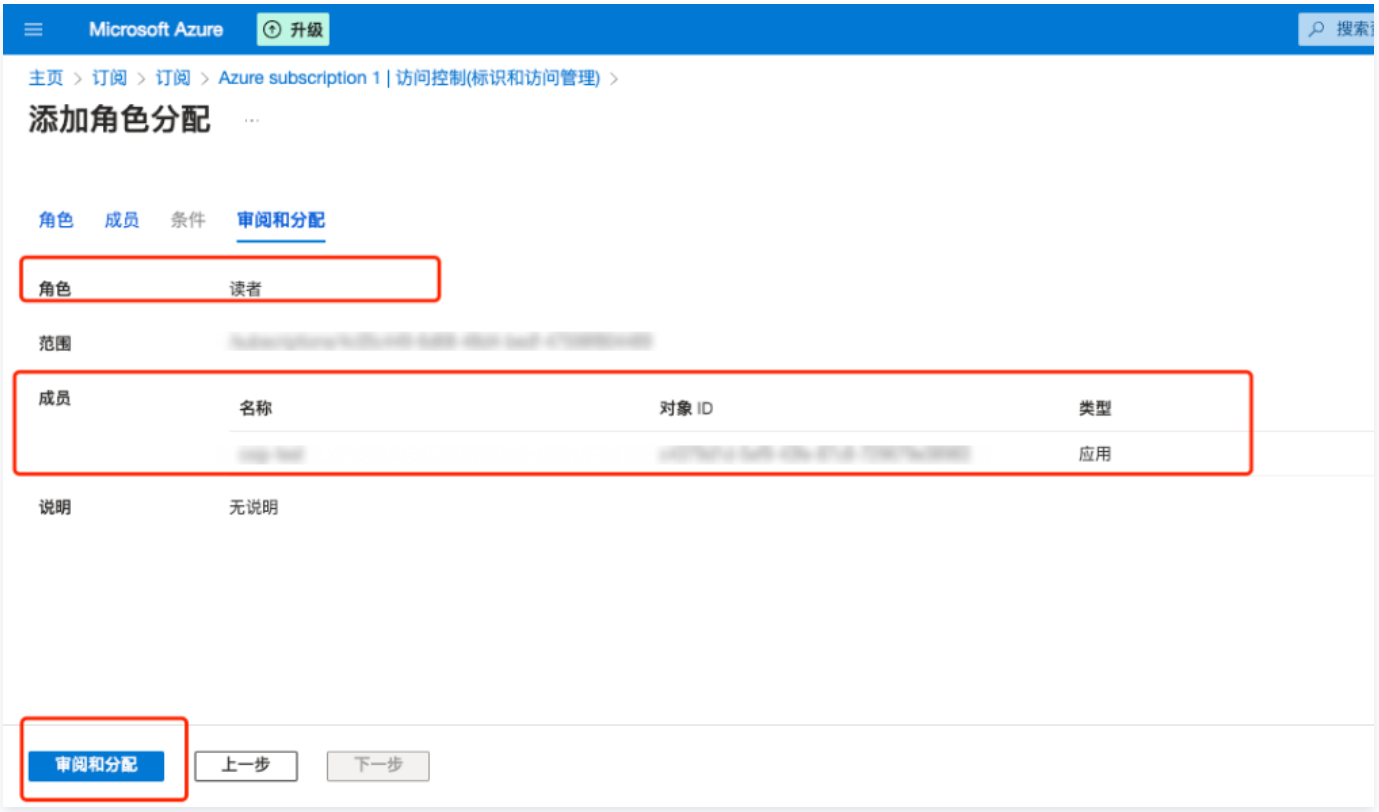
3. 选择**访问控制**，单击**添加**，选择**添加角色分配**。



4. 选择需要**分配的角色**，建议依次选择“读者 ”和“Azure Kubernetes 服务群集用户角色”，单击**下一步**。

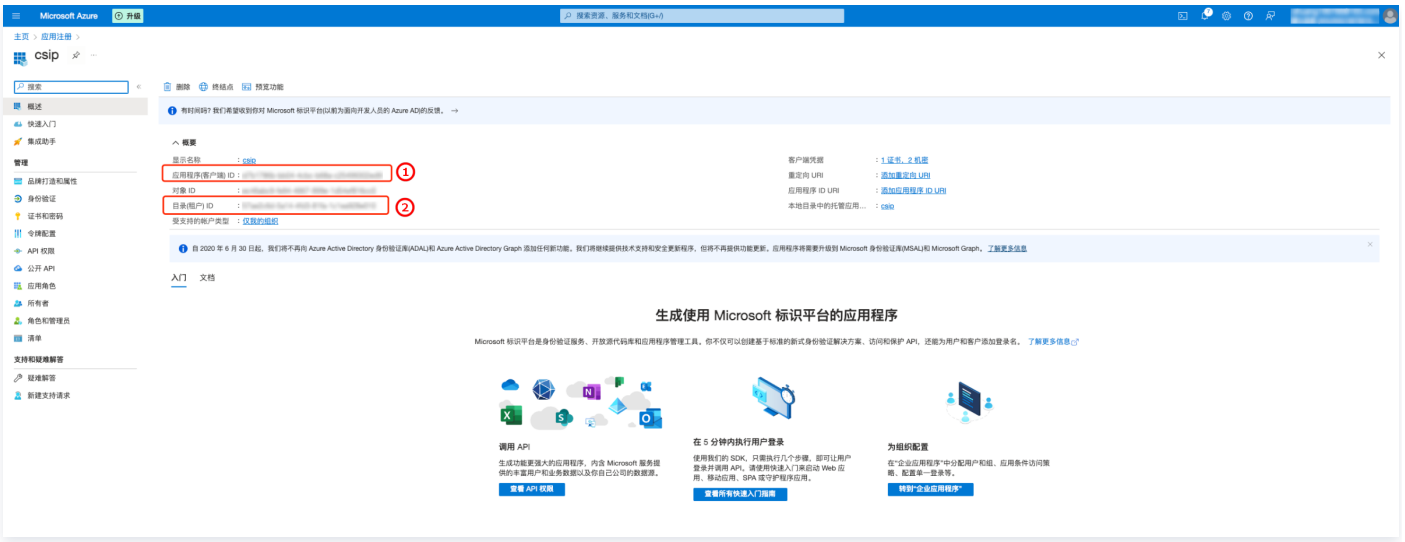


5. 添加需要分配的用户，单击**选择成员**，在搜索框输入要添加的“应用注册”名称，选择该**应用注册**，单击**下一步**。
6. 确定角色与成员，单击**审阅和分配**。



步骤3：获取租户 ID、客户端 ID、客户端密钥

1. 进入刚刚绑定的应用注册页面，单击**概览**，获取“①客户端 ID”与“②租户 ID”。



2. 单击**证书和密码 > 新客户端密码**，填写**说明**，截止期限选择**730天（24个月）**，单击**添加**。

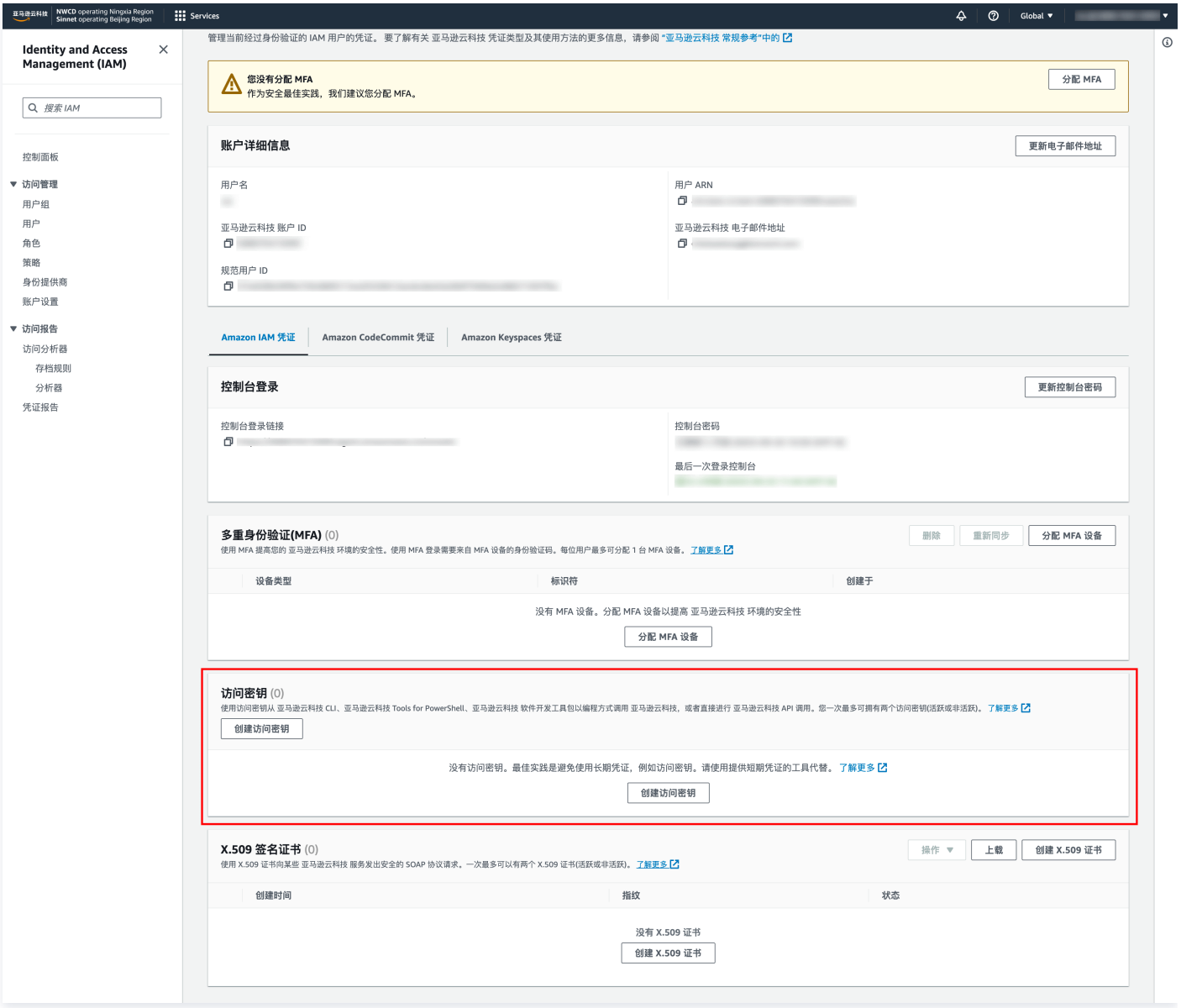
3. 在证书和密钥页面，获取**客户端密钥**。

AWS 账号

快速配置

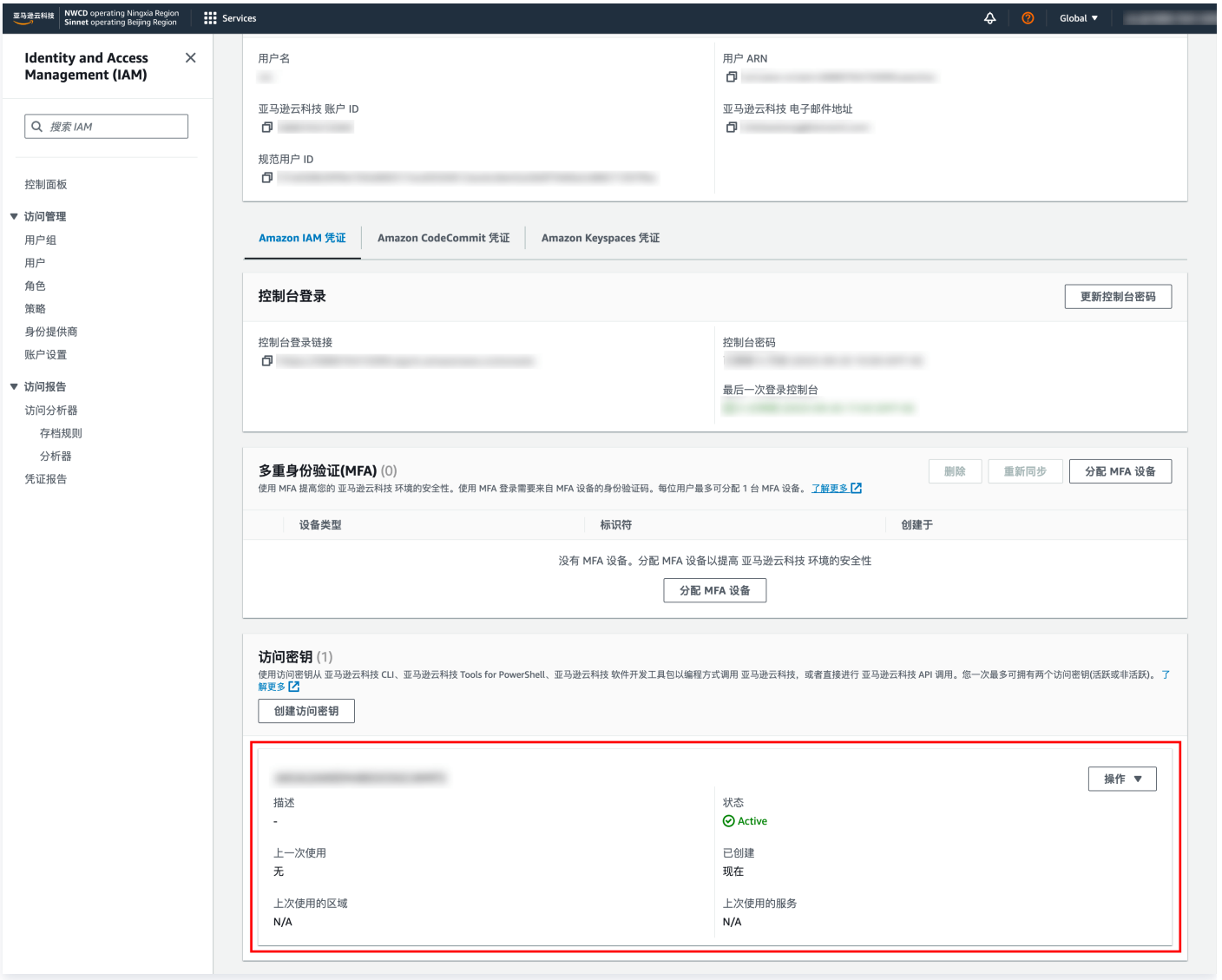
完成时间约为1分钟，但因需要较高权限，需配置主账号的 AK。之后，云安全中心会自动创建一个子账号 AK 以接入资产，并授予对所有资产的只读权限。

1. 请登录 AWS 后前往 安全凭证 页面，单击**创建访问密钥**生成可用于监控或管理亚马逊云科技资源的“访问密钥”、“秘密访问密钥”。



2. 在检索访问密钥页面，查看或下载“访问密钥”、“秘密访问密钥”。

3. 确保“访问密钥”的状态为 Active 后，将“访问密钥”、“秘密访问密钥”填写至“主账号 SecretID”、“主账号 SecretKey”。

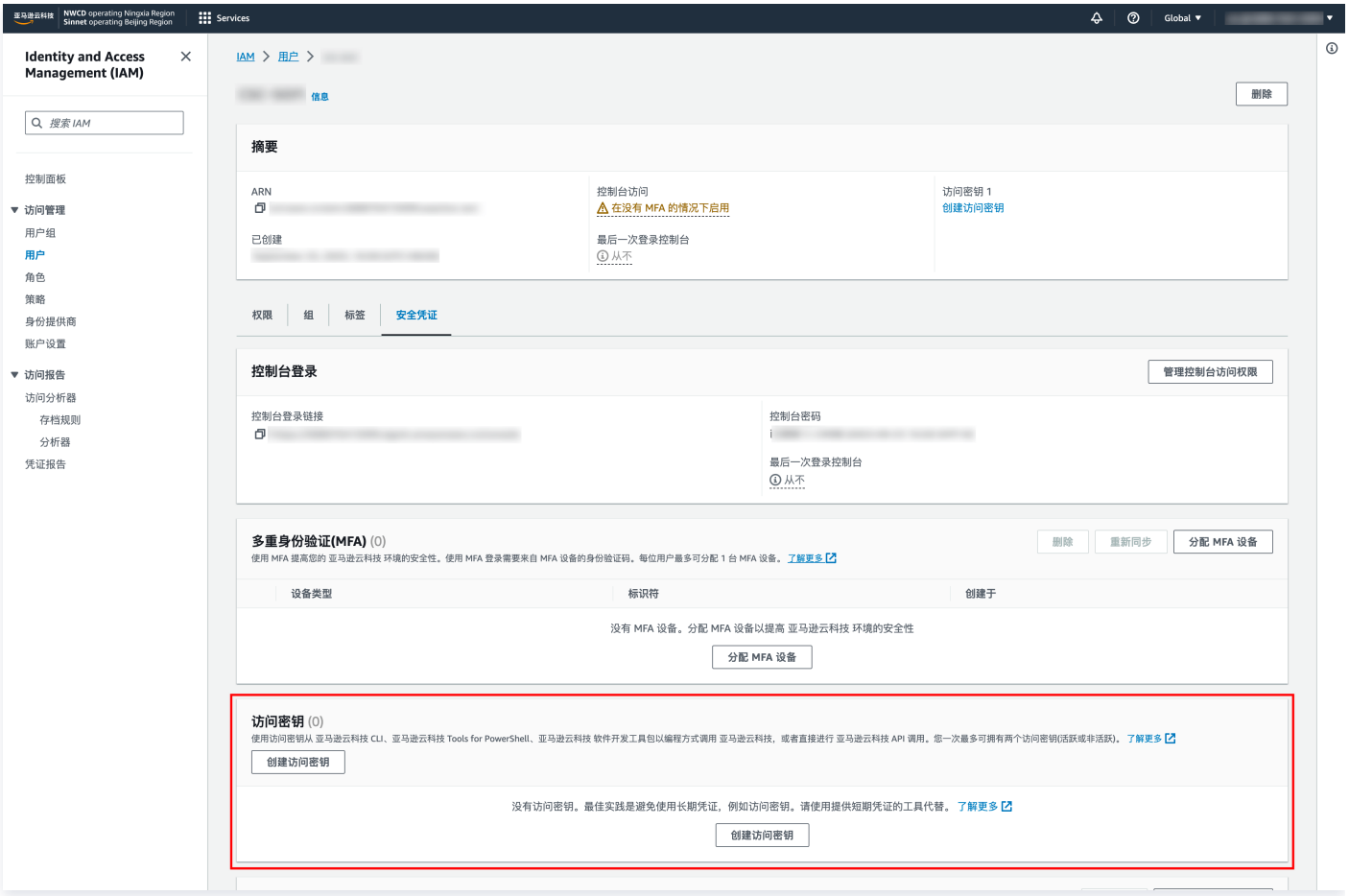


手动配置

完成时间约为5分钟，但权限配置较为复杂，需要为创建好的子账号配置访问密钥（AK），以便更灵活地控制权限范围。

1. 请登录 AWS 后前往 IAM > 用户 页面，单击**创建用户**，创建子账号用于与账户中的 亚马逊云科技进行交互。

2. 进入该子用户详情，单击**创建访问密钥**生成可用于监控或管理亚马逊云科技 资源的“访问密钥”、“秘密访问密钥”。

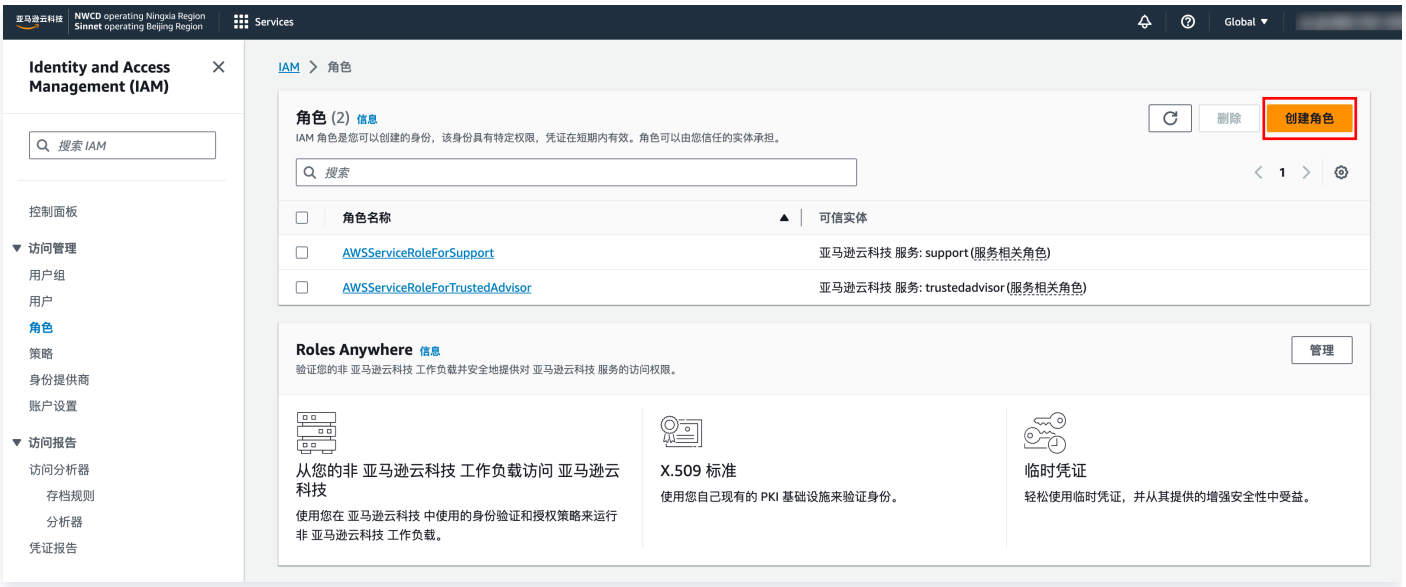


3. 查看或下载“访问密钥”、“秘密访问密钥”，确保“访问密钥”的状态为 Active 后，将“访问密钥”、“秘密访问密钥”填写至“子账号 SecretID”、“子账号 SecretKey”。

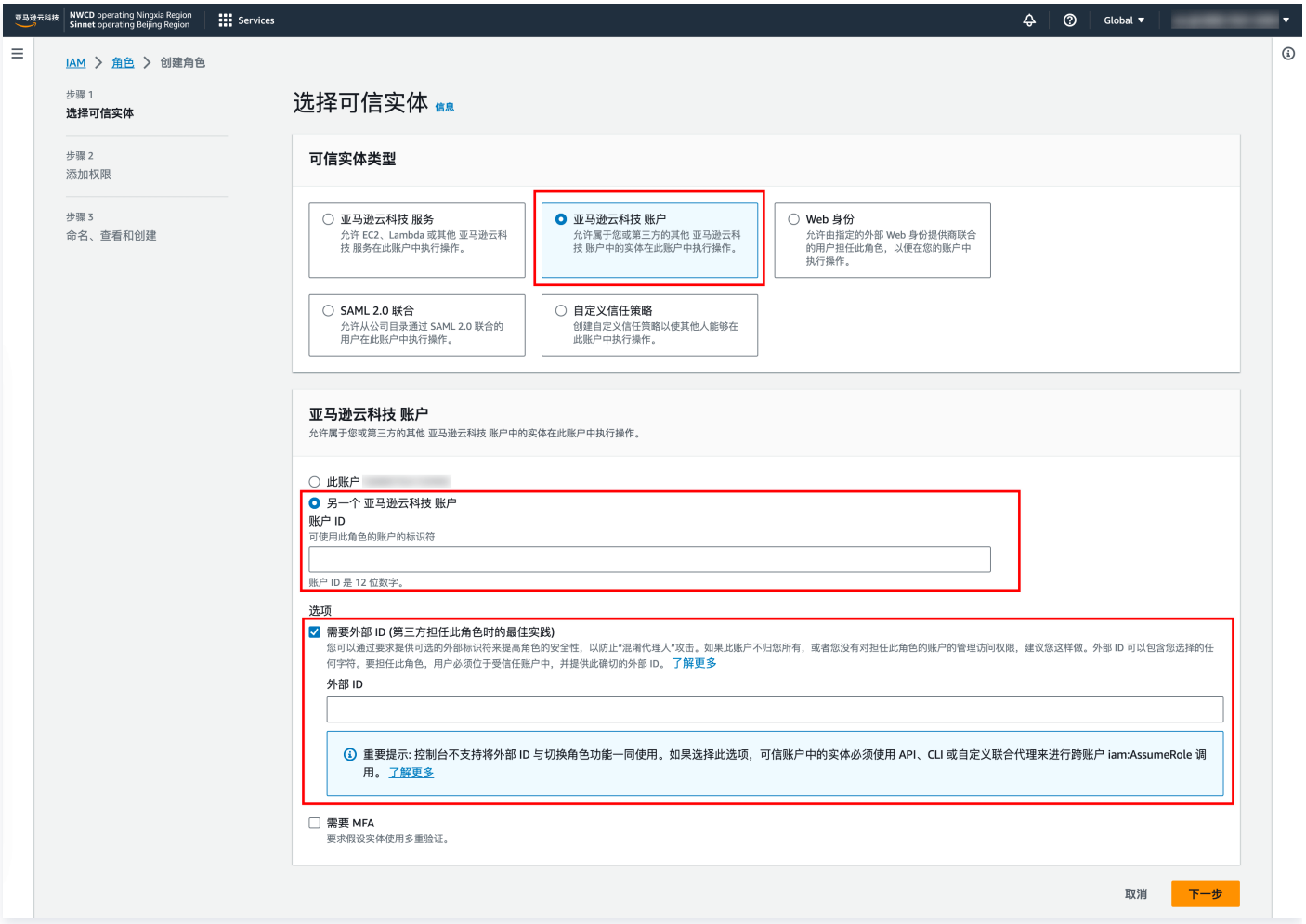
高级配置

较为复杂，但权限范围和期限可控。请按照我们提供的 RoleArn 在 AWS 创建角色，并授权指定 ARN 且带有 uuid 的账号调用 sts:AssumeRole 接口。该接口用于创建账号的临时访问角色。

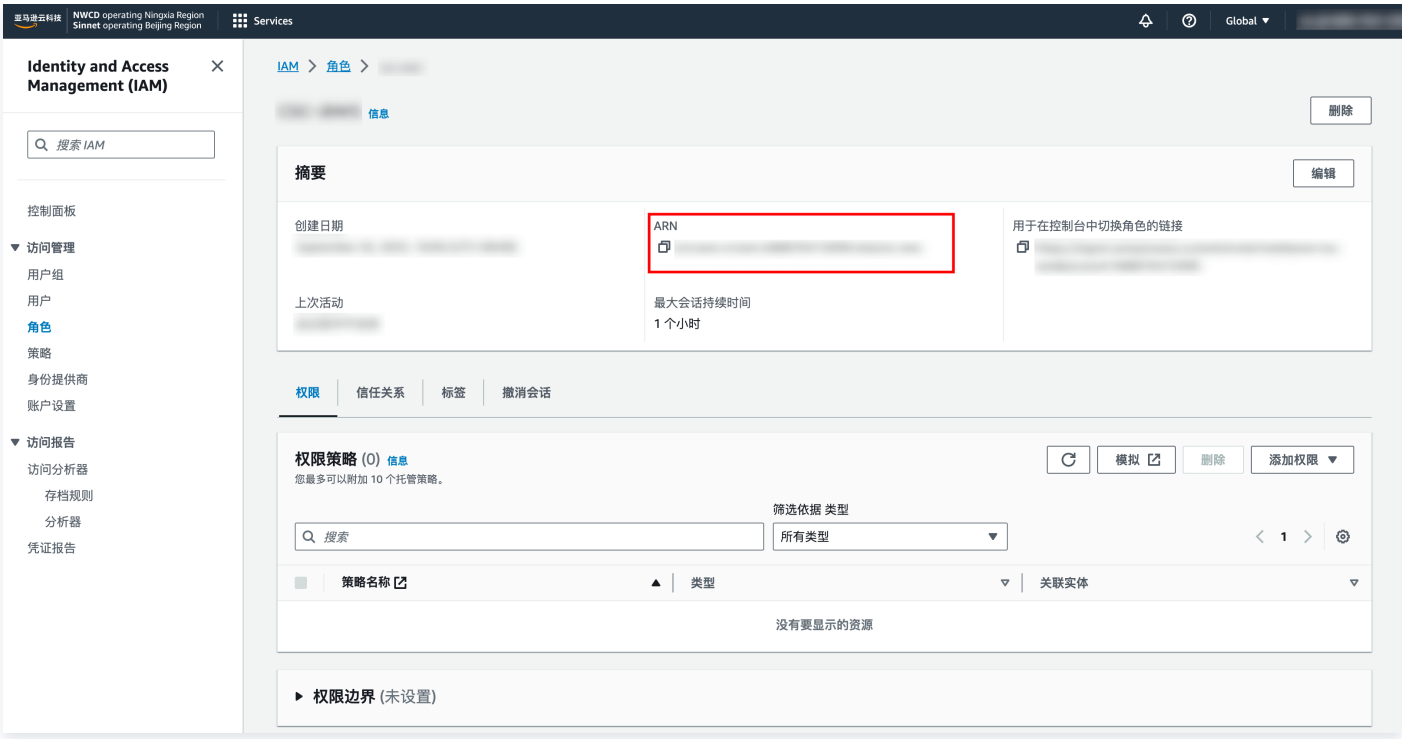
1. 请登录 AWS 后前往 IAM > 角色 页面，单击**创建角色**，该身份具有特定权限，凭证在短期内有效。角色可以由您信任的实体承担。



2. 选择“亚马逊云科技账户”为可信实体类型后，根据所需权限创建角色。



3. 进入该角色详情，将“ARN”复制并填入“RoleArn”框中。


NWCD operating Ningxia Region
Sinnet operating Beijing Region
Services
Global
Identity and Access Management (IAM)
搜索 IAM
控制面板
访问管理
用户组
用户
角色
策略
身份提供商
账户设置
访问报告
访问分析器
存档规则
分析器
凭证报告
IAM > 角色 >
信息
删除
摘要
编辑
创建日期
ARN
用于在控制台中切换角色的链接
上次活动
最大会话持续时间
1 个小时
权限
信任关系
标签
撤消会话
权限策略 (0) 信息
您最多可以附加 10 个托管策略。
模拟
删除
添加权限
筛选依据 类型
搜索
所有类型
1
策略名称
类型
关联实体
没有要显示的资源
权限边界 (未设置)

多账号管理

最近更新时间：2025-08-15 14:42:31

功能简介

用户拥有多个腾讯云主账号且各账号间独立计费，通过多账号管理切换登录各账号、集中管理各账号。集团管理者有效掌握集团安全信息，实现集团安全管理上的透明化与可视化，实时掌握各成员账号云上业务的安全防护状态、风险等信息。

操作场景

切换登录账号

支持一键切换成员账号登录，满足高效且安全的免密码切换。

集中管理账号

无需部署，集中管理集团内外所有账号，各成员账号安全防护状态透明化，支持设置账号的安全管理权限。
支持对集团内外多账号云上业务风险处理闭环，可以对任一成员账号的云上资产进行一键扫描以排查潜在风险。

一、集团账号管理

您需在集团账号管理中创建集团组织后，方可使用云安全中心多账号管理。根据当前登录账号不同状态区分，您可以挑选账号状态相符的步骤开始进行操作。

> **注意**
> 未企业实名认证的个人账号、已加入到其他集团组织的企业账号、之前集团组织创建的账号无法创建集团组织。详情请参见 集团组织设置 。

步骤1：未企业实名认证的个人账号

在 多云多账号管理页面 ，单击**完成实名认证**前往 账号中心控制台 ，按照步骤完成企业实名认证。详情请参见 变更个人认证信息-变更为企业实名认证 。

步骤2：未创建集团组织的企业账号

在 集团账号管理页面 ，单击**创建**，即创建一个集团组织。在该集团组织下，创建成员账号或邀请账号加入集团组织。

步骤3：使用多账号管理

已开通多账号管理的企业账号，可开始使用多账号管理。

二、集团外账号管理

步骤1：接入集团外账号

1. 在 多云多账号管理页面，单击**接入多云账号**。
2. 在配置多云、云外、混合云账号页面，选择账号类型为**腾讯云子账号**，按照选择的创建子账号方式进行相关配置，单击**确定**完成接入。

步骤2：使用多账号管理

已开通多账号管理的企业账号，可开始使用多账号管理。

三、如何灵活的切换账号登录

授权访问成员账号

登录 集团账号管理控制台，授权管理员子账号登录管理成员账号的权限。详情请参见 授权访问成员账号 。

切换登录成员账号

1. 在 多云多账号管理页面，选择对应成员账号，单击**登录账号**。

2. 在登录账号弹窗中，选择所需的权限名称、策略名称，并单击对应**登录成员账号**，即切换登录成功。

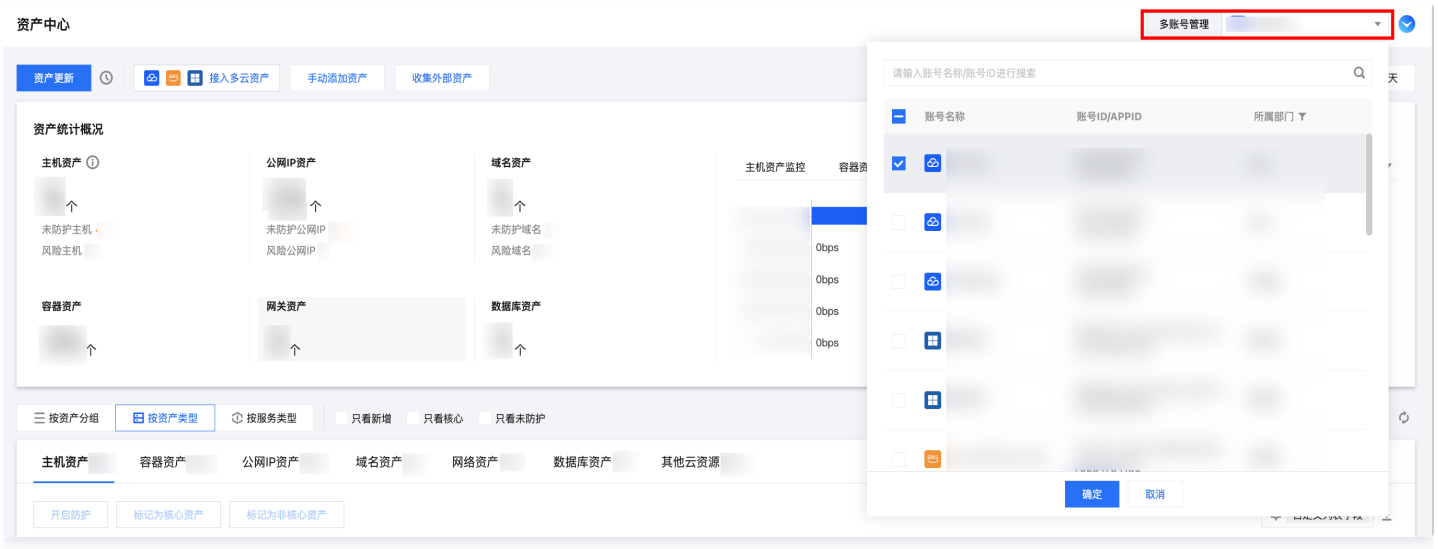
> **注意**
> 管理员主账号、未进行授权的管理员子账号不能切换登录、被邀请进集团组织的成员账号不支持授权登录。

四、如何高效的集中管理账号

使用管理员主账号、子账号登录 云安全中心控制台 后，支持查看集团安全信息，实现集团安全管理上的透明化与可视化，实时掌握各成员账号云上业务的安全防护状态、风险等信息。
在资产中心、风险中心、扫描任务、报告下载等功能模块已适配多账号管理模式，进行跨账号操作以保证集团云上业务资产的安全。

账号切换

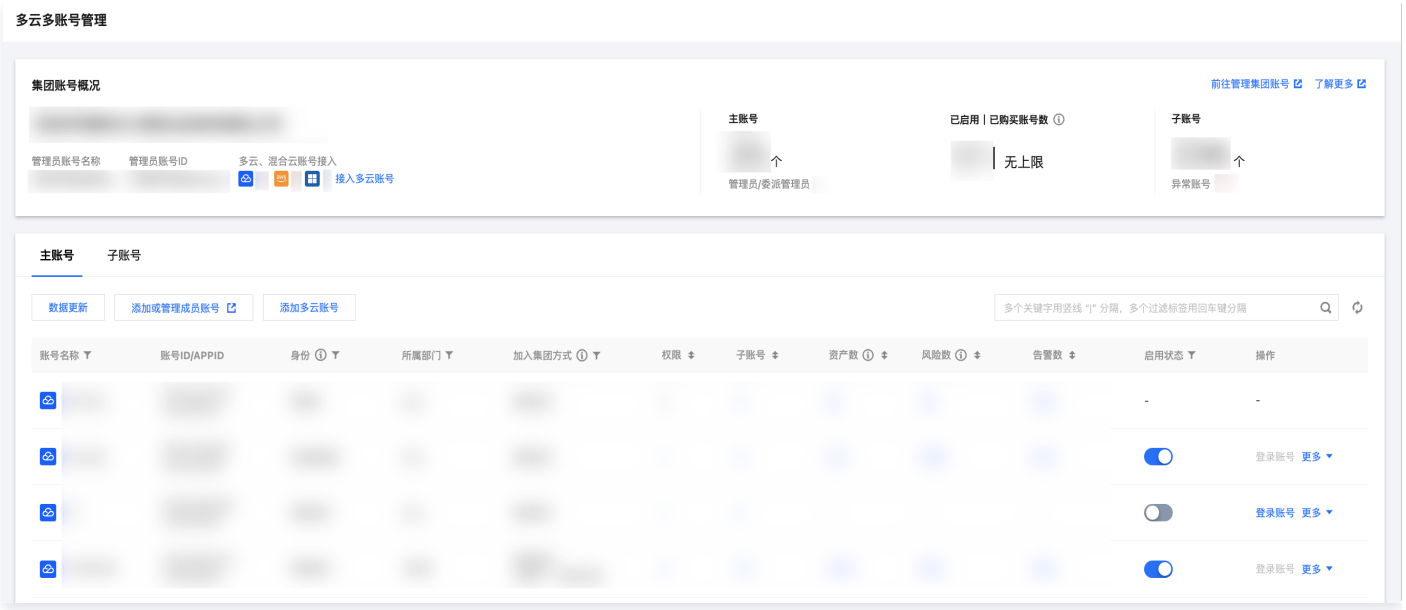
在各功能模块右上角，单击**多账号管理**，下拉筛选框后，可以通过输入**成员账号名称/成员账号 ID** 进行搜索，选中成员账号后单击**确定**，功能模块内数据将切换至该账号所有数据。



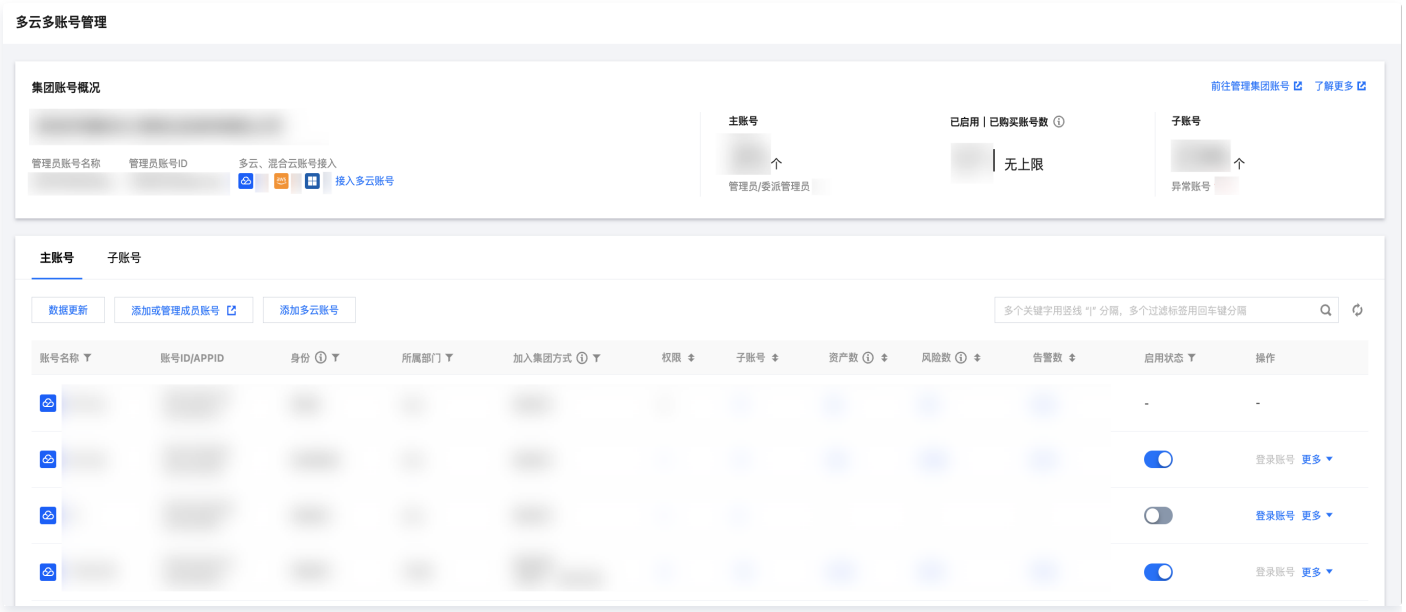
系统设置–多账号管理

在 多云多账号管理页面，无需部署集中管理集团所有账号，各成员账号安全防护状态透明化，支持一键切换成员账号登录，满足高效且安全的免密码切换。不同方式登录后效果如下所示：

- 管理员主账号登录



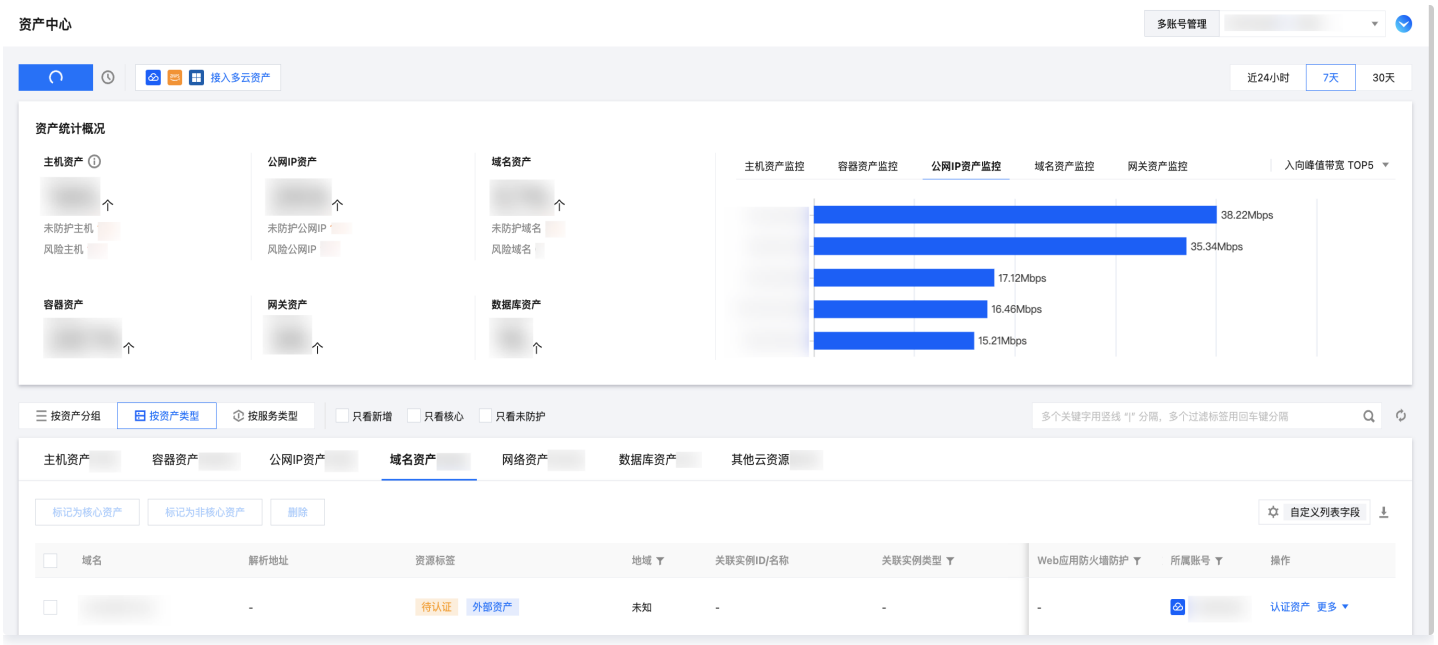
- 管理员子账号登录



- 成员主账号、子账号登录

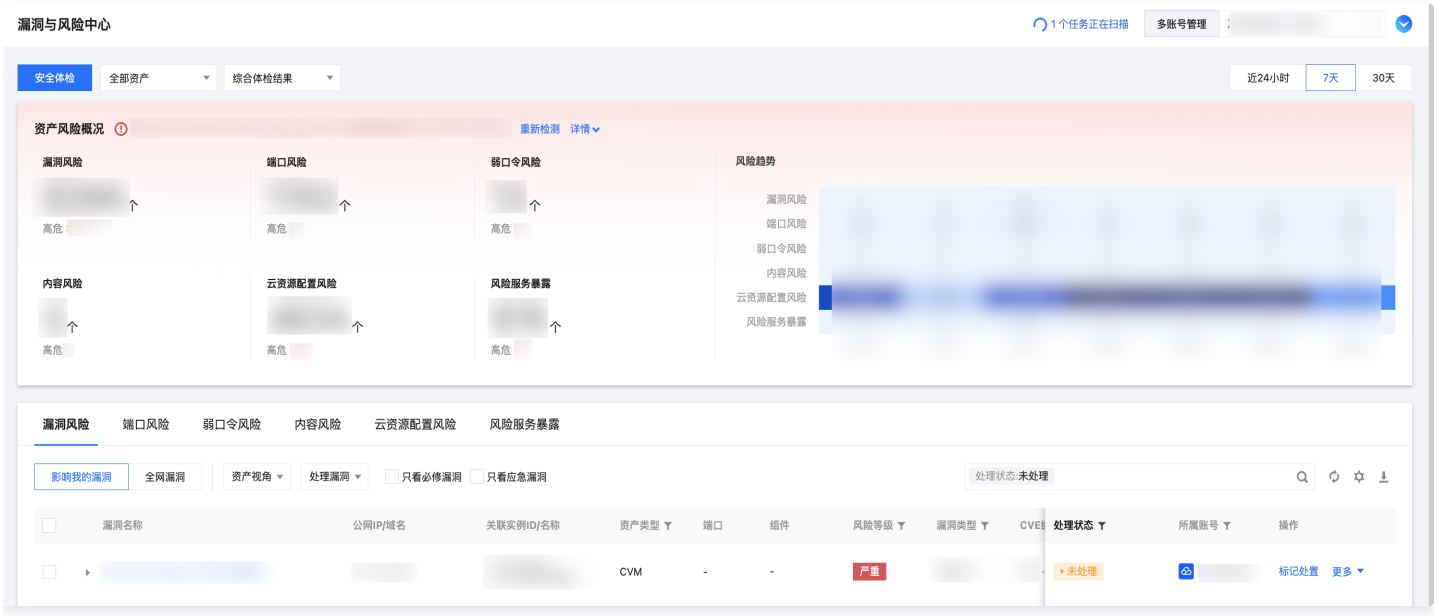
资产中心

在 资产中心页面，管理员账号可以跨账号管理云上业务资产，掌握各资产安全防护状态，对任一账号的云上资产进行一键扫描以排查潜在风险。



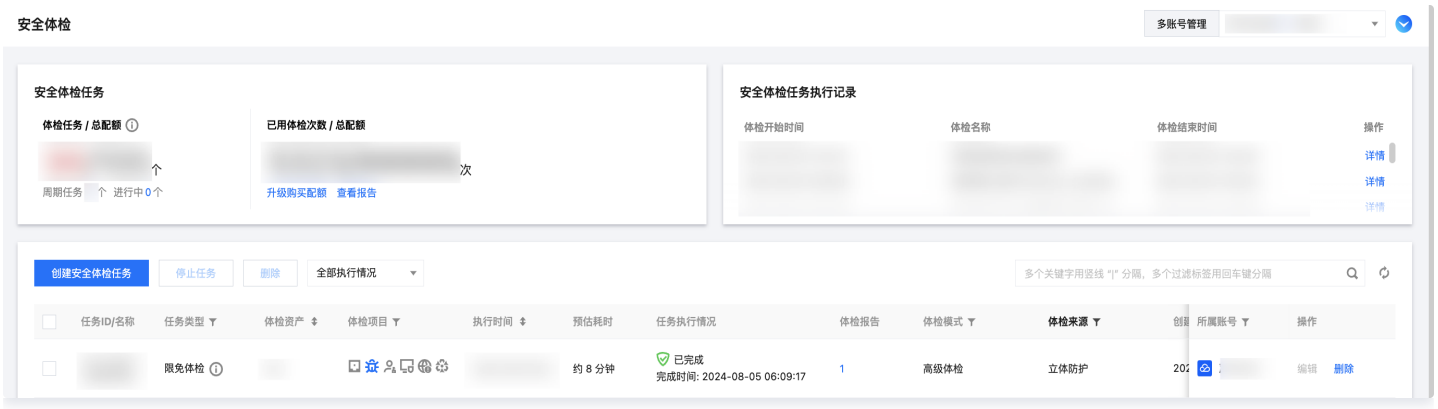
漏洞与风险中心

在 漏洞与风险中心页面，联动各产品能力一站式管控云上业务的端口、漏洞、弱口令、配置、内容等资产风险，管理员账号可以跨账号处理云上业务资产的潜在风险。



安全体检

在 安全体检页面，可视化集团组织下所有账号所有扫描任务的信息并实时反馈各扫描任务执行情况，管理员可以跨账号高效管理各资产扫描任务，支持管理员跨账号对各账号的扫描任务进行编辑、删除、停止任务等操作。



报告下载

在 报告下载页面，联动漏洞扫描服务，管理员可以跨账号下载各扫描任务对应的报告，管理员关注服务号可以随时随地接收报告。

五、常见问题

多账号管理之后的计费标准?

未来新版云安全中心的计费标准请实时关注产品动态。

存量用户的数据情况

云安全中心将在限时免费体验结束前一个月告知用户体验结束，未付费用户的数据将被清除，付费用户的数据将接入新版云安全中心。

如何实现多账号管理，是否需要调整网络架构?

安全产品的系统层数据上打通以实现多账号管理，不需要调整网络架构。

使用过程中，有问题如何联系?

感谢您对腾讯云的信赖与支持，若在使用产品过程中有任何问题可以 提交工单 联系我们处理，我们将尽快为您核实处理！

阿里云账号权限说明

最近更新时间：2025-06-26 16:48:52

权限说明

腾讯云安全中心调用阿里云账号需要的权限和说明如下：

产品	参考的系统策略	配置项	说明

费用与成本（BSS）	AliyunBSSFullAccess
	管理费用与成本（BSS）的权限
		{
		"Action": [
		"bss:",
		"bssapi:"
		],
		"Resource": "*",
		"Effect": "Deny"
		}
			拦截所有费用与成本相关的访问，避免访问用户费用清单。

所有	ReadOnlyAccess
	只读访问所有阿里云资源的权限
		{
		"Action": [
		":Describe",
		":List",
		":Get",
		":Read",
		":BatchGet",
		":BatchDescribe",
		":Query",
		":BatchQuery",
		"actiontrail:Lookup*",
		"actiontrail:Check*",
		"dm:Desc*",
		"dm:SenderStatistics*",
		"ram:GenerateCredentialReport",
		"cloudsso:Check*",
		"notifications:Read*",
		"selectdb:Check*",
		"hbr:Search*",
		"hbr:BrowseFiles",
		"hbr:BatchCountTables",
		"hbr:CheckRole",
		"hbr:PreCheckSourceGroup",
		"nis:Count*",
		"nis:Check*",
		"nis:Is*",
		"sr:HasRole",
		"resourcecenter:Search*",
		"resourcecenter:ExecuteSQLQuery",
		"resourcecenter:ExecuteMultiAccountSQLQuery",
		"clickhouse:Check*"
		],
		"Resource": "*",
		"Effect": "Allow"
		}
			只读访问所有阿里云资源

消息队列 RocketMQ 版	-	{
		"Action": [
		"mq:OnsRegionList",
		"mq:OnsInstanceInServiceList",
		"ons:OnsRegionList",
		"mq:OnsInstanceInServiceList"
		],
		"Resource": "*",
		"Effect": "Allow"
		}
			读取消息队列 RocketMQ 版的Region和服务列表

云安全中心（SAS）	AliyunYundunSASFullAccess
	管理云安全中心（SAS）的权限
		{
		"Action": [
		"yundun-sas:",
		"yundun-aegis:",
		"sasti:"
		],
		"Resource": "",
		"Effect": "Allow"
		},
		{
		"Action": "ram:CreateServiceLinkedRole",
		"Resource": "*",
		"Effect": "Allow",
		"Condition": {
		"StringEquals": {
		"ram:ServiceName": [
		"sas.aliyuncs.com",
		"cloudsiem.sas.aliyuncs.com",
		"cspm.sas.aliyuncs.com"
		]
		}
		}
		}
			阿里云云安全中心管理权限，未来可能用于漏洞修复、告警确认等场景，变更动作均由用户通过控制台触发，云安全中心仅主动触发查询操作。

云盾应用防火墙（WAF）	AliyunYundunWAFFullAccess
	管理云盾应用防火墙（WAF）的权限
		{
		"Action": "yundun-waf:",
		"Resource": "",
		"Effect": "Allow"
		}
			应用防火墙（WAF）管理，变更动作均由用户通过控制台触发，云安全中心仅主动触发查询操作。

云盾云防火墙（CloudFirewall）	AliyunYundunCloudFirewallFullAccess
	管理云盾云防火墙（CloudFirewall）的权限
		{
		"Action": [
		"yundun-cloudfirewall:*",
		"sasti:Get*",
		"sasti:Describe*",
		"sasti:Query*",
		"sasti:List*",
		"sasti:Grant*",
		"bss:QueryAvailableInstances",
		"bssapi:QuerySavingsPlansInstance"
		],
		"Resource": "*",
		"Effect": "Allow"
		}
			云防火墙（CloudFirewall）管理，变更动作均由用户通过控制台触发，云安全中心仅主动触发查询操作。

云服务器（ECS）	安全组相关操作	{ "Action": ["ecs:CreateSecurityGroup", "ecs:ModifySecurityGroupPolicy", "ecs:ModifySecurityGroupAttribute", "ecs:DeleteSecurityGroup", "ecs:AuthorizeSecurityGroup", "ecs:ModifySecurityGroupRule", "ecs:RevokeSecurityGroup", "ecs:AuthorizeSecurityGroupEgress", "ecs:ModifySecurityGroupEgressRule", "ecs:RevokeSecurityGroupEgress", "ecs:JoinSecurityGroup", "ecs:LeaveSecurityGroup",], "Resource": "*", "Effect": "Allow" }	安全组操作，用于主机入侵时，进行隔离。由用户通过控制台触发。

权限脚本配置

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "bss:*",
                "bssapi:*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        },
        {
            "Action": [
                "*:Describe*",
                "*:List*",
                "*:Get*",
                "*:Read*",
                "*:BatchGet*",
                "*:BatchDescribe*",
                "*:Query*",
                "*:BatchQuery*",
                "actiontrail:Lookup*",
                "actiontrail:Check*",
                "dm:Desc*",
                "dm:SenderStatistics*",
                "ram:GenerateCredentialReport",
                "cloudsso:Check*",
                "notifications:Read*",
                "selectdb:Check*",
                "hbr:Search*",
                "hbr:BrowseFiles",
                "hbr:BatchCountTables",
                "hbr:CheckRole",
```

```
                "hbr:PreCheckSourceGroup",
                "nis:Count*",
                "nis:Check*",
                "nis:Is*",
                "sr:HasRole",
                "resourcecenter:Search*",
                "resourcecenter:ExecuteSQLQuery",
                "resourcecenter:ExecuteMultiAccountSQLQuery",
                "clickhouse:Check*",
                "yundun-waf:*",
                "yundun-cloudfirewall:*",
                "sasti:Get*",
                "sasti:Describe*",
                "sasti:Query*",
                "sasti:List*",
                "sasti:Grant*",
                "ecs:CreateSecurityGroup",
                "ecs:ModifySecurityGroupPolicy",
                "ecs:ModifySecurityGroupAttribute",
                "ecs:DeleteSecurityGroup",
                "ecs:AuthorizeSecurityGroup",
                "ecs:ModifySecurityGroupRule",
                "ecs:RevokeSecurityGroup",
                "ecs:AuthorizeSecurityGroupEgress",
                "ecs:ModifySecurityGroupEgressRule",
                "ecs:RevokeSecurityGroupEgress",
                "ecs:JoinSecurityGroup",
                "ecs:LeaveSecurityGroup"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "mq:OnsRegionList",
                "mq:OnsInstanceInServiceList",
                "ons:OnsRegionList",
                "ons:OnsInstanceInServiceList"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "yundun-sas:*",
                "yundun-aegis:*",
                "sasti:*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
```

```
                "StringEquals": {
                    "ram:ServiceName": [
                        "sas.aliyuncs.com",
                        "cloudsiem.sas.aliyuncs.com",
                        "cspm.sas.aliyuncs.com"
                    ]
                }
            }
        }
    ]
}
```

访问权限管理

最近更新时间：2024-07-22 10:44:31

本文档将指导您如何查看和使用云安全中心特定资源的权限，并指导您使用云安全中心控制台特定部分的策略。

操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略，使用户拥有在云安全中心（Cloud Security Center，CSC）控制台查看和使用特定资源的权限。

SOC 的全读写策略

如果您希望用户拥有**管理**云安全中心的权限，您可以对该用户使用名称为：QcloudSSAFullAccess 的策略，该策略通过让用户对云安全中心所有资源都具有操作权限，从而达到目的。可将预设策略 QcloudSSAFullAccess 授权给用户具体操作步骤，请参见 操作步骤 。

SOC 的只读策略

如果您希望用户拥有**查询**云安全中心的权限，但是不具有创建、删除、处理的权限，您可以对该用户使用名称为：QcloudSSAReadOnlyAccess 的策略，可将预设策略 QcloudSSAReadOnlyAccess 授权给用户，具体操作步骤，请参见 操作步骤 。

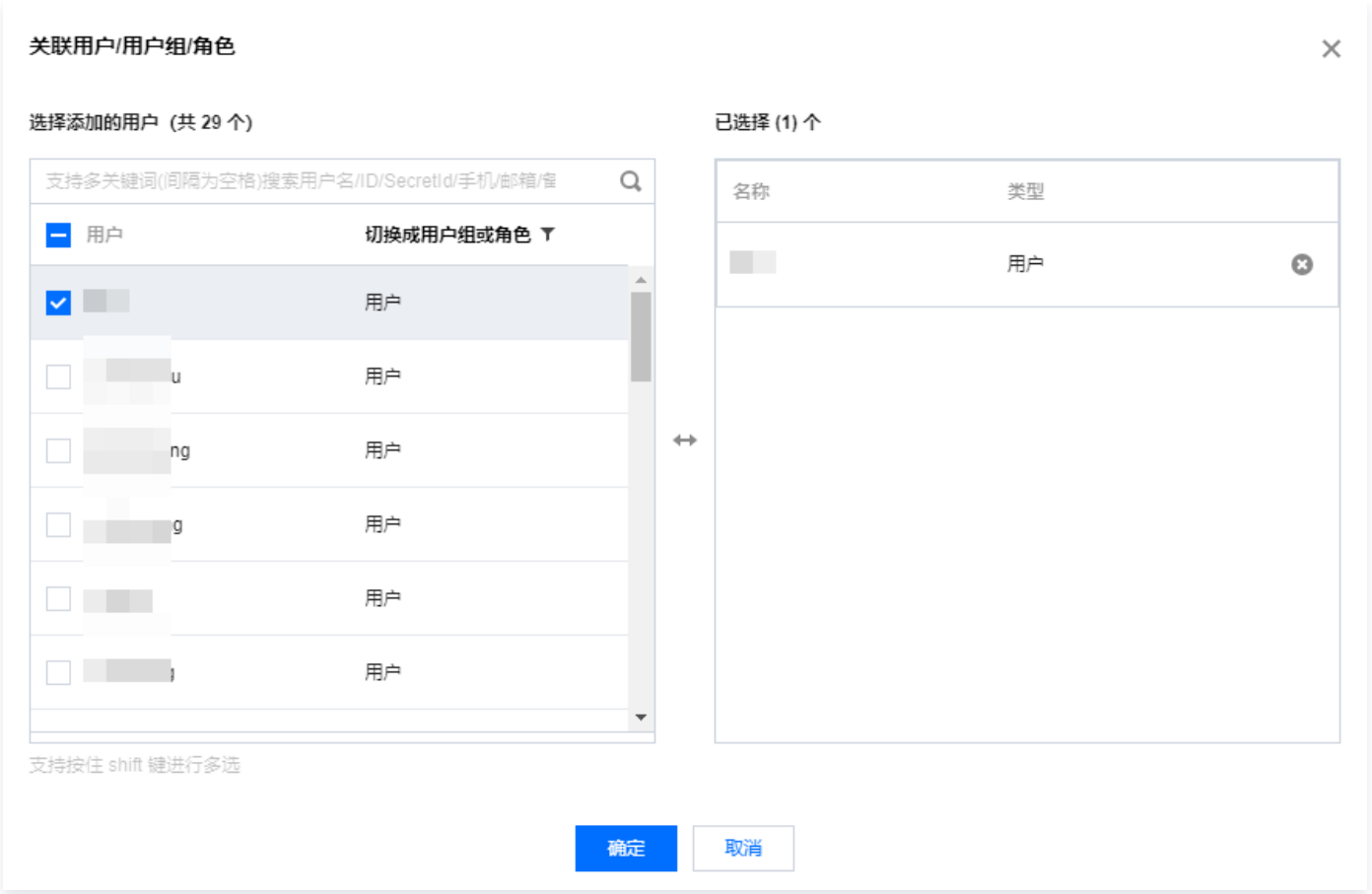
SOC 相关资源的策略

如果您希望用户拥有**使用**云安全中心云资产、合规管理、云安全配置、响应中心及 UBA 的权限，您可以对该用户使用名称为：QcloudAuditFullAccess 的策略。该策略通过让用户对操作审计所有资源都具有操作权限，从而达到目的，可将预设策略 QcloudSSAReadOnlyAccess 授权给用户，具体操作步骤，请参见 操作步骤 。

操作步骤

1. 登录 访问管理控制台，在左侧导航中，单击**策略**，进入策略页面。
2. 在策略页面的搜索框中，输入策略名称（根据实际需求搜索），如输入“QcloudSSAFullAccess”进行搜索。
3. 在“QcloudSSAFullAccess”策略的右侧操作栏中，单击**关联用户/组/角色**。

4. 在关联用户/用户组/角色页面，选中需要配置权限的子用户，单击**确定**即可。


关联用户/用户组/角色
选择添加的用户（共 29 个）
支持多关键词(间隔为空格)搜索用户名/ID/SecretId/手机/邮箱/备
用户
切换成用户组或角色
用户
用户
用户
用户
用户
用户
支持按住 shift 键进行多选
已选择 (1) 个
名称
类型
用户
确定
取消