云安全中心

云安全中心（旧版）

腾讯云

【联系我们】

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

文档目录

云安全中心（旧版）
产品简介
产品概述

最近更新时间：2025-04-25 18:54:42

什么是云安全中心

云安全中心（Cloud Security Center，CSC）是腾讯云一站式安全管理平台，通过资产中心、风险中心、告警中心、高级安全管理，帮助用户实现事前威胁检测、事中响应处置、事后溯源分析的安全运营闭环，一键搞定安全问题。

- 资产中心：支持管理34种云上资产。
- 风险中心：一键检测漏洞、配置不当等6大风险。
- 告警中心：聚合、关联分析日志和处置响应。
- 高级安全管理：集团账号统一纳管。

产品功能

资产中心

腾讯云公有云上自研的最全资产管理系统，支持自动同步腾讯云的34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。

风险中心

创建资产体检任务，检测端口风险、漏洞风险、弱口令风险、内容风险、云资源配置风险和服务暴露六大风险，并将以上风险信息分类进行管理。支持发起定时任务、周期任务，持续监测企业安全情况。

告警中心

云安全中心统一接入了云防火墙、Web 应用防火墙、主机安全、容器安全服务的日志数据，基于对告警日志的分析和聚合，将三道防线的告警统一展示，可以在告警中心统一处置以上产品的告警信息。

待办事项

为提升安全运营的效率，云安全中心智能分析和汇总了资产中心、风险中心和告警中心的信息，并整理为待办；单击待办可以进一步在各个产品进行处理。

体检任务

管理资产体检任务，对资产体检任务进行编辑、暂停、删除。

报告下载

对于已经完成的资产体检任务，云安全中心会自动生成 PDF 格式的安全报告，提供预览或下载。

日志审计

云安全中心原生接入云防火墙、Web 应用防火墙、主机安全、容器安全服务的日志，可以在日志审计页面根据日志字段，一站式检索以上安全产品的日志。

多账号管理

对于腾讯云集团账号用户，云安全中心支持通过多账号管理切换登录各账号、集中管理各账号的资产、告警、风险等信息。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。

应用场景

最近更新时间：2025-11-28 16:17:12

云上安全预防

适用场景

业务上云之后，由于公有云自身的特点以及业务上频繁的变更可能会带来很多威胁，例如云上服务器直接面向公网开放了 Telnet 访问；又例如云上数据库直接面向公网开放了服务访问，同时还未加密码验证。针对此类问题，需要对云上的各种安全情况进行集中的安全预防与检查。而云安全中心则集成了此类功能，可为客户提供完整的云上安全预防能力。

解决方案

云安全中心提供泄露监测、互联网攻击面测绘、云安全配置管理、漏洞管理四类功能对客户云上资源做集中的安全预防管理，分别覆盖云 API 密钥和关键信息泄露、云上服务暴露、云资源的配置风险、云服务器的漏洞问题四类云上主要安全问题。同时结合集中的云上资产管理能力，可以为客户提供全局的资产风险管理视角。

统一威胁运营

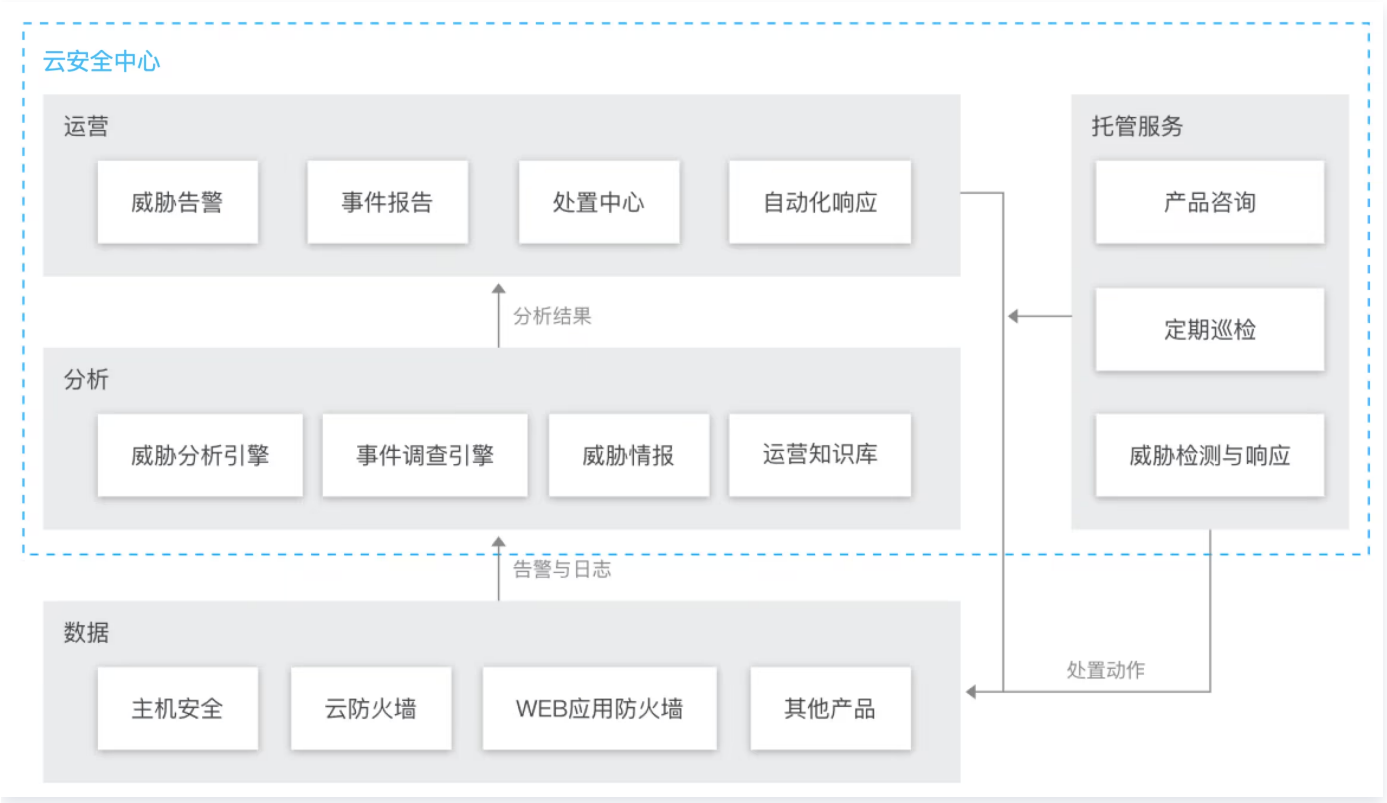
适用场景

云上威胁可能通过网络入侵、主机入侵等各种手段进入企业云上资产并造成进一步损失。为防御和检测威胁，主机安全、云防火墙、Web 应用防火墙往往是企业上云的必然选择，但也由此带来诸多问题：如告警众多并且管理分散、处置和封禁入口多样、无法有效进行处置、告警关系缺失导致无法按照攻击事件完整还原攻击过程等。这些问题都将直接造成威胁运营效率低下。

针对上述问题，腾讯云安全中心整合腾讯云主机安全、网络安全多方数据与能力，并将腾讯多年威胁分析经验和威胁情报数据应用于帮助客户进行威胁运营，解决威胁运营中的各类问题。

解决方案

威胁运营方案将以云安全中心为核心平台，采集并整合分析主机安全、云防火墙、Web 应用防火墙各类告警与日志，通过告警定性、事件调查、威胁情报分析等手段对告警进行集中分析，筛选高价值告警，针对失陷告警生成事件报告回溯整个攻击过程。
同时依靠云原生能力，云安全中心整合了主机安全、云防火墙、Web 应用防火墙、安全组等各类产品的处置与封禁能力，可以为企业客户提供集中处置、一键处置、自动处置，极大的提升威胁响应效率。腾讯云还可以提供云上威胁托管运营服务，帮助缺少运营人力和能力的客户进行实时威胁监测与响应。



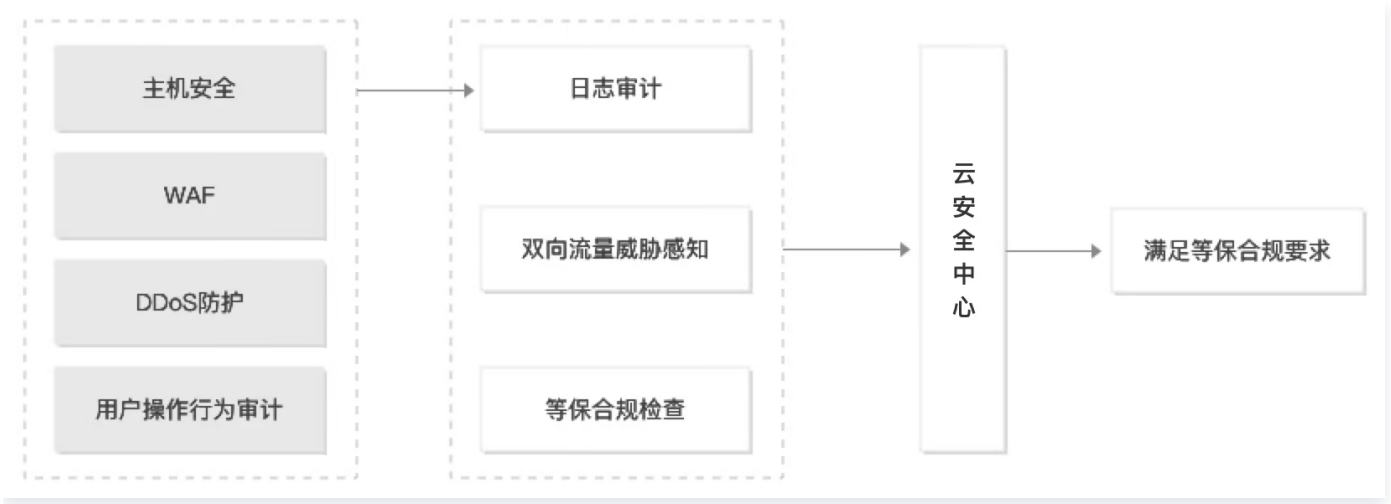
等保合规

适用场景

等级保护2.0标准正式实施后，以“一个中心三重防护”为核心框架针对云上合规的要求进行了进一步细化，对云上资产对外发起的攻击检测、日志审计及集中管理等要求都需要客户采取相应技术措施进行满足。同时针对安全管理方面提出的各项管理要求，也需要有相应的工具和产品帮助客户更容易且更有效地落地。

解决方案

云安全中心提供的等保自查、网络入侵检测、日志审计等功能，可以帮助客户有效满足等级保护合规要求。同时云安全中心可帮助客户实现等级保护标准要求中的安全管理中心相关要求的落地，在满足等保要求的基础上，切实提升客户云上安全水平。


主机安全
WAF
DDoS防护
用户操作行为审计
日志审计
双向流量威胁感知
等保合规检查
云安全中心
满足等保合规要求

高可用性

最近更新时间：2026-03-20 19:15:42

本文为您介绍云安全中心支持的地域及容灾能力，帮助您了解服务的高可用保障。

概念说明

在了解容灾能力前，请先了解地域和可用区的基础概念，请参见 地域和可用区 。

支持地域

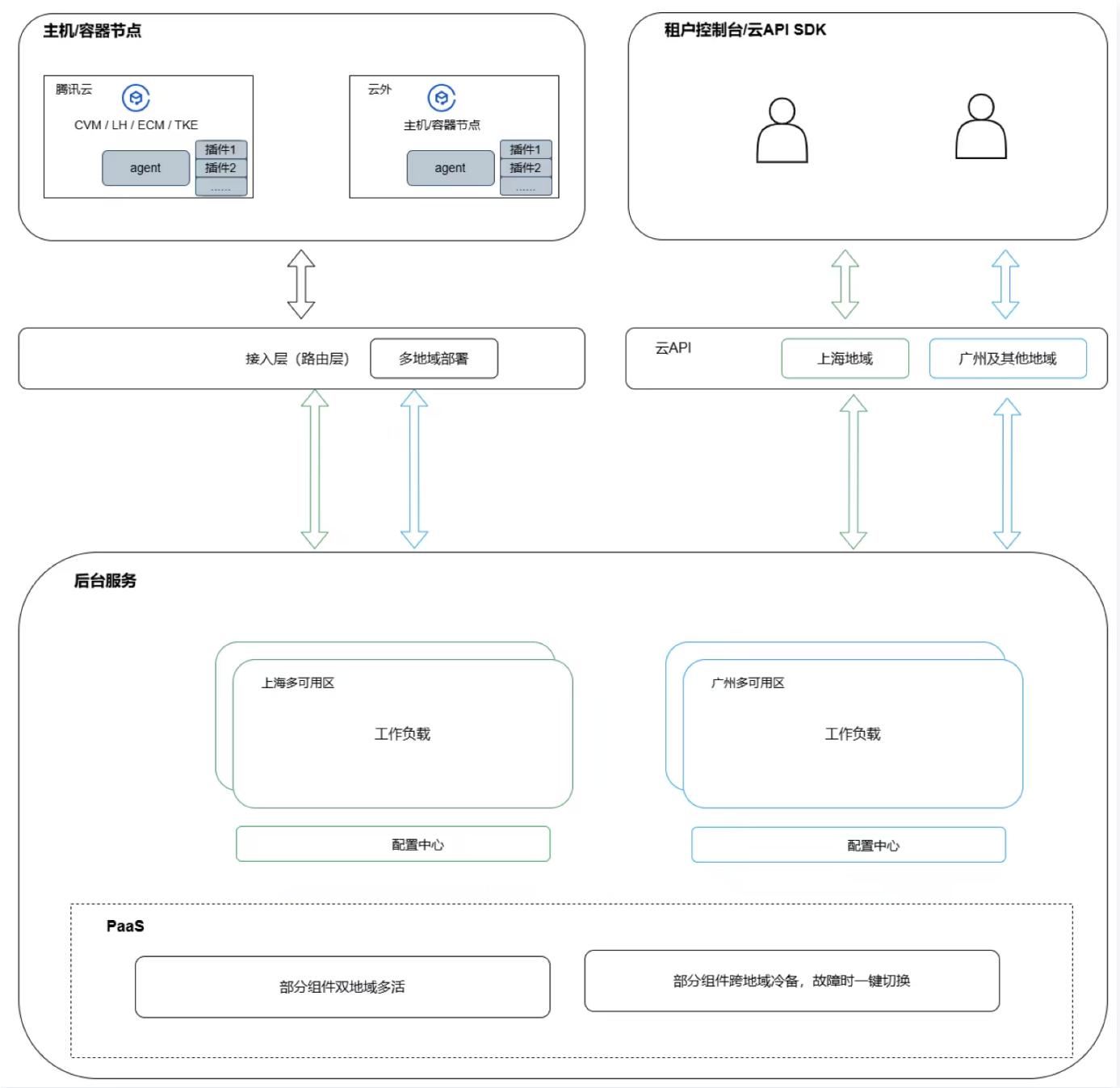
云安全中心服务在当前腾讯云支持的地域和可用区中，产品功能保持一致，不因云服务器所在地域或可用区的不同而有所差异，仅底层部署和容灾架构存在差异。

容灾能力

云安全中心当前已支持以下两种容灾模式。服务可用性标准请参见 云安全中心服务等级协议 。

跨地域容灾

工作负载和部分 PaaS 支持异地双活，部分 PaaS 支持异地冷备故障一键切换，目前已支持广州和上海地域。



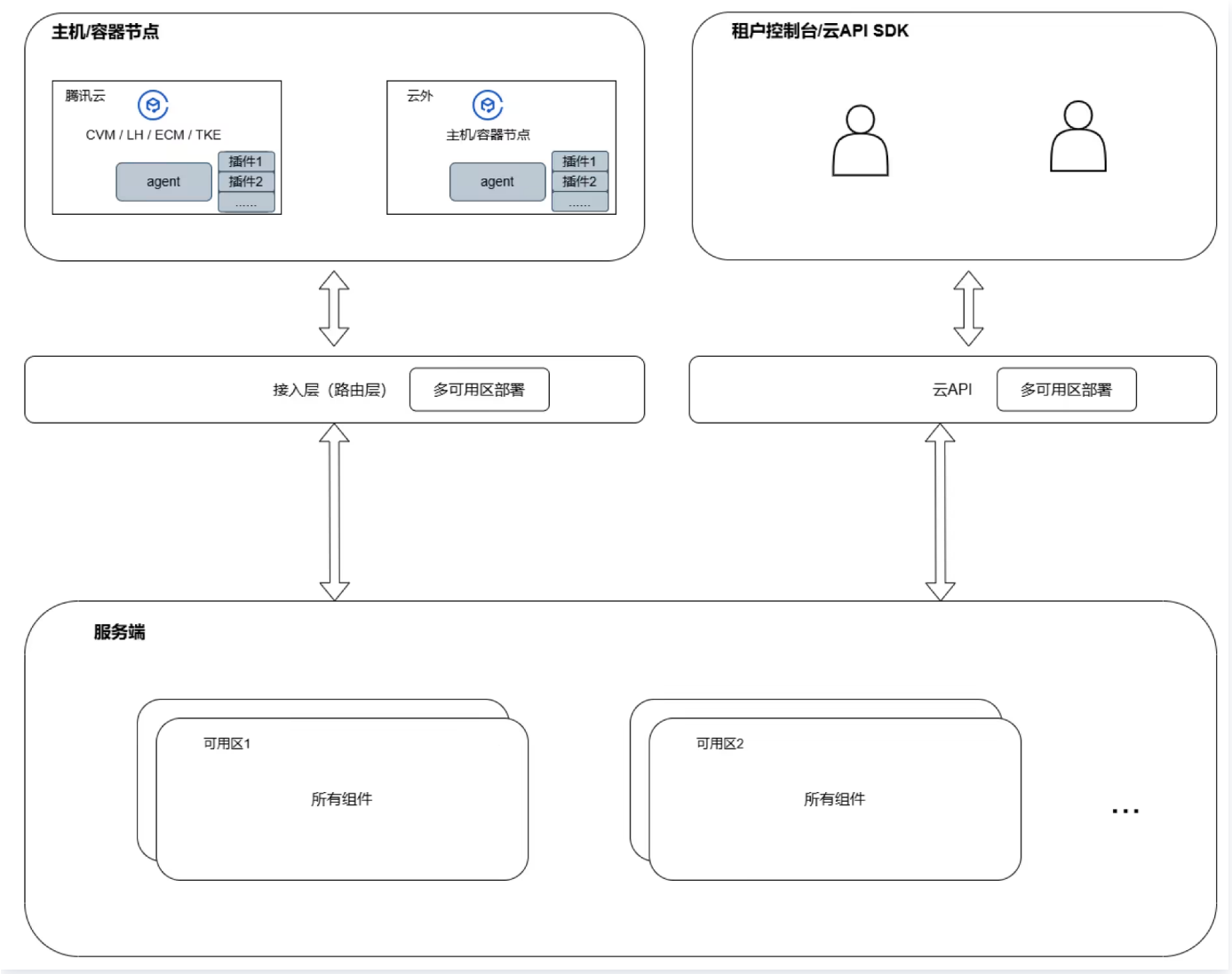
架构说明：

- **采用双地域多可用区多活架构。**
- **部分 PaaS 组件采用双地域冷备策略，故障时支持一键切换。**
- **单地域部分可用区故障：可用性不受影响，自动切换到其他可用区。**
- **单地域全部可用区故障：可用性短时降低，一键切换后可快速恢复服务。**

> **说明：**
> 一键切换由腾讯云运维人工操作。

跨可用区双活容灾

多个可用区同时提供服务，任一可用区故障时其他可用区可自动接管，目前已支持广州、上海及新加坡地域。



架构说明：

- 接入层（路由层）、云 API 和服务端均采用多可用区部署。
- 任一可用区故障时，系统自动将流量切换到其他可用区。

购买指南
计费概述

最近更新时间：2026-05-07 09:49:32

版本说明

腾讯云安全中心为用户提供三个付费版本，分别是高级版、企业版和旗舰版。每个版本按照功能和默认规格划分，以适应不同规模和需求的客户。计费详情如下：

计费相关		免费版	高级版	企业版	旗舰版	弹性拓展
基础价格		-	1,800元/月	4,800元/月	12,800元/月	-
可购买时长		-	6个月、1年、2年、3年	3个月、6个月、1年、2年、3年		-
折扣		-	• 购买6个月及以下：无折扣 • 购买1年：85折 • 购买2年：7折 • 购买3年：5折			-
资产与风险管理	资产管理	支持	支持	支持	支持	-
	资产体检	-	400次/月	1,200次/月	4,800次/月	4元/次/月，拓展步长300次
	扫描任务管理	1	10	20	50，可扩展至不限制	-
	云暴露面	-	-	-	支持	-
	端口扫描	支持	支持	支持	支持	-
	应急漏洞扫描	-	支持	支持	支持	-
	深度漏洞扫描	-	支持	支持	支持	-

	弱口令扫描	-	支持	支持	支持	-
	云资源配置检查	-	支持	支持	支持	-
攻击与告警处置	告警接入	-	支持	支持	支持	-
	告警聚合、事件调查与关联分析	-	支持	支持	支持	-
	处置能力（依赖其他安全产品）	-	支持	支持	支持	-
管理	安全报告	-	支持	支持	支持	-
	日志投递（投递Ckafka）	-	-	-	支持	-
	日志接入	-	支持	支持	支持	-
	多账号管理	-	-	-	可扩展	3,000元/账号/月，超过10个不额外收费，若成员账号已购买旗舰版，则多账号功能免费

选型指引

云安全中心是一站式的云上安全管理平台，根据不同用户的需求场景提供高级版、企业版和旗舰版三种套餐，建议您从云上资产数、集团账号、日志审计、重要时期安全保障四个角度选择最适合您需求场景的套餐：

功能类型	高级版	企业版	旗舰版
云上资产数，例如：公网 IP、域名资产的数量	100	300	900及以上
集团账号，是否使用腾讯云集团账号解决方案	否	否	是
重要时期安全保障，是否需要进行互联网攻防演练	否	是	是

资产体检说明

- 云安全中心支持对资产进行安全体检，涵盖端口、弱口令、应急漏洞、深度漏洞、服务暴露、网站内容风险、云资源配置等方面。
- 每次体检会消耗资产体检次数，即1次扫描1个资产（例如：公网 IP、域名）消耗1资产/次，云安全中心高级版、企业版、旗舰版分别包含400、1200、4800个资产体检数，支持付费扩展。
- 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。

增值服务计费说明

云 API 异常监测

计费策略：（基础服务计费 + AK 资产数计费*当前 APPID 下全部 AK 资产数）*服务时长

基础服务计费	AK 资产数计费
6,000元/月	100元/个/月

计费示例：
账号 A 下有4个 AK，购买云 API 异常监测服务2个月，所付金额为（6000 + 100*4）*2 = 12,800（元）。

多账号场景说明
多账号管理员可为其成员账号统一购买服务，选择多成员时只需支付一次基础服务费用，AK 资产数费用按选择的多成员账号 AK 资产总数计算，付费的 AK 资产数作为配额在账号间共享。

其他情况说明如下：

场景	订单归属	服务可用性	配额共享	购买限制
多账号管理员为其成员账号统一购买服务	管理员账号	管理员与成员默认均可用该服务	管理员与成员账号间配额共享	成员账号不可再单独购买该服务
成员账号单独购买服务 管理员账号单独购买服务	分别归属于成员账号、管理员账号	成员默认可用该服务，管理员可见成员数据	单独购买的成员账号与管理员统一购买的账号间配额不共享	管理员不可再为该成员统一购买服务，不可管理该成员订单

示例

1. **计费示例：**

   账号 A下有2个成员账号 B 和 C。A、B、C 账号下 AK 资产数分别为2、5、3，A 统一为 B、C 购买云 API 异常监测服务2个月，所付金额为（6000 + 100*10）*2 = 14,000（元）

2. **配额共享示例：**

   账号 A 下有2个成员账号 B 和 C。A、B、C 账号下 AK 资产数分别为2、5、3。

   - A 统一为 B、C 购买云 API 异常监测服务，付费资产数为10（配额为10），配额共享。若 A 的 AK 资产数由2变为0，B 的资产数由5变为7，三个账号总配额数仍为10，不需要进行扩容。
   - A 统一为 B 购买云 API 异常监测服务，付费资产数为7（配额为7）；C单独购买服务，付费资产数为3（配额为3）。A 与 B 间配额共享，与 C 间配额不共享。若 A 的 AK 资产数由2变为0，C 的资产数由3变为5，A 不需要进行扩容；C资产数超出配额2，需变配扩容。

DNS 威胁监测

计费策略：基础服务计费 * 服务时长 + 按 DNS 解析数后付费

服务器数量（当前覆盖类型：CVM、ECM）	基础服务计费	按 DNS 解析数后付费
大于等于0，小于50	3,000元/月	每月自带100万次 DNS 解析数（全部服务器共用），超出部分100元/1,000万次/月后付费（100亿次请求封顶，不额外收费）
大于等于50，小于100	4,000元/月	
大于等于100，小于200	5,000元/月	
大于等于200，小于500	6,000元/月	
大于等于500，小于1,000	7,000元/月	
大于等于1,000，小于2,000	8,000元/月	
大于等于2,000，小于5,000	9,000元/月	
5,000及以上	10,000元/月	

计费示例：

账号 A 下有40个 CVM 服务器，购买 DNS 威胁监测服务1个月，该月 DNS 解析量7,700万，所付金额为 3,000 * 1 +（77,000,000−1,000,000）/10,000,000 *100 = 3,760（元）。

多账号场景说明

多账号管理员可为其成员账号统一购买服务，选择多成员时只需支付一次基础服务费用，服务器数量按选择的多成员账号资产总数计算，基础服务包含的资产数作为配额在账号间共享。

其他情况说明如下：

场景	订单归属	服务可用性	配额共享	购买限制
多账号管理员为其成员账号统一购买服务	管理员账号	管理员与成员默认均可用该服务	管理员与成员账号间配额共享	成员账号不可再单独购买该服务
成员账号单独购买服务 管理员账号单独购买服务	分别归属于成员账号、管理员账号	成员默认可用该服务，管理员可见成员数据	单独购买的成员账号与管理员统一购买的账号间配额不共享	管理员不可再为该成员统一购买服务，不可管理该成员订单

示例

1. **计费示例：**

   账号 A 下有2个成员账号 B 和 C。A、B、C 账号下服务器数分别为20、60、10，A 统一为 B、C 购买 DNS 威胁监测服务2个月，所付基础服务金额为4,000 *2 = 8,000（元）

2. **配额共享示例：**

   账号 A 下有2个成员账号 B 和 C。A、B、C 账号下 AK 资产数分别为20、60、10。

   - A 统一为 B、C 购买DNS威胁监测服务，资产总数90（基础服务对应资产数为大于等于50，小于100），配额共享。若 A 的资产数由20变为25，B 的资产数由60变为61，三个账号总资产数仍小于100，不需要进行扩容。
   - A 统一为 B 购买DNS威胁监测服务，资产总数为80（基础服务对应资产数为大于等于50，小于100）；C 单独购买服务，资产数为10（基础服务对应资产数为大于等于0，小于50）。A 与 B 间配额共享，与 C 间配额不共享。若 A 的资产数由20变为25，C 的资产数由10变为60，A 不需要进行扩容；C 资产数超出基础服务对应资产数，需变配扩容。

数据安全态势管理（数据库风险监测）

计费策略：（基础服务版本 + 扩展包）* 服务时长

计费项	规格	单价
专业版	3 个数据库实例； 吞吐量峰值 8,000 条 SQL/秒； 2 亿条在线 SQL 存储； 0.5 B 日志存储空间。	5,800 元/月
日志存储扩展包	1 TB 日志存储	1,000 元/月
数据库实例扩展包 （每 1 个数据库实例扩展包，包含： 1 个数据库实例； 1,000 条 SQL 秒吞吐量； 2,000万 条在线 SQL 语句存储 0.1 TB 日志存储空间。）	0 – 20 个	1,800 元/个/月
	21 – 50 个	1,700 元/个/月
	51 – 100 个	1,600 元/个/月
	101 – 200 个	1,500 元/个/月
	201 – 300 个	1,400 元/个/月
	301 – 400 个	1,300 元/个/月
	401 – 500 个	1,200 元/个/月
	500 以上（不含 500）	1,000 元/个/月

计费示例：
账号 A 下有 4 个 数据库资产需要纳管，购买数据安全态势管理（数据库风险监测）专业版服务 3 个月，另外加购一个数据库实例扩展包，所付金额为（5,800 + 1,800）* 3 = 22,800（元）。

多账号场景说明

多账号管理员可为其成员账号统一购买服务，选择多成员时只需支付一次基础服务费用，AK 资产数费用按选择的多成员账号 AK 资产总数计算，付费的 AK 资产数作为配额在账号间共享。

其他情况说明如下：

场景	订单归属	服务可用性	配额共享	购买限制
多账号管理员为其成员账号统一购买服务	管理员账号	管理员与成员默认均可用该服务	管理员与成员账号间配额共享	成员账号不可再单独购买该服务
成员账号单独购买服务 管理员账号单独购买服务	分别归属于成员账号、管理员账号	成员默认可用该服务，管理员不可见成员数据	单独购买的成员账号与管理员统一购买的账号间配额不共享	管理员不可再为该成员统一购买服务，不可管理该成员订单

示例

1. **计费示例：**

   账号 A 下有 2 个成员账号 B 和 C，A 需管理 2 个数据库、B 需管理 2 个数据库、C 需管理 1 个数据库，总计需管理 5 个数据库。购买数据安全态势管理（数据库风险监测）专业版服务 3 个月，同时需额外购买 2 个数据库实例扩展包（专业版默认包含 3 个数据库，5−3=2），所付金额为（5,800 + 1,800 * 2）* 3 = 28,200（元）。

2. **配额共享示例：**

- **示例 1（“A 购买服务并为 B、C 统一购买” 的共享场景）：**

  账号 A 下有成员 B、C，A、B、C 需管理的数据库数量分别为 2、2、1，总计 5 个。
  A 统一为 B、C 购买数据安全态势管理（数据库风险监测）服务：选择专业版 + 2 个数据库实例扩展包，对应配额为 “数据库实例 5 个、日志存储 0.7 T（0.5 T+0.1 T×2）、在线 SQL2.4 亿（2.0 亿 + 0.2 亿 ×2）”，配额在 A、B、C 间共享。
  若后续 A 的数据库数量变为 1、B 的数据库数量变为 3，三者总数据库数量仍为 1+3+1=5，未超出配额，无需扩容；若日志存储需求从 0.7 T 增至 0.8 T，超出当前日志存储配额，需购买 1 个日志存储扩展包扩容。

- **示例 2（对 “A 为 B 购买、C 单独购买” 的部分共享场景）：**

  账号 A 下有成员 B、C，A 为 B 购买数据安全态势管理（数据库风险监测）服务（专业版 + 1 个数据库实例扩展包，配额：数据库实例 4 个、日志存储 0.6 T、在线 SQL 2.2 亿），配额在 A、B 间共享；C 单独购买专业版（配额：数据库实例 3 个、日志存储 0.5T、在线 SQL 2.0 亿），与 A、B 配额不共享。
  若 A 的数据库数量变为 0、B 的数据库数量变为 4，A+B 总数据库数量为 4，未超配额，无需扩容；若 C 的数据库数量变为 4，超出自身 3 个的数据库实例配额，需购买 1 个数据库实例扩展包扩容。

数据安全态势管理（对象存储异常监测）

计费策略：基础服务计费（按对象存储数量梯度计费）*服务时长 + 日志处理计费

对象存储数量	基础服务计费	按日志处理量后付费
大于等于0，小于50	6,000元/月	每月自带1000万条日志处理数，超出部分100元/1000万条
大于等于50，小于100	7,000元/月	
大于等于100，小于200	8,000元/月	
大于等于200，小于500	9,000元/月	
500及以上	10,000元/月	

计费示例：

账号 A 下有 70个对象存储，购买对象存储异常监测服务1个月，日志处理量为5000万，所付金额为7,000*1 +（5000−1000）/1000 *100 = 7,400（元）。

相关操作

支持选择监测的对象存储范围（全部/自选），可随时在控制台开启/关闭对象存储的监测，开启监测的对象存储将会进行异常调用、权限风险等监测。若勾选【新增自动监测】，后续账号下新增对象存储资产时，将自动开启监测。若剩余可监测数量不足将自动关闭，可在扩容后手动开启。

多账号场景说明

多账号管理员可为其成员账号统一购买服务，选择多成员时只需支付一次基础服务费用，对象存储数量按选择的多成员账号 对象存储资产总数计算，所在阶梯的对象存储资产数作为配额在账号间共享。

其他情况说明如下：

场景	订单归属	服务可用性	配额共享	购买限制
多账号管理员为其成员账号统一购买服务	管理员账号	管理员与成员默认均可用该服务	管理员与成员账号间配额共享	成员账号不可再单独购买该服务
成员账号单独购买服务 管理员账号单独购买服务	分别归属于成员账号、管理员账号	成员默认可用该服务，管理员可见成员数据	单独购买的成员账号与管理员统一购买的账号间配额不共享	管理员不可再为该成员统一购买服务，不可管理该成员订单

示例

1. **计费示例：**

   账号 A下有2个成员账号 B 和 C。A、B、C 账号下 对象存储 资产数分别为20、50、30，A 统一为 B、C 购买对象存储监测服务2个月，所付预付费金额为8,000*2 = 16,000（元）

2. **配额共享示例：**

   账号 A 下有2个成员账号 B 和 C。A、B、C 账号下对象存储资产数分别为20、50、30。

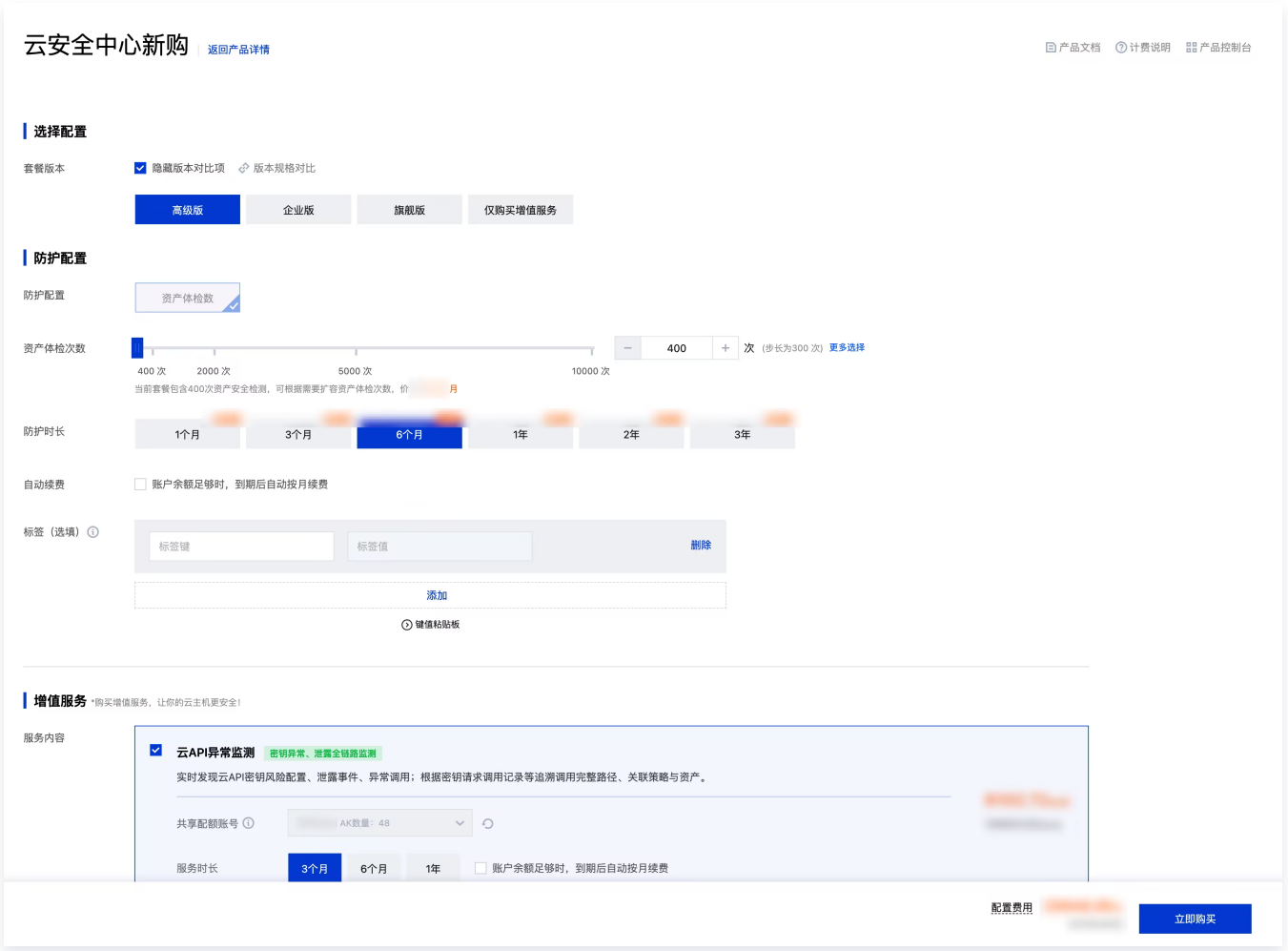
   - A 统一为 B、C 购买对象存储异常监测服务，基础服务对应资产数为100（配额为100），配额共享。若 A 的 对象存储资产数由20变为0，B 的资产数由50变为70，三个账号总配额数仍为100，不需要进行扩容。
   - A 统一为 B 购买对象存储异常监测服务，基础服务对应资产数为70（配额为70）；C单独购买服务，基础服务对应资产数为30（配额为30）。A 与 B 间配额共享，与 C 间配额不共享。若 A 的对象存储资产数由20变为0，C 的资产数由30变为50，A 不需要进行扩容；C资产数对应新的基础服务梯度，需变配扩容。

购买方式

最近更新时间：2025-12-24 17:15:52

云安全中心按照套餐版本（可选仅购买安全服务）+防护配置的方式进行购买。

1. 进入 云安全中心购买页，根据需求选择套餐版本，或者按您的需求设置购买内容，系统会为您自动计算所需费用。



2. 选择完毕后，单击立即购买，完成支付流程即购买成功。

续费说明

最近更新时间：2023-04-27 11:24:49

云安全中心资源在到期后14天会被销毁（详情请参见 云安全中心-欠费说明 ）。为保证服务能稳定正常运行，需要您关注云安全中心套餐到期时间，并注意在到期前进行续费。建议您将云安全中心设置为到期自动续费，您也可以在 云安全中心续费页面 或 费用中心 对资源进行手动续费。

欠费说明

最近更新时间：2023-04-27 11:24:50

- 产品到期当天，云安全中心套餐将被调整为免费版。
- 产品功能和规格将调整为免费版套餐，深度漏洞扫描、弱口令扫描、云资源配置检查等付费功能将无法使用。
- 产品到期14天后，系统回收所有云安全中心的资源，删除配置信息且配置信息无法恢复，只能重新购买后再次进行配置。

退费说明

最近更新时间：2025-04-25 18:54:42

如果您未使用云安全中心产品，在购买5天内，云安全中心支持5天内无理由退货退款。
使用云安全中心产品是指使用过云安全中心的功能，包括但不限于资产体检等；以下举例情况均属于已使用产品、不属于5天无理由退款范围：

- 购买云安全中心产品后，进行过资产体检任务。
- 购买云安全中心产品后，下载过安全体检报告。

退款途径

用现金购买的现金券以及购买产品时使用的优惠券（代金券/折扣券）不支持退还，购买产品时使用的非优惠券费用按支付方式（现金/赠送金/现金券）及支付比例退还到支付方腾讯云账户。

退款方式

确认符合5天无理由退款规则后，您可以 提交工单 申请退货退款。

快速入门

最近更新时间：2024-02-26 11:32:41

步骤1：登录注册

登录 腾讯云官网 。若没有账号，请参考 账号注册教程 ，进行账号注册。

步骤2：立即体验

进入 云安全中心控制台 ，即可使用云安全中心免费版，对云上资产安全情况进行盘点，对云上安全产品的安全事件进行统一监测。

步骤3：使用云安全中心

开通云安全中心高级版 后，即可使用云安全中心完整功能，实现云上安全的一站式自动化及可视化安全运营管理。

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

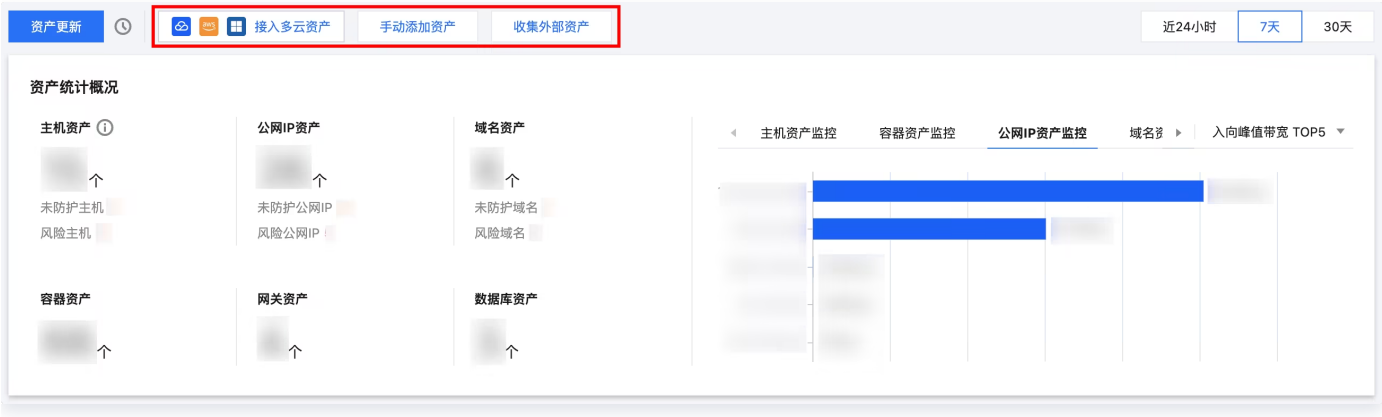
1. 在 资产中心页面，选择目标资产，单击资源标签列下的，可以添加自定义产品标签。

2. 在编辑标签弹窗中，选择标签键和标签值，单击**确定**。

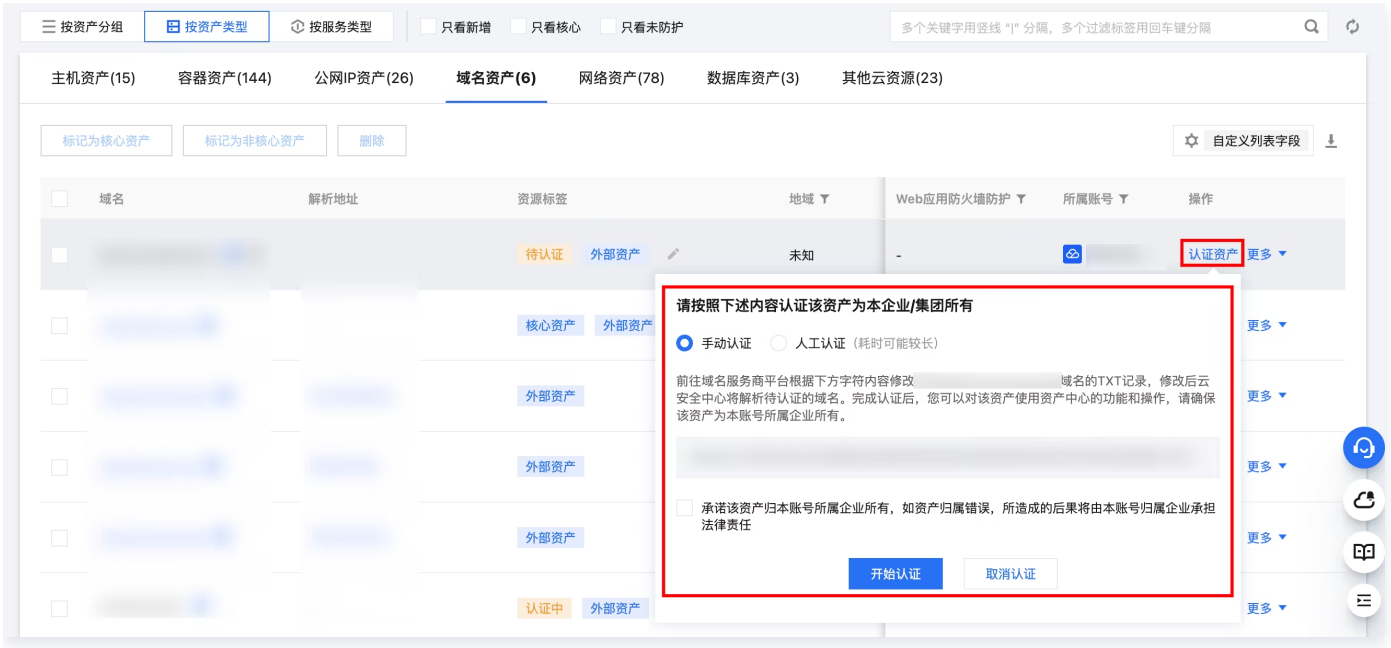
3. 添加标签后，单击**资源标签**，可以按照自定义标签分类查看资产。

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**。

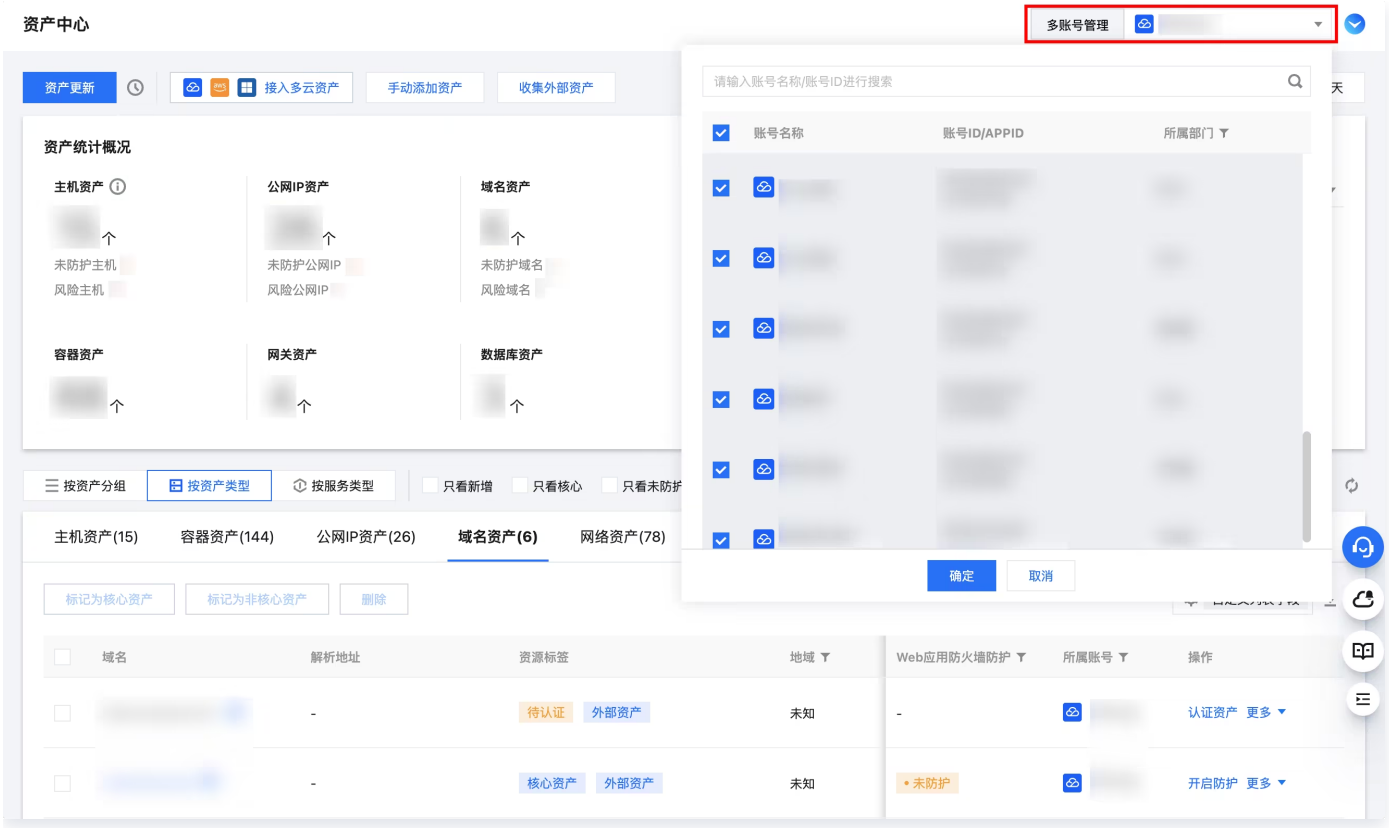
- 在收集外部资产弹窗中，开启外部资产收集开关，开启后，云安全中心将会使用腾讯安全网络空间资产发现和情报信息收集能力，主动获取您所在企业的外部资产，并自动导入到对应资产列表中；输入企业关键词（为确保收集信息的准确性，建议输入企业或集团的注册公司名称、主站域名或证书），勾选服务协议，单击**确定**。

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。


资产中心
多账号管理
资产更新
接入多云资产
手动添加资产
收集外部资产
资产统计概况
主机资产
公网IP资产
域名资产
未防护主机
风险主机
未防护公网IP
风险公网IP
未防护域名
风险域名
容器资产
网关资产
数据库资产
请输入账号名称/账号ID进行搜索
账号名称
账号ID/APPID
所属部门
确定
取消
按资产分组
按资产类型
按服务类型
只看新增
只看核心
只看未防护
主机资产(15)
容器资产(144)
公网IP资产(26)
域名资产(6)
网络资产(78)
标记为核心资产
标记为非核心资产
删除
域名
解析地址
资源标签
地域
Web应用防火墙防护
所属账号
操作
待认证
外部资产
未知
认证资产
更多
核心资产
外部资产
未知
未防护
开启防护
更多

安全体检
功能简介

最近更新时间：2025-12-17 16:46:21

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5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

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、边缘服务器	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、风险服务暴露
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	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	-	-	✓	✓
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

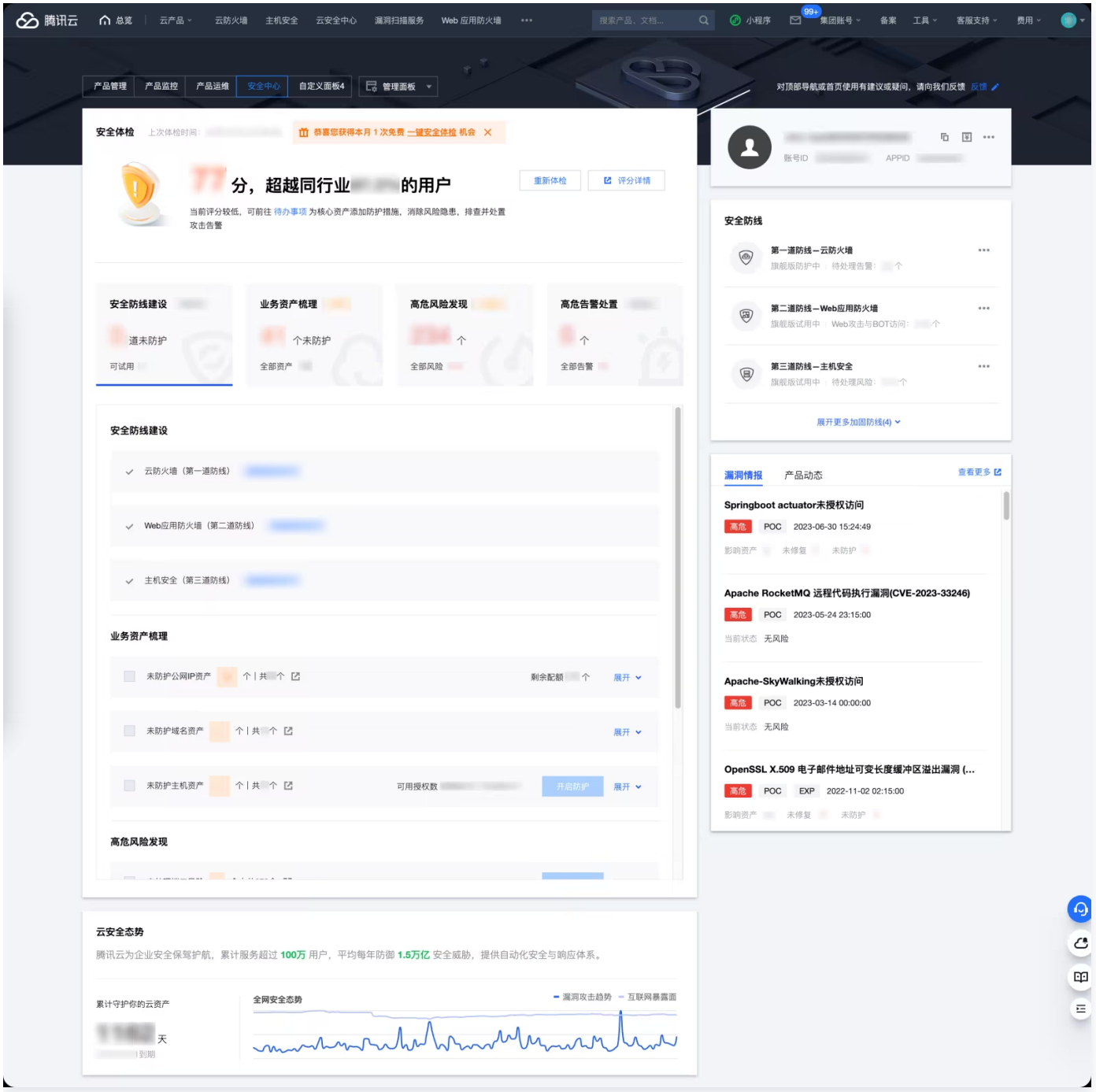
安全体检入口

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

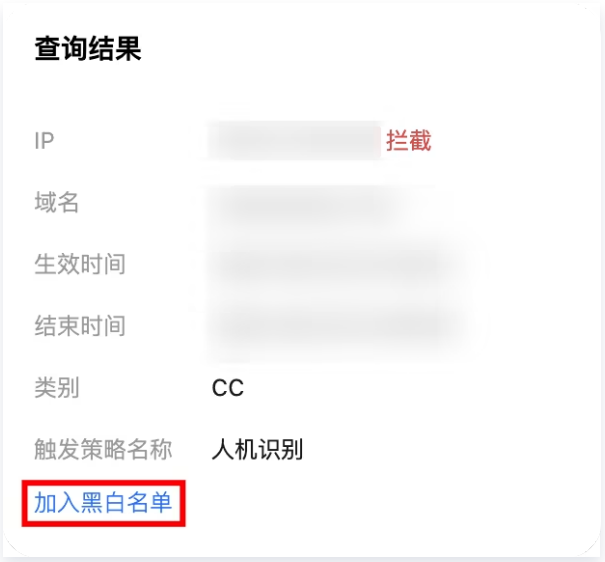
> **说明**
>
> - 适用于腾讯云 Web 应用防火墙，如果您使用的是其他 WAF 产品，请自行添加。
> - 已购买 Web 应用防火墙 。
> - 完成防护域名的添加及正常接入，当前域名处于正常防护，且开启 BOT 管理规则总开关，详情请参见 快速入门 。

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：2025-12-11 14:40:12

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，网络安全等级保护三级技术要求	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。
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	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。

				护三级技术要求	
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	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。

库不建议对公网开放访问					
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	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。

				级技术要求	
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	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

				范，网络安全等级保护三级技术要求	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，网络安全等级保护三级技术要求	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，

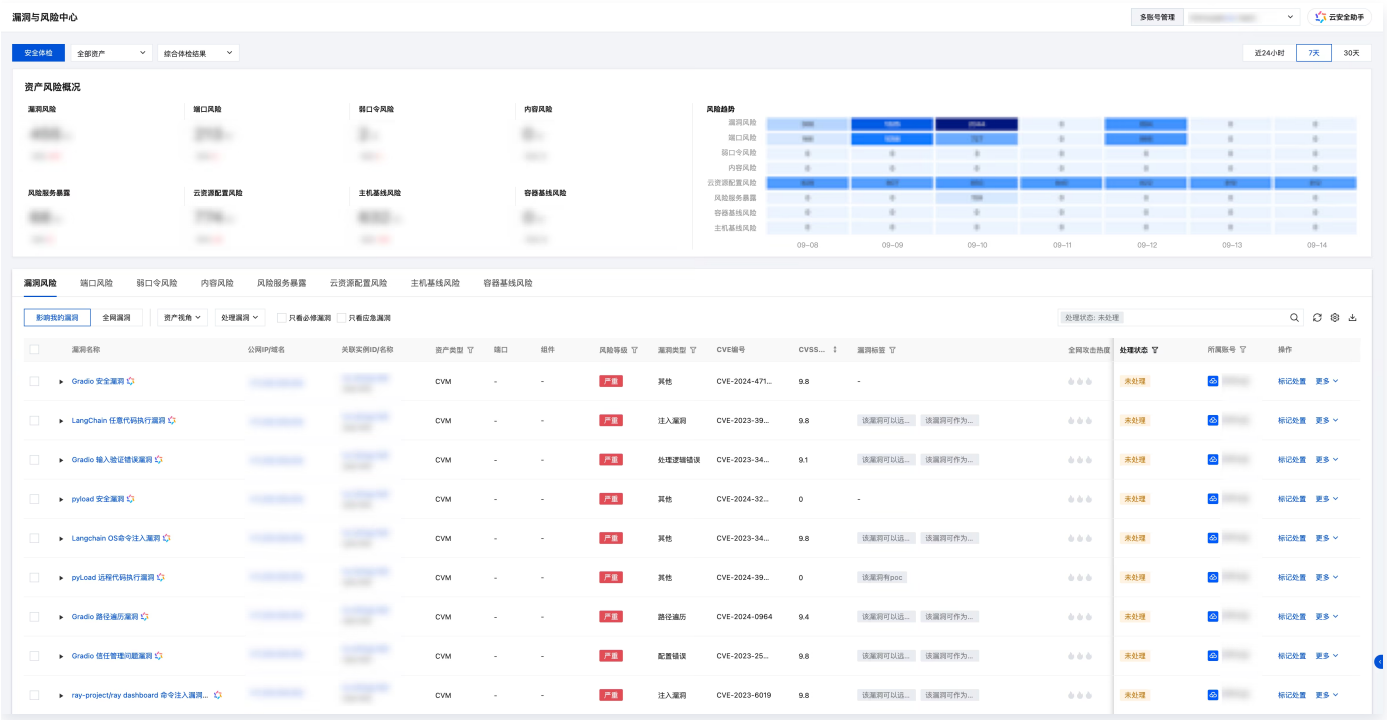
					再增加一层保护，登录保护可使用腾讯云虚拟 MFA 设备，降低主账号被恶意登录的可能性。
主账号应使用 MFA 进行操作保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，MFA（Multi-Factor Authentication）即多因子认证，是一种简单有效的安全认证方法，它可以在用户名和密码之外，再增加一层保护，操作保护中启用虚拟 MFA，可为您的敏感操作提供二次校验，降低误操作或恶意操作的风险。
主账号应开启登录保护	基础安全防护	account	高危	默认安全规范	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。

漏洞与风险中心

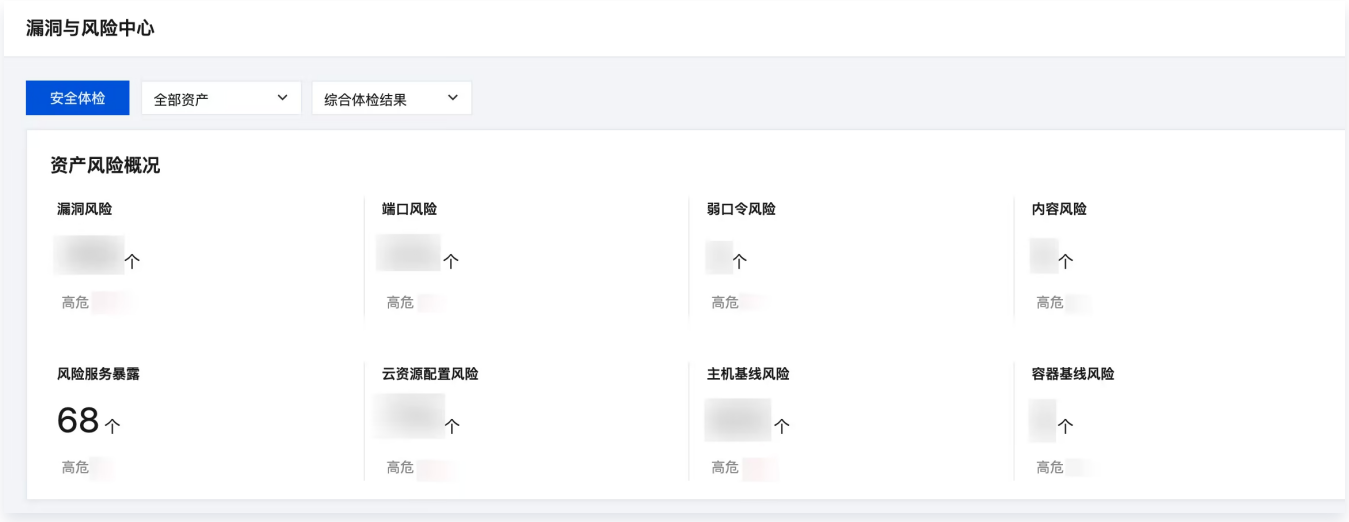
最近更新时间：2025-09-17 21:26:21

漏洞与风险中心功能展示了现有资产的风险数据，支持检测的风险类型包括漏洞风险、端口风险、弱口令风险、风险服务暴露、云资源配置风险、主机&容器基线风险。统计了当前风险概况，有助于快速定位具体风险，进行风险处理。

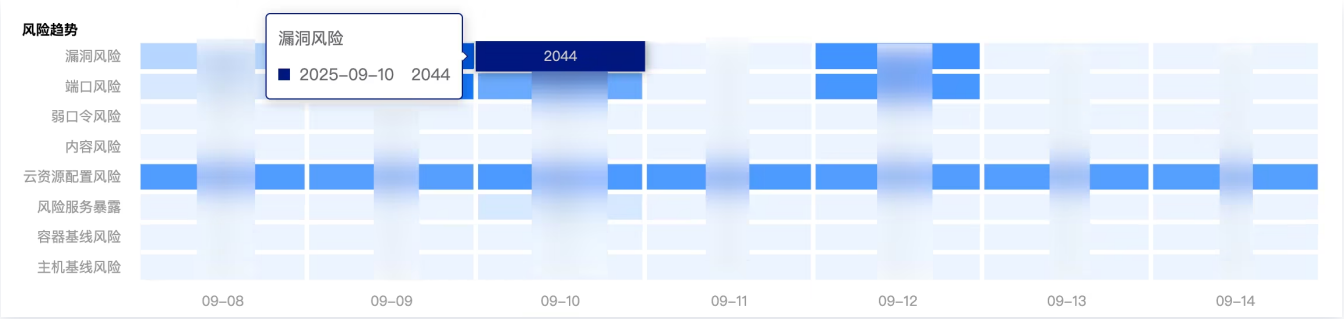


查看风险概况

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. 在漏洞与风险中心页面，查看风险概况，支持按照**资产**与**扫描任务**进行筛选。
3. 选择风险类型，单击**数字**，页面下方切换显示对应的风险类型详情；单击**高危数字**，页面下方切换显示对应的高危风险类型详情。

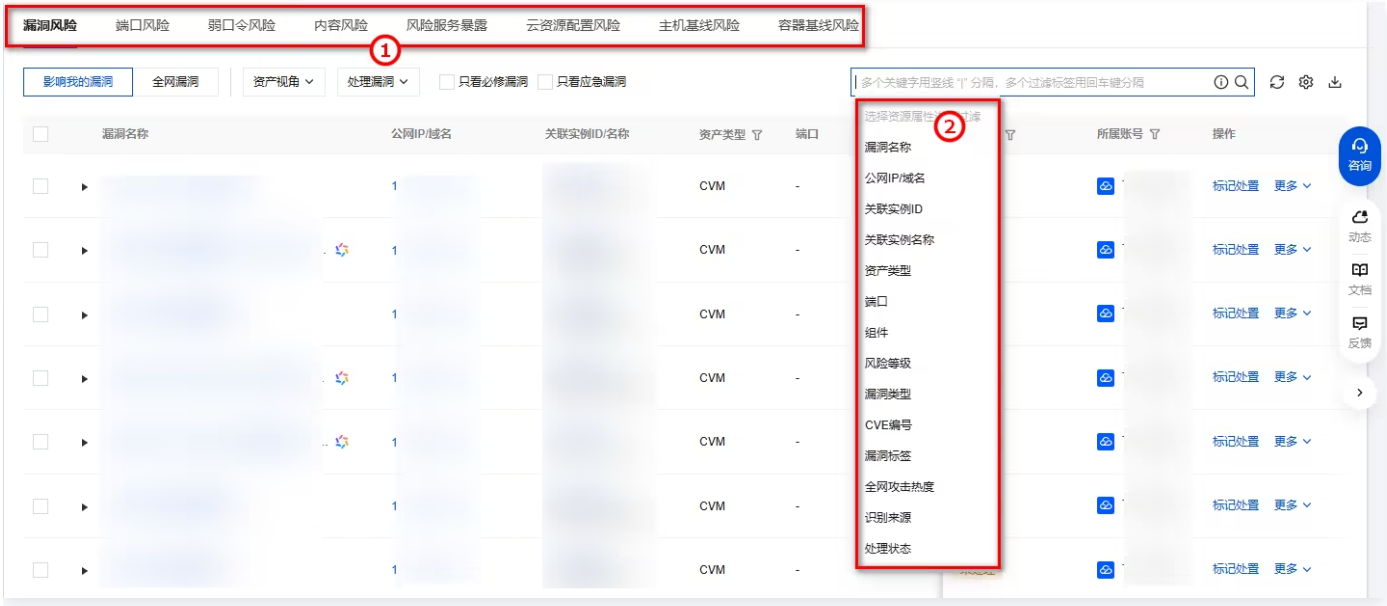


4. 在风险趋势中，可查看不同时间段内的风险数量，鼠标悬浮在图中数字上，可显示扫描时间、风险数量。



查看不同类型风险详情

在 漏洞与风险中心页面，单击①**风险类型**可查看各类风险详情，默认显示未处理的风险。单击②**条件筛选框**可重置筛选条件，显示全部风险内容。



> **说明：**
> 以漏洞风险为例。

影响我的漏洞

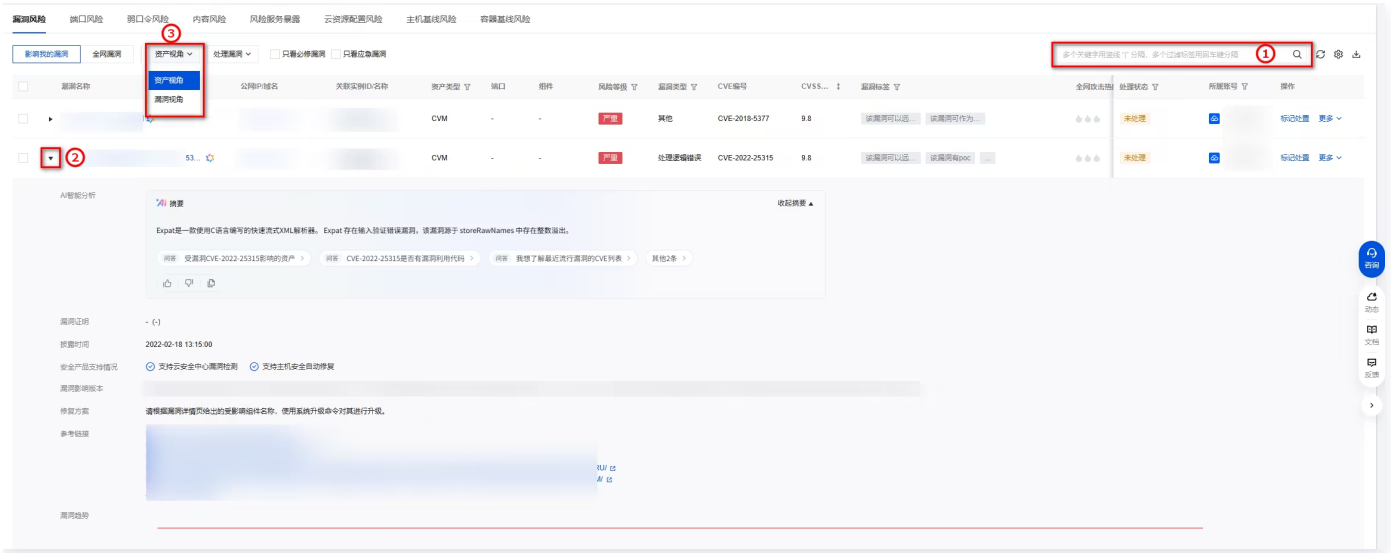
在影响我的漏洞页签，查看已扫描资产的漏洞风险，包括漏洞名称、影响资产、风险等级、端口组件、漏洞类型、CVE 编号、扫描时间、处理状态等。

①单击**搜索框**，以关键字对风险进行筛选定位。

②单击漏洞名称旁边的▶，查看漏洞详情。

③支持切换显示视角。

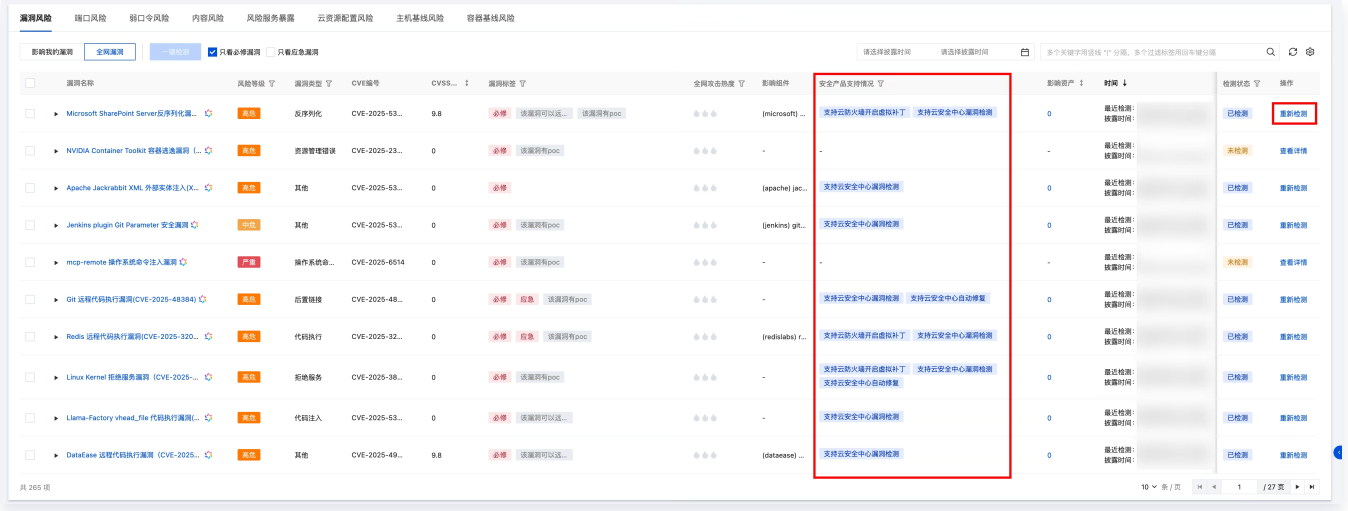
- 资产视角：以资产为单位显示每个资产的漏洞风险。
- 漏洞视角：以漏洞为单位显示每种漏洞影响的资产数量与端口，单击**影响资产数栏的数字**，跳转至**资产视角**中该漏洞风险所影响的资产信息。



全网漏洞

在全网漏洞页签，支持查看所有收录的漏洞信息，包含已监测和未检测的漏洞。

- 若存在支持检测的安全产品，可以一键发起检测。

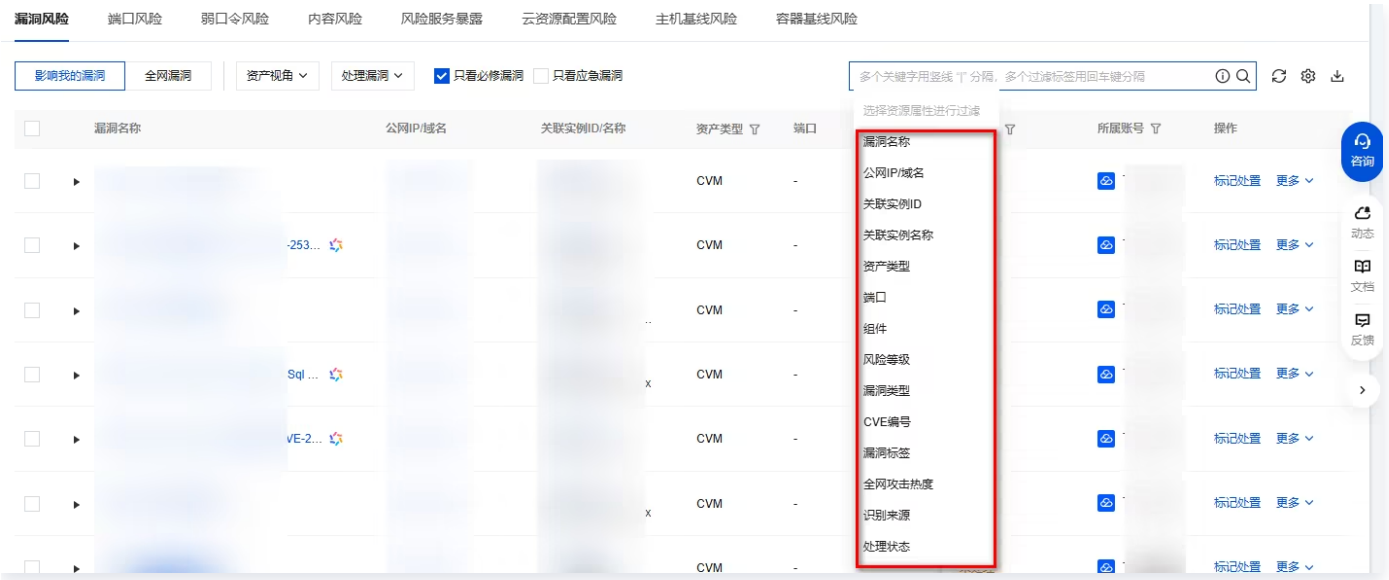


- 若无支持检测的安全产品，可以查看漏洞详情并自主排查与修复。

风险管理

筛选风险

在 漏洞与风险中心页面，单击**搜索框**，以关键字对风险进行筛选定位。



标记状态

标为已处置

建议使用主机安全和云防火墙，对安全风险进行封禁等防御措施。防御处置后的风险可以标为已处置，处理状态更改为已处置，若下次扫描任务中仍然检测到此风险，则处理状态重新变回未处理。

1. 在 漏洞与风险中心页面 ，支持单个或批量将风险状态标为已处置。
   - 单个：选择目标风险，单击操作列的**标记处置**。

   - 批量：选择一个或多个风险，单击左上角的**处理漏洞 > 标记处置**。

2. 在确认窗口中，单击**确定**，即可将目标风险标记为已处置。

标记为忽略

当扫描误报产生风险误报时或认为该风险无需处理时，可将该风险忽略，后续扫描任务中该风险将被过滤。

1. 在 漏洞与风险中心页面 ，支持单个或批量将风险状态修改为忽略。

- 单个：选择目标风险，单击操作列的**更多 > 标记忽略**。

- 批量：选择一个或多个风险，单击左上角的**处理漏洞 > 标记忽略**。

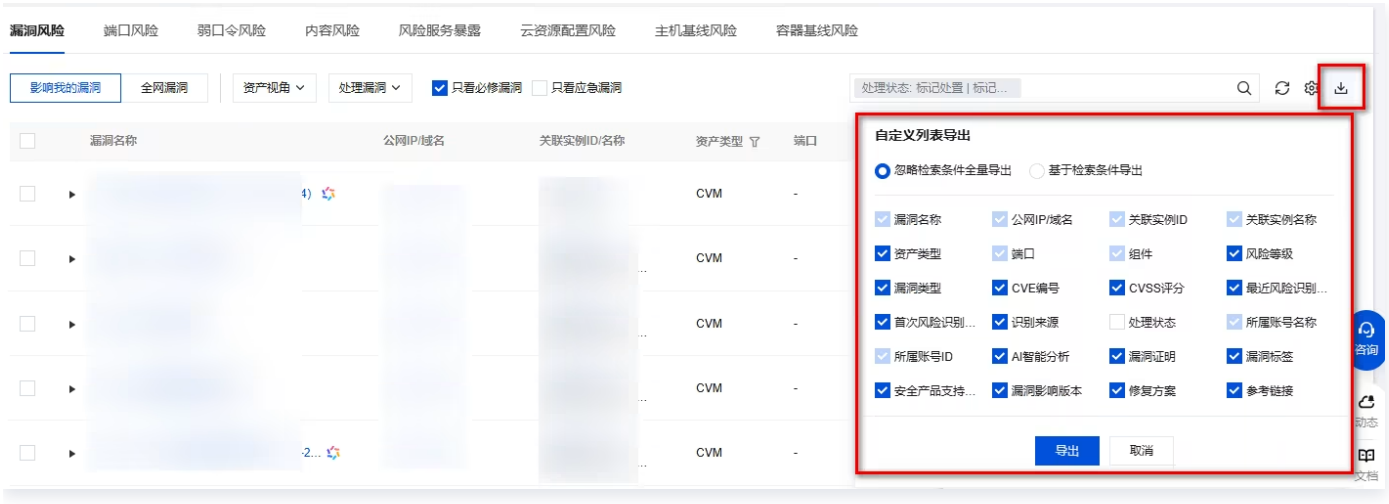
2. 在确认窗口中，单击**确定**，即可将目标风险状态修改为忽略。

取消标记

当告警需要重新研判时，取消标记后处理状态将恢复为未处理。
当已处置或已忽略风险时，在 漏洞与风险中心页面 ，选择目标风险，可单击操作列的**取消标记处置**或**取消标记忽略**，进行取消操作。

下载数据

在 漏洞与风险中心页面 ，单击右上角的 ，选择需要导出的行和列内容，然后单击**导出**将数据保存至本地。


漏洞风险
端口风险
弱口令风险
内容风险
风险服务暴露
云资源配置风险
主机基线风险
容器基线风险
影响我的漏洞
全网漏洞
资产视角
处理漏洞
只看必修漏洞
只看应急漏洞
处理状态: 标记处置 | 标记...
漏洞名称
公网IP/域名
关联实例ID/名称
资产类型
端口
CVM
自定义列表导出
忽略检索条件全量导出
基于检索条件导出
漏洞名称
公网IP/域名
关联实例ID
关联实例名称
资产类型
端口
组件
风险等级
漏洞类型
CVE编号
CVSS评分
最近风险识别...
首次风险识别...
识别来源
处理状态
所属账号名称
所属账号ID
AI智能分析
漏洞证明
漏洞标签
安全产品支持...
漏洞影响版本
修复方案
参考链接
导出
取消
咨询
动态
文档

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

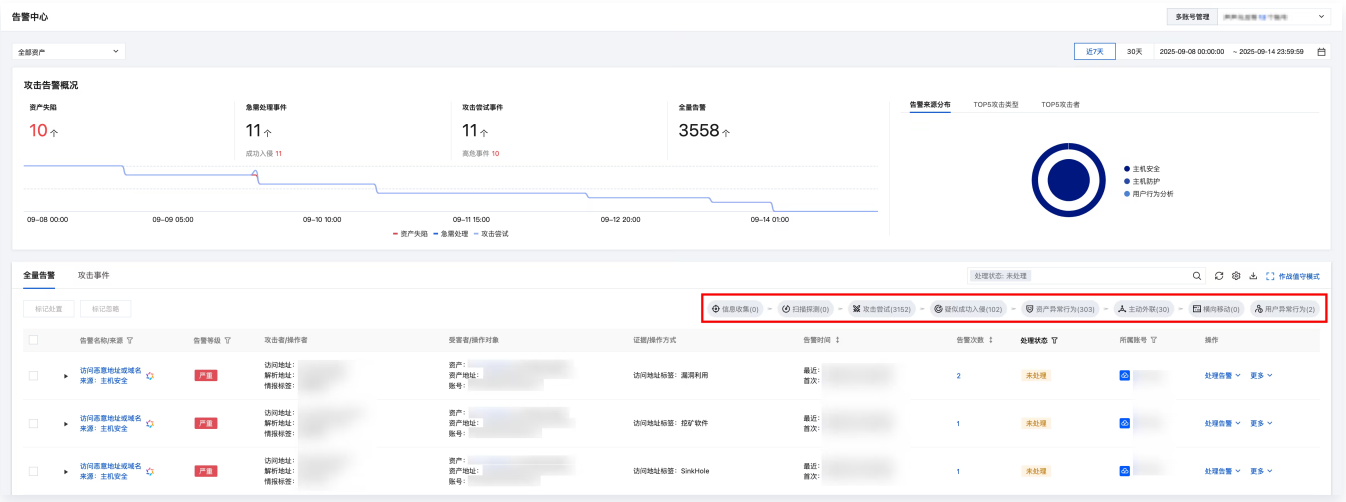
告警中心

最近更新时间：2025-11-28 16:17:12

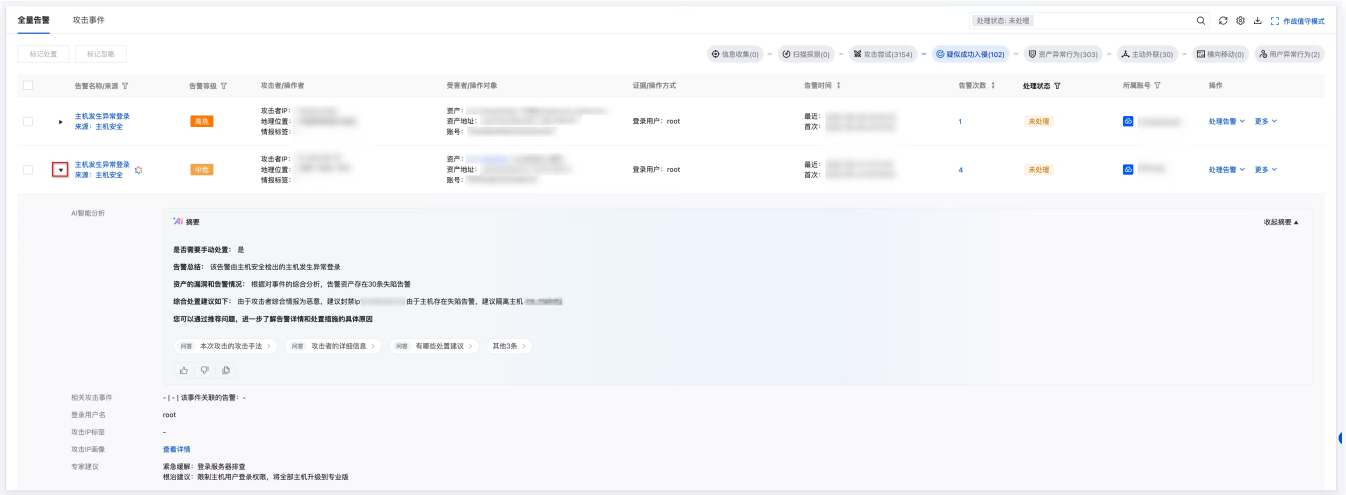
告警中心是一个集中监控和分析云上安全威胁的一体化功能，通过汇聚云安全中心、主机安全、容器安全、云防火墙和 Web 应用防火墙等来源的告警，基于 ATT&CK 框架进行告警关联分析，实现统一的安全威胁发现与管理，帮助用户快速发现和处置安全隐患。

告警定位

1. 登录 **云安全中心控制台**，在左侧导览中，单击**告警中心**。
2. 在全量告警页签，选择对应的**攻击阶段**以定位告警。



3. 单击目标告警名称的 ▶，展开并查看告警详情，根据列表中提供的**攻击者、受害者和证据**定位攻击源头与受影响资产，并可参考 **AI 智能分析**提供的相关建议进行排查处置。



告警管理

1. 登录 **云安全中心控制台**，在左侧导览中，单击**告警中心**。
2. 在全量告警页签，单击**筛选框**，支持以关键字对告警进行筛选定位。

3. 单击目标告警名称操作列的**处理告警**，可对告警进行如下操作：

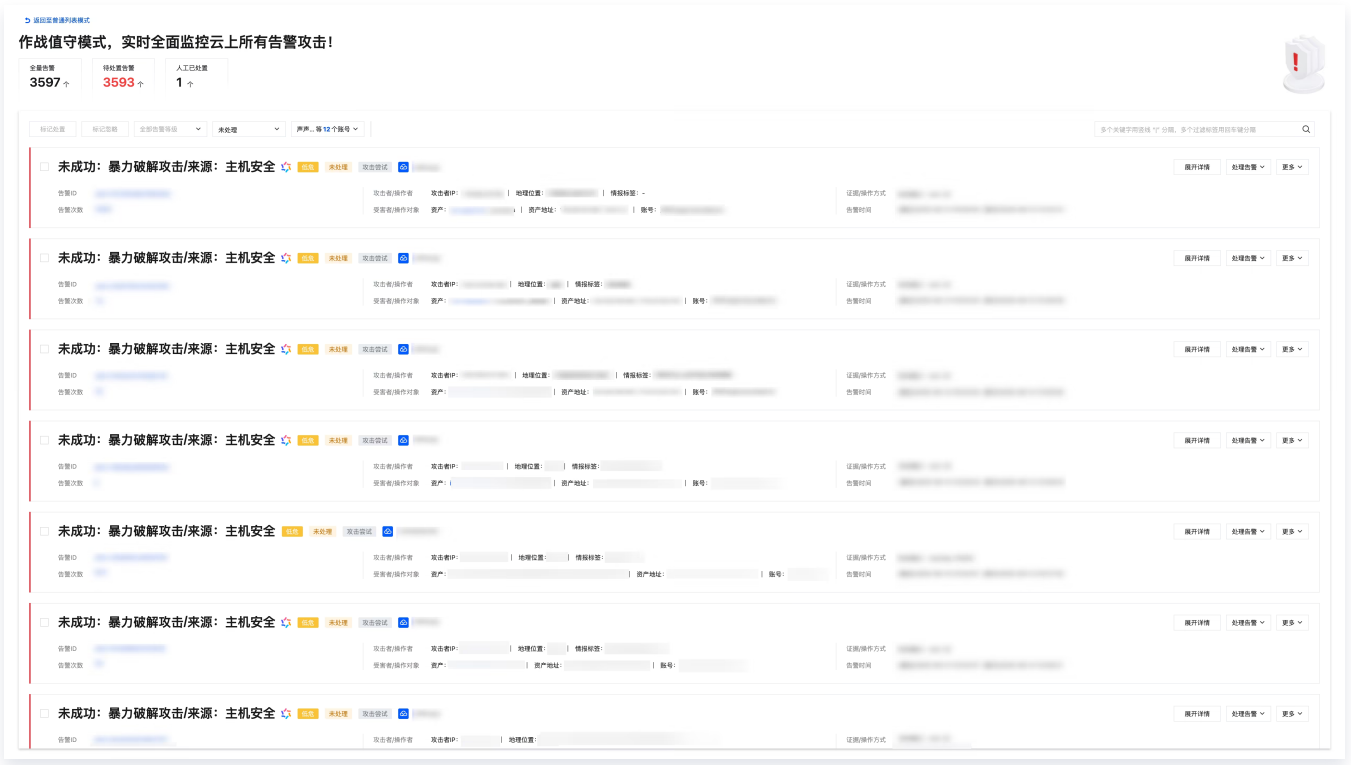
处理类型	处理建议	操作说明
标为已处置	建议使用主机安全和云防火墙，对安全告警进行封禁回连地址、隔离资产等防御措施。防御处置后的告警可以标为已处置。	1. 支持单个或批量将告警状态标为已处置。 ○ 单个：选择目标告警，单击操作列中的**标记已处置**。 ○ 批量：选择一个或多个告警，单击左上角的**标记已处置**。 2. 在确认窗口中，单击**确定**，即可将目标告警标记为已处置。
标记忽略	当产生告警误报时或认为该告警无需处理时，可将该告警忽略，后续相同告警将被过滤。	1. 支持单个或批量将告警状态修改为忽略。 ○ 单个：选择目标告警，单击操作列的忽略。 ○ 批量：选择一个或多个告警，单击左上角的忽略。 2. 在确认窗口中，单击**确定**，即可将目标告警状态修改为忽略。
取消标记	当告警需要重新研判时，取消标记后处理状态将恢复为未处理。	当已处置或已忽略告警时，选择目标告警，可单击操作列中的**取消标记处置**或**取消标记忽略**，进行取消操作。

4. 在全量告警页签，单击右上角的 ，选择需要导出的行和列内容，然后单击**导出**将数据保存至本地。

作战值守模式

1. 登录 **云安全中心控制台**，在左侧导览中，单击**告警中心**。
2. 在全量告警页签，单击右上角的**作战值守模式**，启动作战值守模式。

3. 此时安全大屏将实时滚动更新增量告警信息，帮助您快速获取新增待处置威胁。



云边界分析
功能简介

最近更新时间：2026-01-13 16:09:42

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）

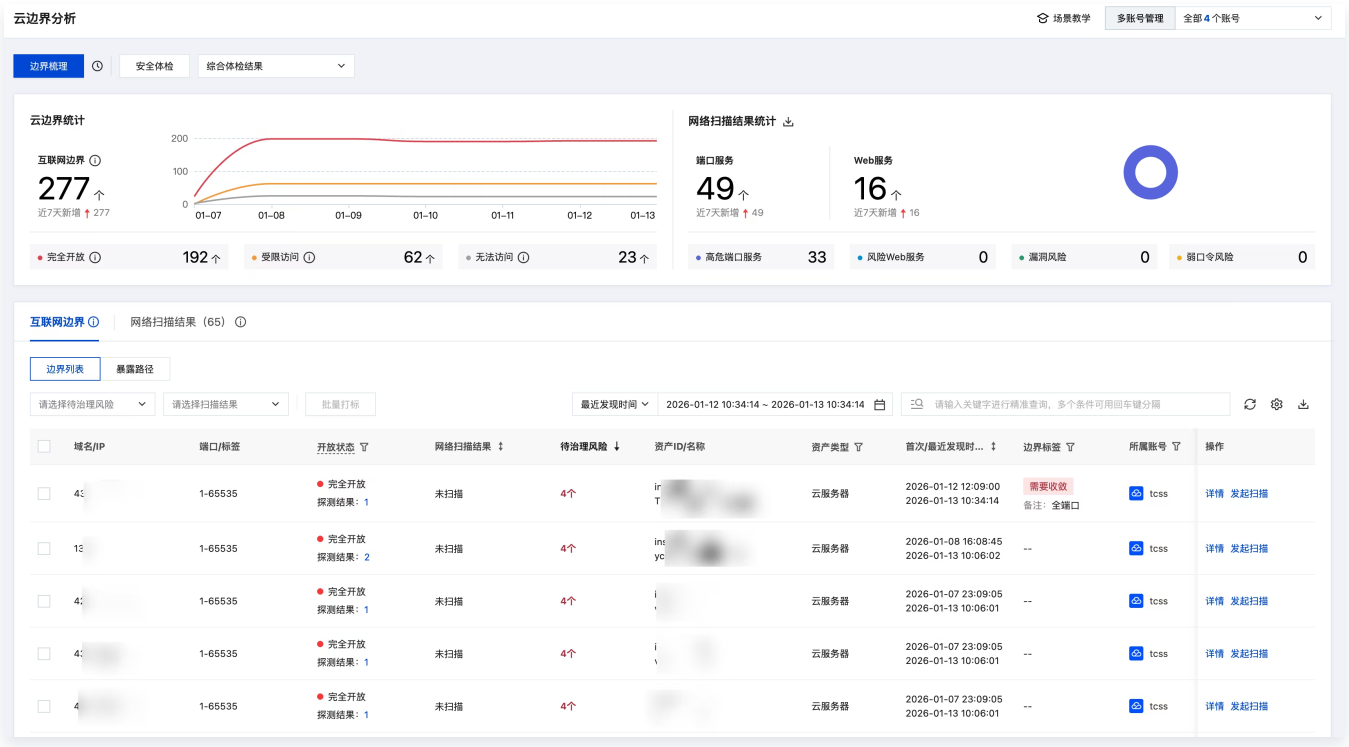
- 负载均衡的安全组开放了允许0.0.0.0/0访问80端口，两台云服务器均处于关机状态。

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**的形式展示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
	容器与中间件	容器服务
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
亚马逊云	计算	云主机EC2
	网络	负载均衡 ELB
		弹性公网IP
		弹性网卡 ENI
	数据库	云数据库 RDS
		云数据库 DocumentDB
		MemoryDB 内存数据库服务
		ElastiCache 内存缓存
	Serverless	Lambda
	CDN	CloudFront

查看统计面板

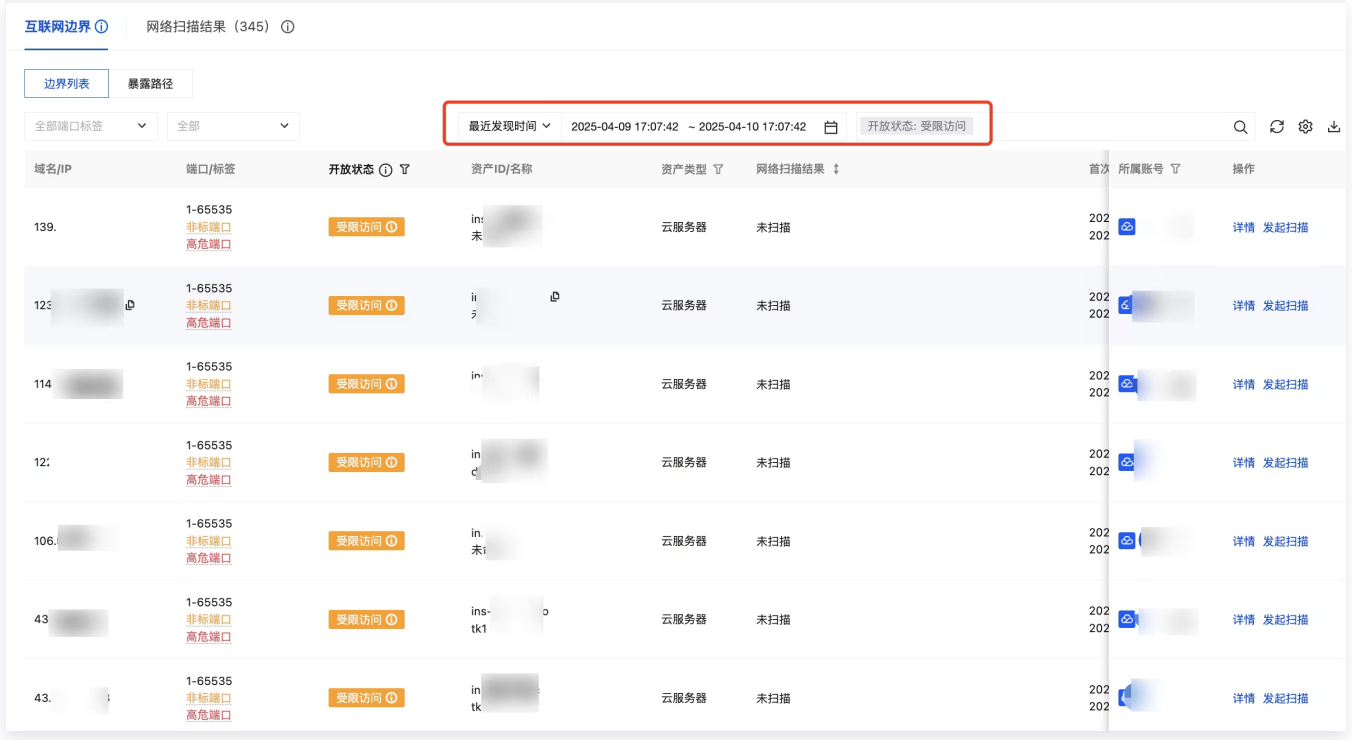
最近更新时间：2025-11-28 16:17:12

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，仅白名单里的地址可访问该端口。
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。



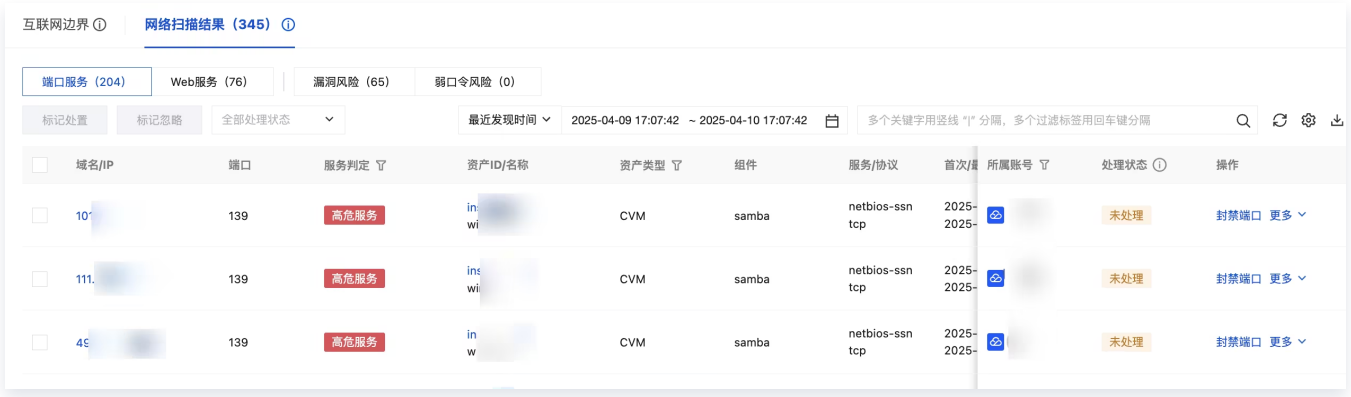
4. **云边界数量趋势图**：展示了近7天边界数量的整体趋势。

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。

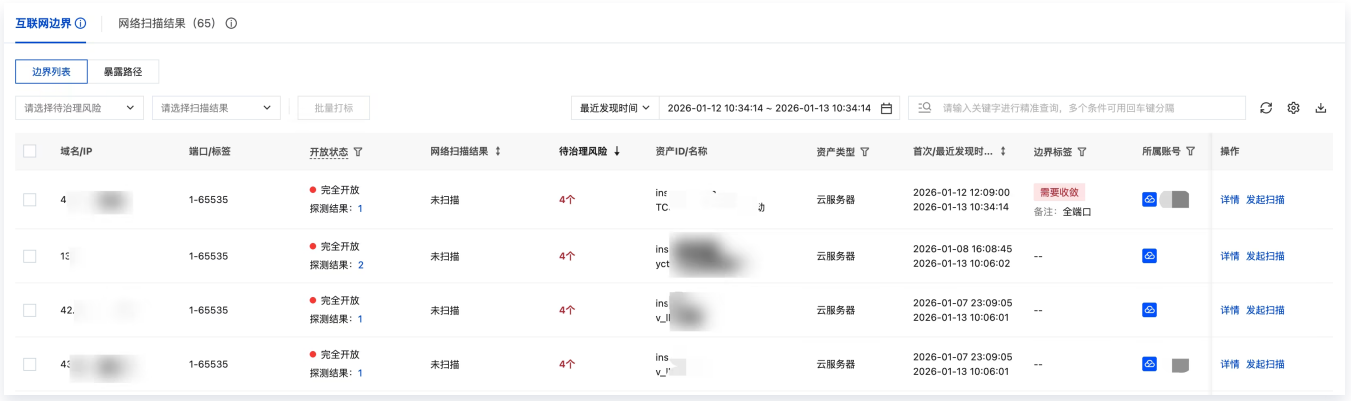
5. 通过调整体检任务，可以查看不同体检任务的结果。综合体检结果即根据所有体检任务的结果进行汇总。体检任务的切换只影响扫描结果，不影响互联网边界的结果。

查看边界列表

最近更新时间：2026-01-13 16:09:42

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就会被定义为一个边界。
开放状态	• 完全开放 探测结果：1 • 受限访问 探测结果：1 • 无法访问 探测结果：0	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。 云安全中心将通过公网服务器对您的端口进行最简单的连通性探测，来获取端口是否可访问。
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。
待治理风险	4个	云安全中心会对您的网络边界进行评估，梳理存在的配置风险。

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. 选择目标数据，将鼠标移至**待治理风险**时，可以查看该数据的待治理风险信息。

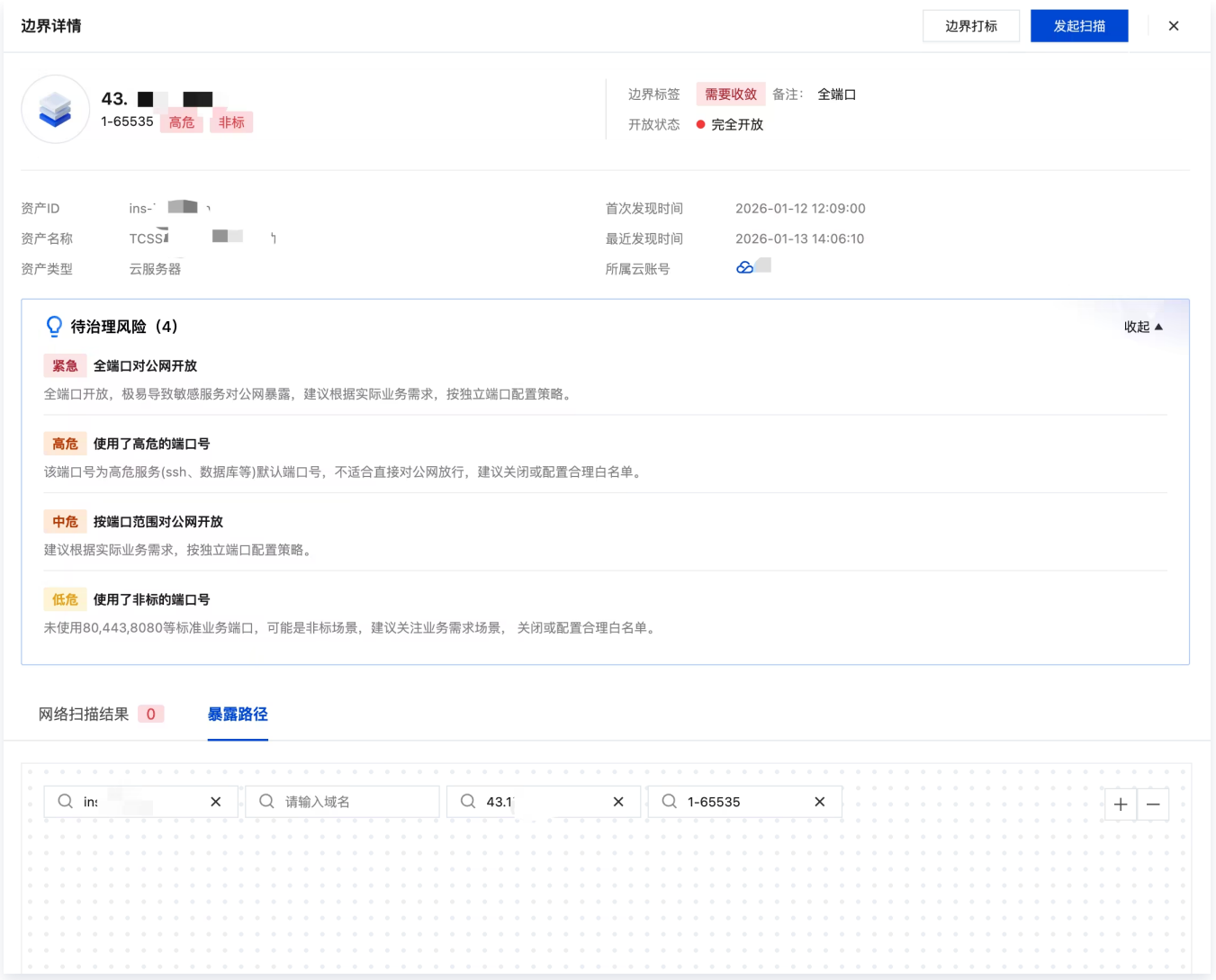
4. 选择目标数据，在**边界标签**处，单击**编辑**，即可对该数据进行打标，系统将边界数据分为合理业务、需要收敛、临时开放三种类型，方便您持续治理云边界。

5. 单击后侧的**导出**，可以将数据进行导出，格式是 Excel。

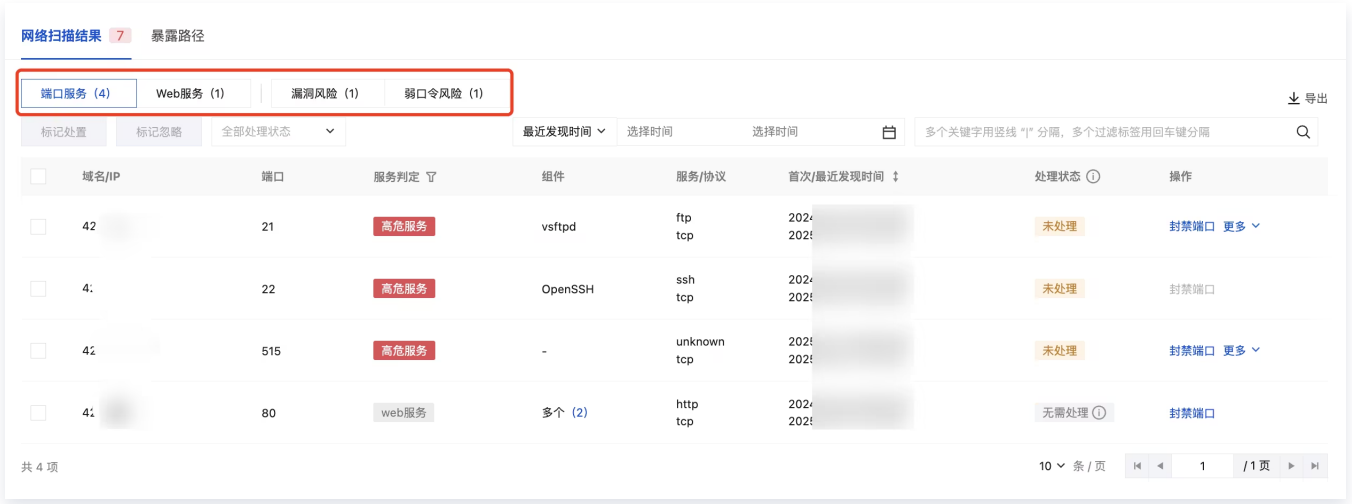
边界详情

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**。

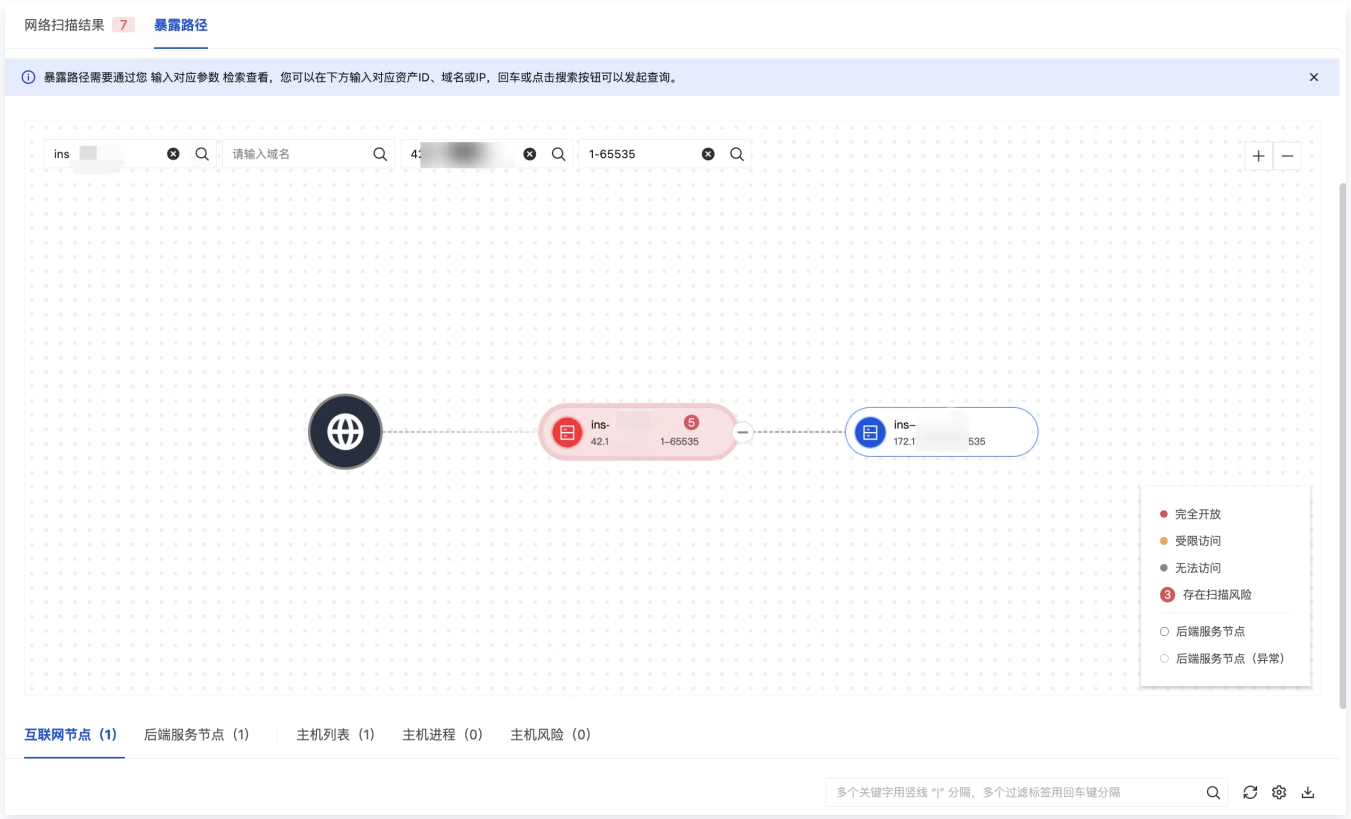
3. 在边界详情页面上方提供了互联网边界的详情信息、待治理风险。



4. 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**。



5. 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：2025-12-11 14:40:12

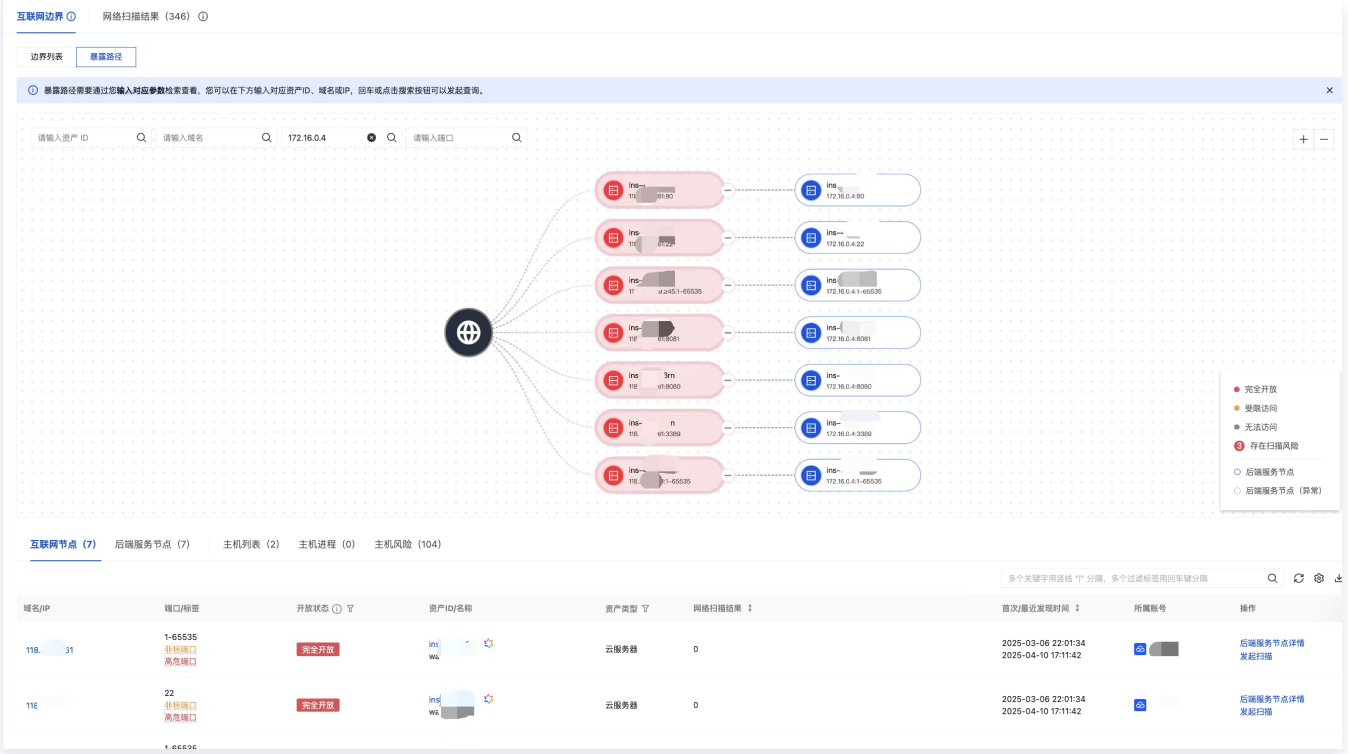
功能介绍

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，将鼠标悬停于节点上，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。

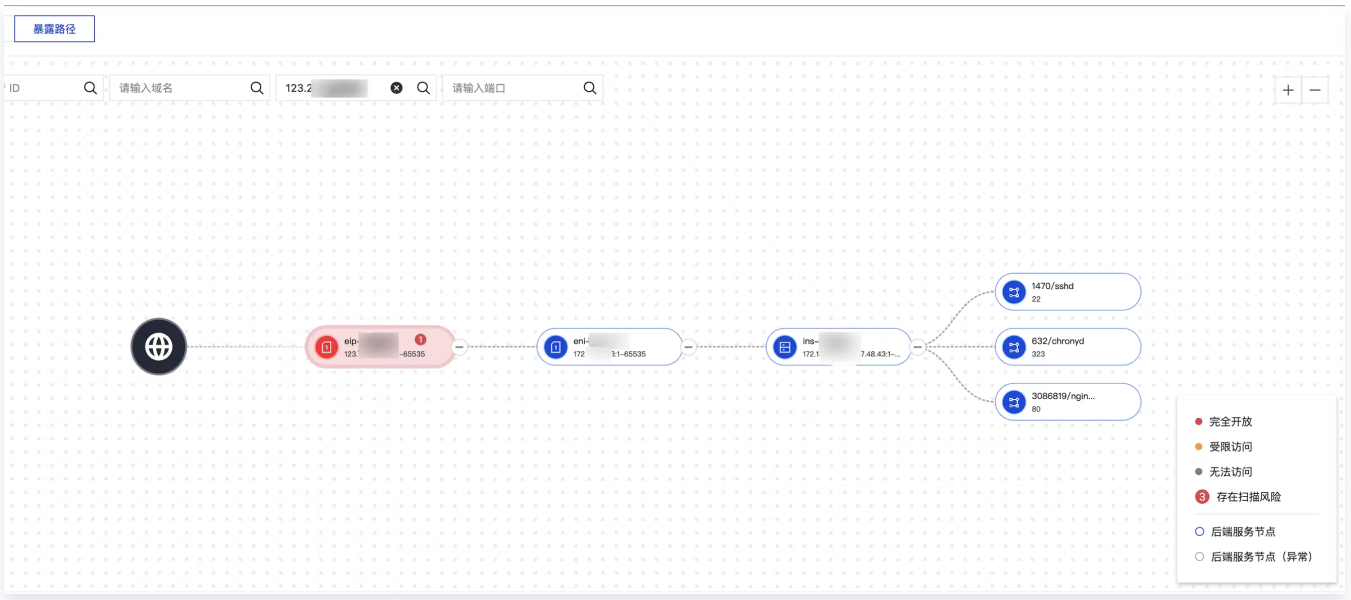
- **主机进程列表：展示通过主机安全采集到的主机进程信息，以便您了解主机上的应用信息、端口监听情况。**

- **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

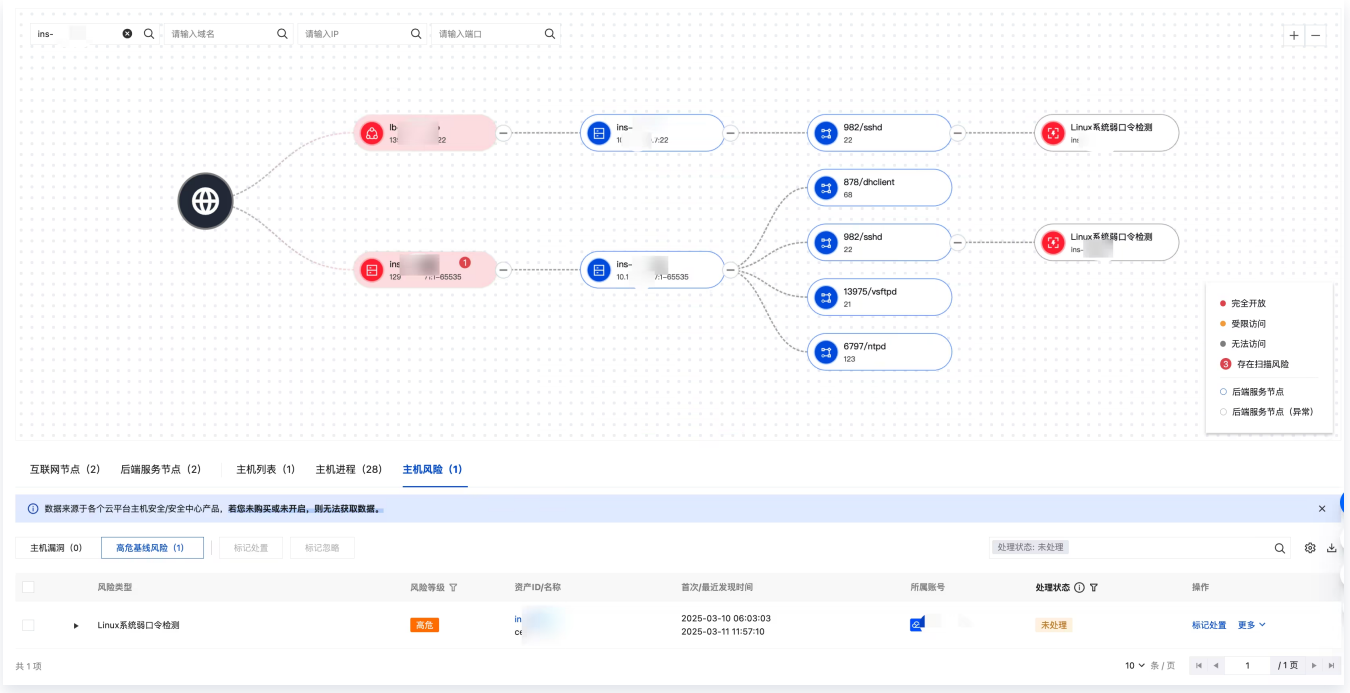
下图的路径关系如下：

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。

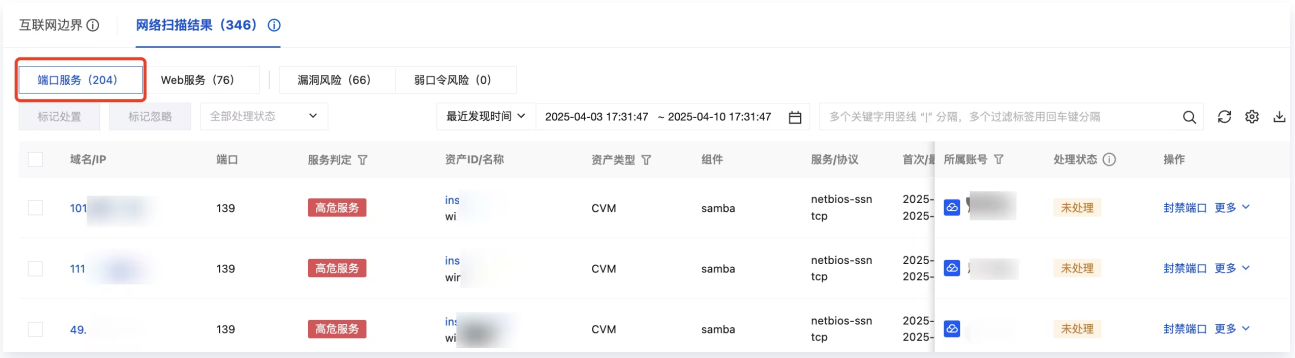


2. 分析可知，资产通过安全组开放了所有端口，并且配置了公网 IP(129.***.***.***)。同时通过负载均衡（139.***.***.***）开放了22端口。资产存在 Linux 系统弱口令，该弱口令可能是入侵的主要原因。可以根据该方向进行排查。

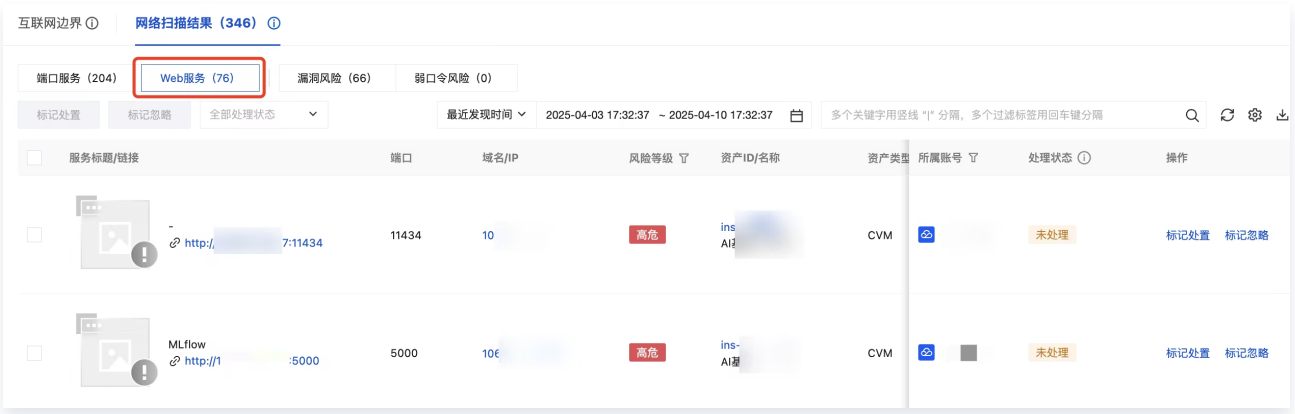
查看扫描结果

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。

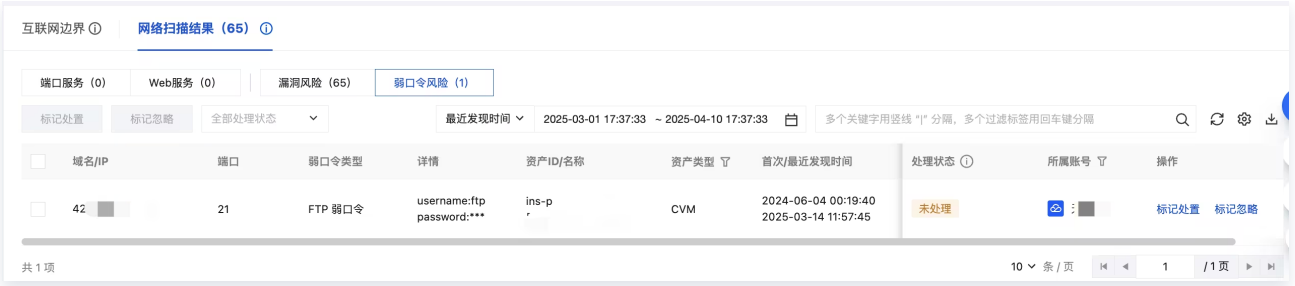


   - **Web 服务**：查看扫描发现的 Web 服务，包括预览页、标题、状态响应码、组件等。云安全中心会将高危 Web 服务进行标注。



   - **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。


互联网边界
网络扫描结果（65）
端口服务（0）
Web服务（0）
漏洞风险（65）
弱口令风险（1）
标记处置
标记忽略
全部处理状态
最近发现时间
2025-03-01 17:37:33 ~ 2025-04-10 17:37:33
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
域名/IP
端口
弱口令类型
详情
资产ID/名称
资产类型
首次/最近发现时间
处理状态
所属账号
操作
21
FTP 弱口令
username:ftp
password:***
CVM
2024-06-04 00:19:40
2025-03-14 11:57:45
未处理
标记处置
标记忽略
共 1 项
10 条 / 页
1
/ 1 页

云 API 异常监测
云 API 密钥安全使用方案

最近更新时间：2025-11-13 14:52:01

云 API 密钥是构建腾讯云 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。
云 API 密钥包含 SecretId(AK) 和 SecretKey(SK)，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/SK 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/SK 面临风险和安全治理必要性

1. 凭证泛滥，AK资产管理难

随着业务扩张各企业 AK 数量激增，90%企业存在 AK 超量超权限发放问题。尤其在多云多账号场景下 AK 分布较为分散，使得管理更加困难，各企业经常会出现“僵尸AK”或未清理的冗余 AK。

2. 权限滥用，横向移动防不住

主账号 AK 滥用、子账号过度授权，攻击可利用单一凭证完成：创建子账号 > 提权 > 接管云资源（如数据库、存储桶）> 执行恶意命令等，甚至登录云平台控制台扩大攻击面，造成大规模数据泄露或服务中断。
编程访问和 API 账号未分开申请和使用，也是权限不可控的一个重要原因。

3. 云 API 调用缺少监控，恶意调用未感知

缺少动态监控机制及 API 调用行为追踪机制，无法发现 AK/SK 代码泄露及异常操作（如列举资源、查看数据、敏感 API 调用）。凭证泄露后企业难以及时感知、快速定位，导致攻击者可以持续利用泄露凭证进行隐蔽操作。

典型案例

示例场景	攻击路径	总结反思
某科技公司被攻击者利用 AK 登录服务器删除备份进行勒索	攻击者通过拿到泄露的 AK 注册第三方某云管家，通过云服务器 CVM 自动化助手 TAT，对机器下发命令重置密码后，SSH 登录植入勒索病毒，删除所有镜像和备份并发送勒索信。	1. 云上发现多个客户注册某云管家，普遍是攻击者在使用来进行资源查看和 AK/SK 验证，建议关注云 API 异常监测中的外部多云厂商的调用。 2. 结合主机安全勒索病毒检测能力，对病毒进行隔离处置。 3. 尽量使用堡垒机等进行 SSH 的最小化管理，对异常登录进行告警。

		4. 做好数据和应用的多地灾备，**注意 AK 的权限收敛治理**。
某公司被攻击者利用 AK 调用云服务获取源代码	攻击者通过外部 Web 漏洞入侵并找到明文密钥，通过境外 IP 请求 API 重置服务器的密钥，植入后门并进行内网扫描，**访问客户 COS 获取源代码**。	1. 关注云 API 异常监测中的 COS 相关告警，对 COS 权限进行收敛。 2. 借助云安全中心云边界分析进行暴露面收敛、主机安全进行漏洞防御。 3. 关注云 API 异常监测中的可疑 IP 调用高危接口、CVM 高危操作的告警。
某公司被攻击者利用泄露 AK 购买服务器挖矿	攻击者通过泄露的主账号 AK 新增用户，登录控制台并购买服务器挖矿，造成客户财产损失。	1. 主 AK 直接使用并且给了多个业务，溯源发现是硬编码在客户端被逆向导致泄露（硬编码在客户端时，请求源为客户的 IP，数量较大）。 2. 关注云 API 异常监测中的根密钥调用高危接口告警。 3. 关注子用户新增告警，关注 AK 的调用源 IP 过多的情况。 4. 关注主机安全/ DNS 威胁监测挖矿告警。

常见 AK 泄露方式

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。

2. 客户端反编译导致的凭证提取

小程序/APP 开发者将SecretId/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流量并利用其发起恶意请求。

5. 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SecretId/SecretKey。

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，一个用户仅是某个 COS 桶的使用者时，不应授予其其他服务的访问权限（如 CAM 读写权限），也不应分配全部 COS 权限，只需授予该用户对特定存储桶的必要访问权限即可。
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。

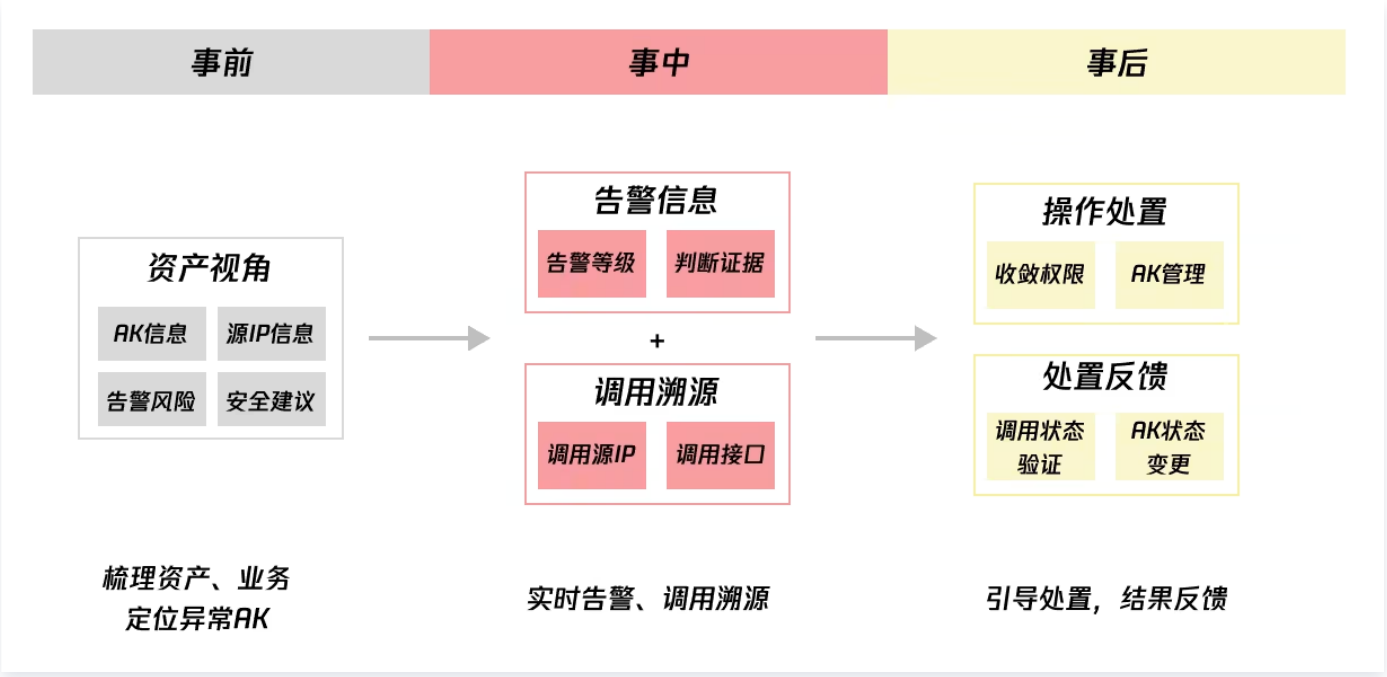
- AK 列表：梳理 AK 资产，了解我有多少把 AK，备注每把 AK 是什么业务在用。
- 调用源 IP：梳理调用源 IP，了解每个调用源 IP 属于哪个业务。
- 风险权限收敛：查看 AK 配置检查结果，梳理是否有不需要的高权限接口。
- 应急响应：当提前掌握好上面的情况后，出现 AK 泄露导致异常调用时，可以快速的完成 AK 替换。

功能简介

最近更新时间：2025-11-28 16:17:12

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。

- **事前：**建立完整的 AK、账号资产列表，多视角（AK 视角、账号视角、调用源 IP 视角）梳理 AK 资产列表和业务关系、调用源 IP 和接口，引导进行 AK 权限治理。
- **事中：**基于 AK + IP + 接口的基线外请求进行告警，高危接口调用告警，异常 IP 调用告警，黑客工具特征告警。
- **事后：**及时对异常 AK 进行高危权限回收，访问源 IP 控制，追踪 AK 泄露源，及时替换业务 AK。



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

功能版块	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，定位出建议关注的异常 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。	
账号列表		基于账号视角，展示账号基本信息、安全建议、关联告警与风险、最近登录时间以及账号保护状态。	清晰汇总每个账号现存的安全问题数量、告警与风险条目，并提供安全建议，支持一键开启账号保护。	账号列表
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
配置风险列表		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。	配置风险
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。		
	IP 隐藏策略	通过为指定 AK 配置调用源 IP 加白策略，该 AK 后续所有访问 IP 将自动隐藏，不在调用源 IP 列表中展示。		

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。

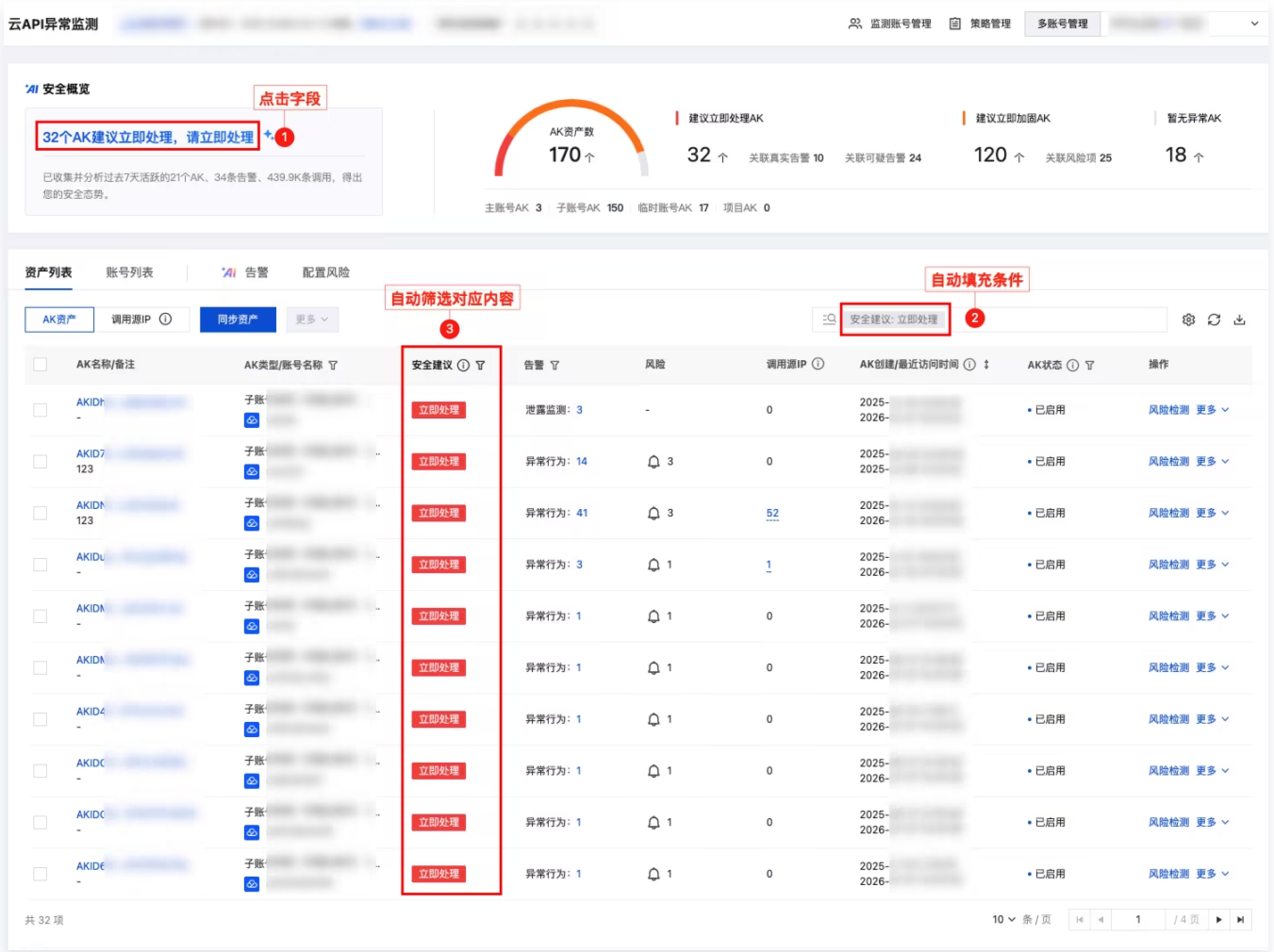
统计面板

最近更新时间：2026-02-06 15:55:11

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（包含项目密钥与临时密钥）并按不同安全建议分类统计 AK 数量。同时，关联并呈现这些AK 所对应的真实/可疑告警及风险项。

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天内有调用行为的 AK 数量、相关告警数及 AK 调用次数，得出您的安全态势。
4. 单击“关注的字段”，下方列表的搜索框中自动添加条件并筛选出对应内容。



资产列表

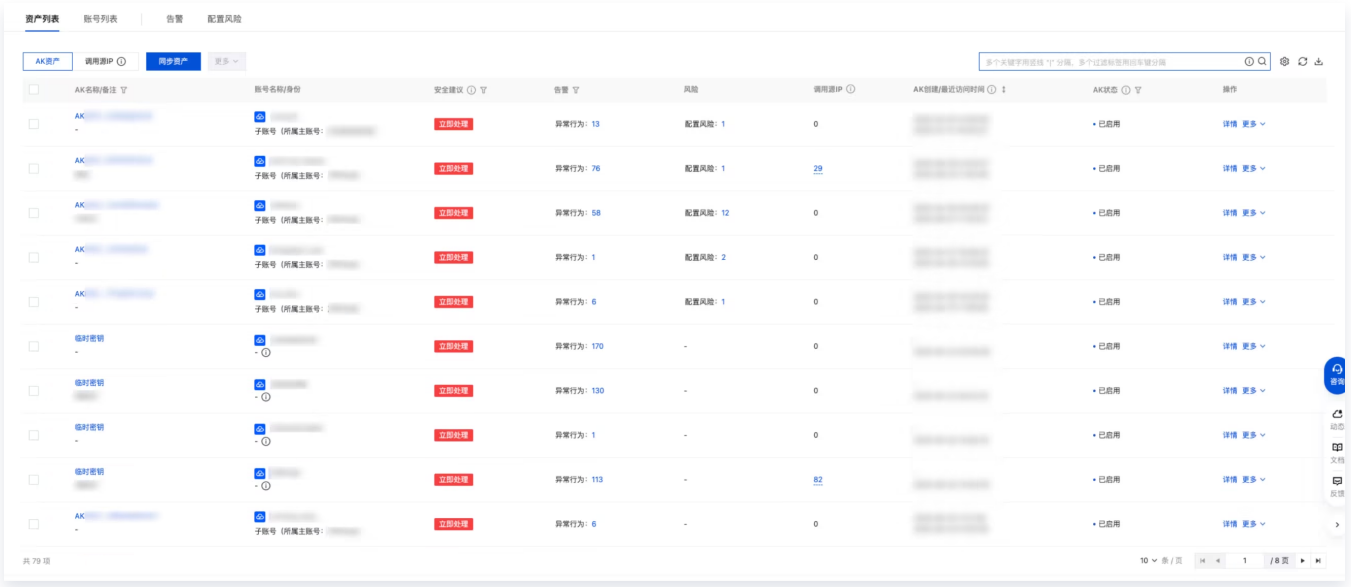
最近更新时间：2025-11-28 16:17:12

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“-”。 • 支持筛选主账号密钥/子账号密钥/临时密钥。
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。 • 鼠标悬浮查看账号名称、账号 ID与 APPID。

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	• 异常行为：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	• 配置风险：x	近期未处理风险，单击拉起 **AK 详情**抽屉，定位到**配置风险**页签。
调用源 IP	1	• 近七天调用该 AK 的 IP 数量。 • 鼠标悬浮查看源 IP、地域、IP 类型以及备注。
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 • 已删除	展示 AK 禁用/启用/删除状态。 支持筛选已禁用/已启用/已删除。

3. 在 AK 资产中，选择所需 AK，单击**详情/更多**。

操作类型		说明
详情		单击拉起AK详情抽屉。
更多	风险检测	单击后重新检测该AK。
	API密钥管理	单击跳转至**访问管理** > **API 密钥管理**。
	修改 AK 备注	修改 AK 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。

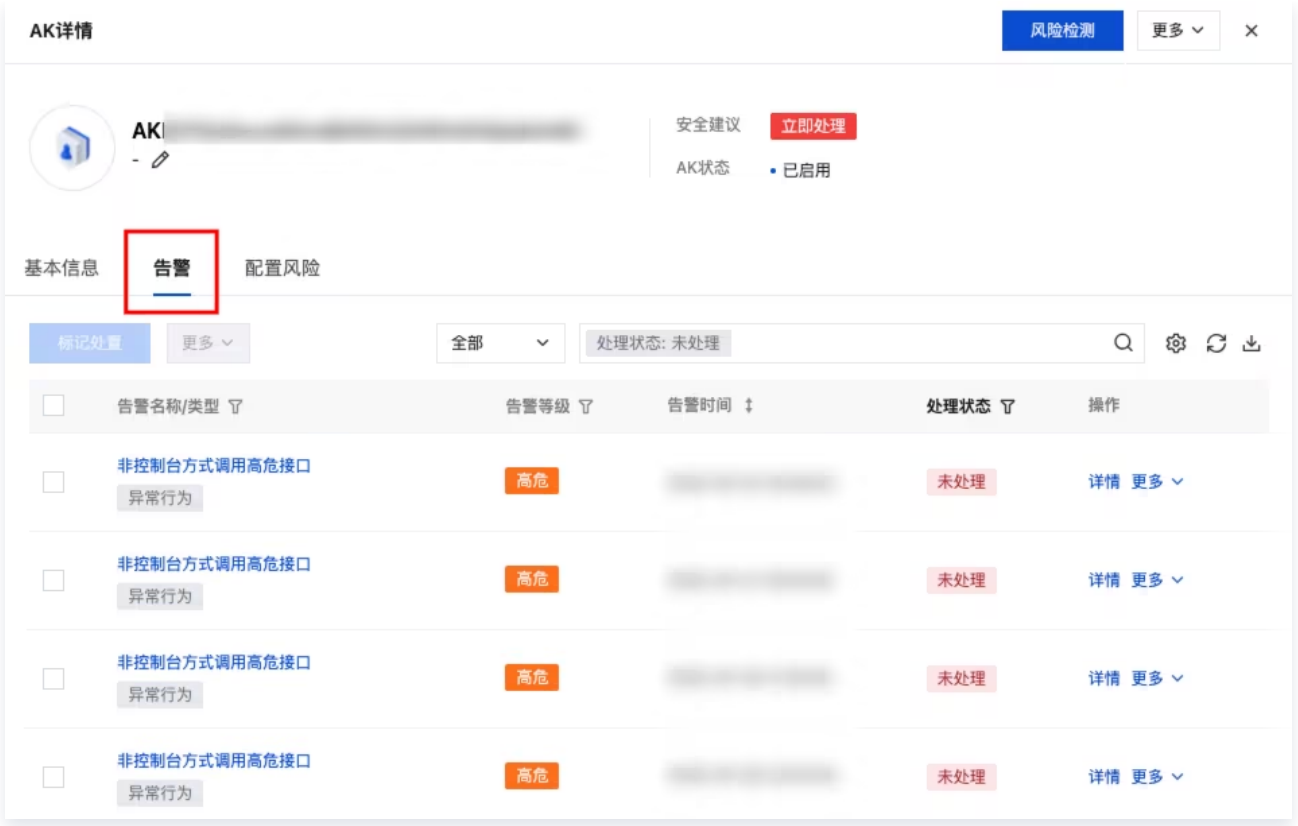
	添加告警策略	单击拉起**添加告警策略**抽屉，并填充对应 IP。
	前往查看日志	单击跳转至**日志分析 > 增值服务日志检索**。

AK 详情

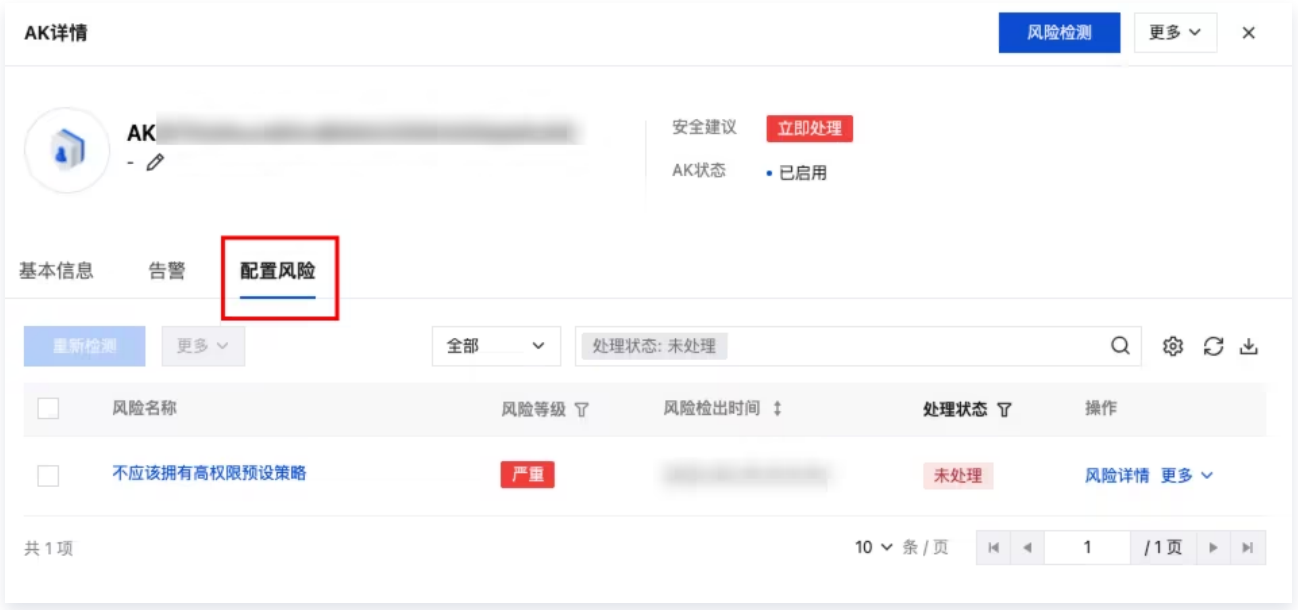
1. 登录 云安全中心控制台，在左侧导览中，单击**云 API 异常监测**。
2. 在**资产列表 > AK 资产**中，选择所需资产，单击**详情**。

3. 在 AK 详情页面，查看 AK 基本信息、关联告警与配置风险、调用记录与关联资产。
   - 查看 AK 基本信息，AK 基本信息包括：账号名称、账号身份、账号 ID/APPID、所属主账号、CAM 策略、AK 创建时间以及最近访问时间。

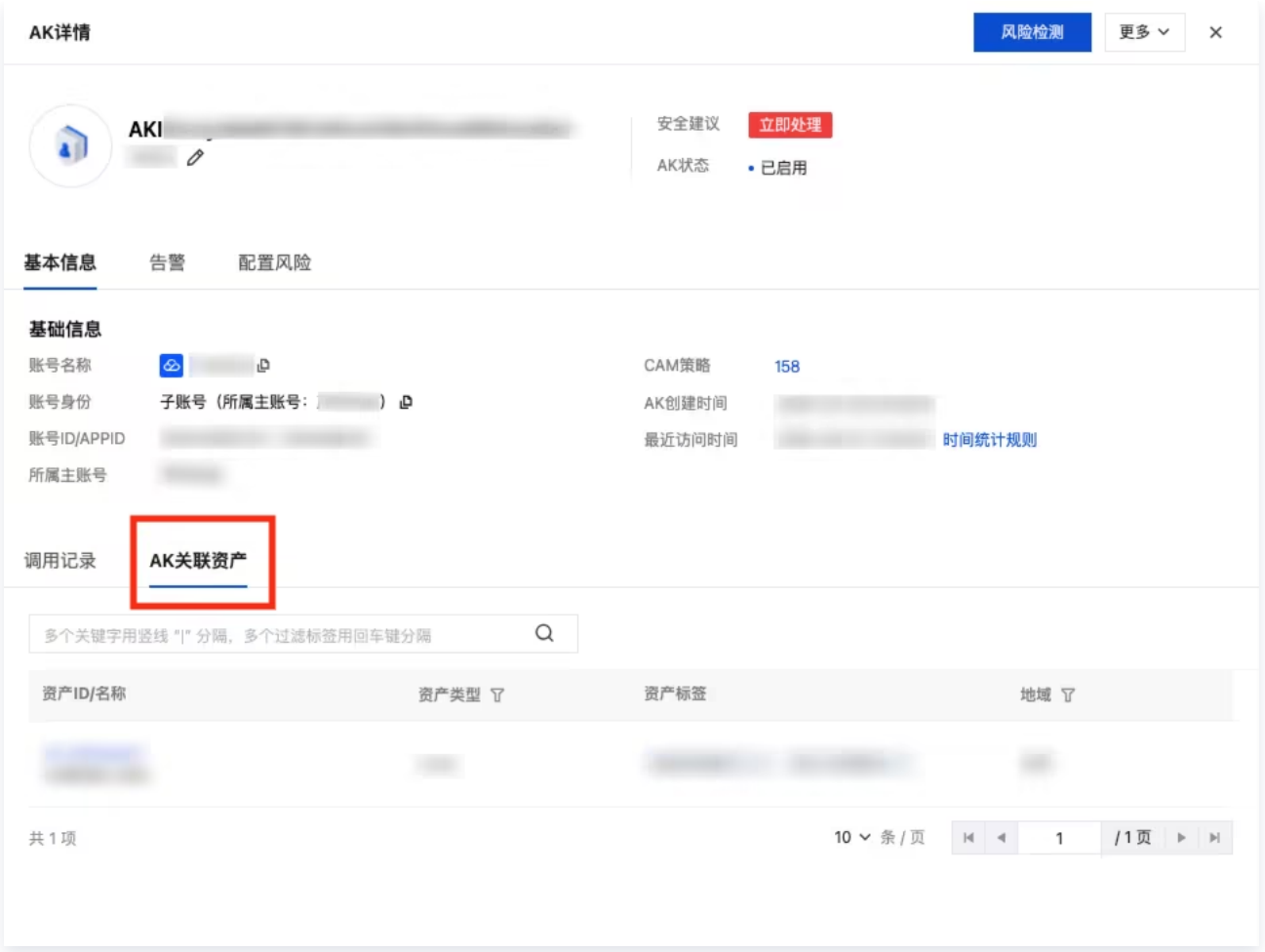
   - 查看 AK 告警信息，默认展示未处理告警，单击**详情**可打开**告警详情抽屉**，相关字段说明可参考 告警 。



- 查看 AK 配置风险信息，默认展示未处理风险，单击**详情**可打开**风险详情抽屉**，相关字段说明可参考配置风险。



- 查看 AK 关联资产，包括资产 ID/名称、资产类型、资产标签以及地域。



字段名	示例	说明
资产 ID/名称	ins-xxx xxx	该资产在云平台中的唯一标识符及其自定义名称。 单击资产 ID 可以跳转到**资产中心** > **主机资产**详情。
资产类型	CVM	该资产所属的云服务产品类型。 支持筛选 CVM/Lighthouse。
资产标签	-	同步资产中心标签信息。
地域	北京	该资产所在的数据中心的地理区域。 支持筛选北京/广州/中国香港/上海/上海金融/新加坡。

- 查看调用记录，包括调用该 AK 的 IP 地址、IP 类型、调用方式、服务名称、成功与失败的调用次数、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.x.x.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	• 账号内（已备注）	• 账号内（已备注）：在云安全中心资产列表中识别到的调用源 IP，有备注。

	• 账号内（未备注） • 账号外（已备注） • 账号外（未备注） • 局域网（已备注） • 局域网（未备注）	• 账号内（未备注）：在云安全中心资产列表中识别到的调用源 IP，无备注。 • 账号外（已备注）：非账号内 IP 但有备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 局域网（已备注）：局域网 IP 地址，有备注。 • 局域网（未备注）：局域网 IP 地址，无备注。
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 用户（角色）/策略	1 用户：xxx 策略：1	该 AK 关联的 CAM 策略个数，单击**数字**打开 CAM 策略详情弹窗。 临时密钥由于聚合展示,所以展示用户（角色）。
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**访问管理 > 策略 > 具体策略详情**。

- 更多
  - 添加白名单策略：单击拉起**添加白名单策略**抽屉，填充生效策略、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**。

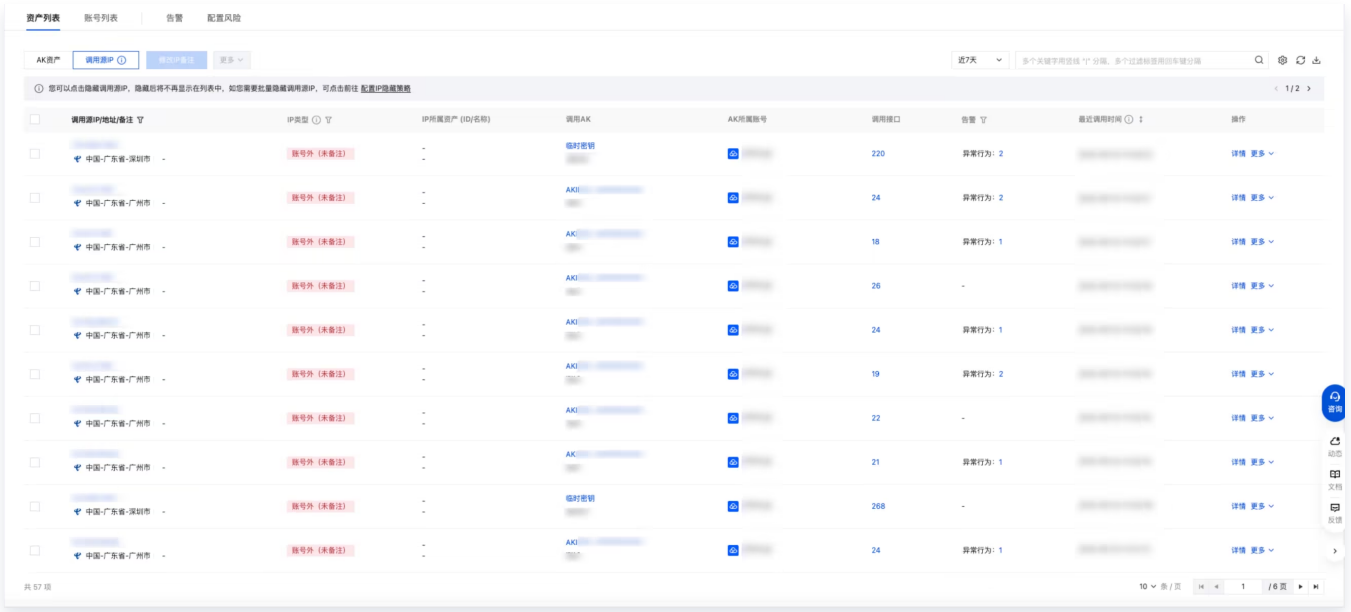
调用源 IP

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：

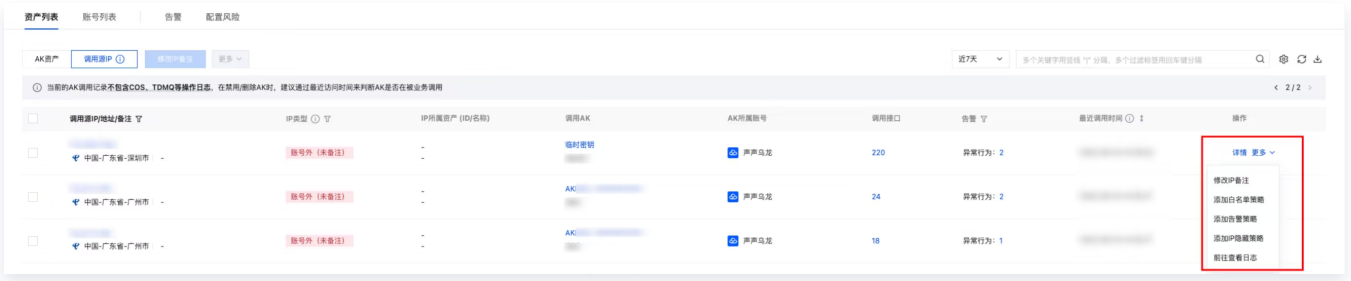
- 列表数据聚合逻辑：一天内同一 IP 调用同一账号下的 AK。
- 仅展示永久密钥的 API 请求。



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	• 账号内（已备注） • 账号内（未备注） • 账号外（已备注） • 账号外（未备注） • 局域网（已备注） • 局域网（未备注）	• 账号内（已备注）：在云安全中心资产列表中识别到的调用源 IP，有备注。 • 账号内（未备注）：在云安全中心资产列表中识别到的调用源 IP，无备注。 • 账号外（已备注）：非账号内 IP 但有备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 局域网（已备注）：局域网IP地址，有备注。 • 局域网（未备注）：局域网IP地址，无备注。
IP 所属资产（ID/名称）	ins-xxx 机器1号	展示 AK 所属资产。

调用 AK	1	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	1	单击**数字**打开数字**调用源 IP 详情**抽屉。
告警	• 异常行为：x • 泄露监测：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。 • 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。
	添加告警策略	单击拉起**添加告警策略**抽屉，并填充对应 IP。
	添加 IP 隐藏策略	单击拉起**添加IP隐藏策略**抽屉，并填充对应 IP。
	前往查看日志	单击跳转至**日志分析 > 增值服务日志检索**。

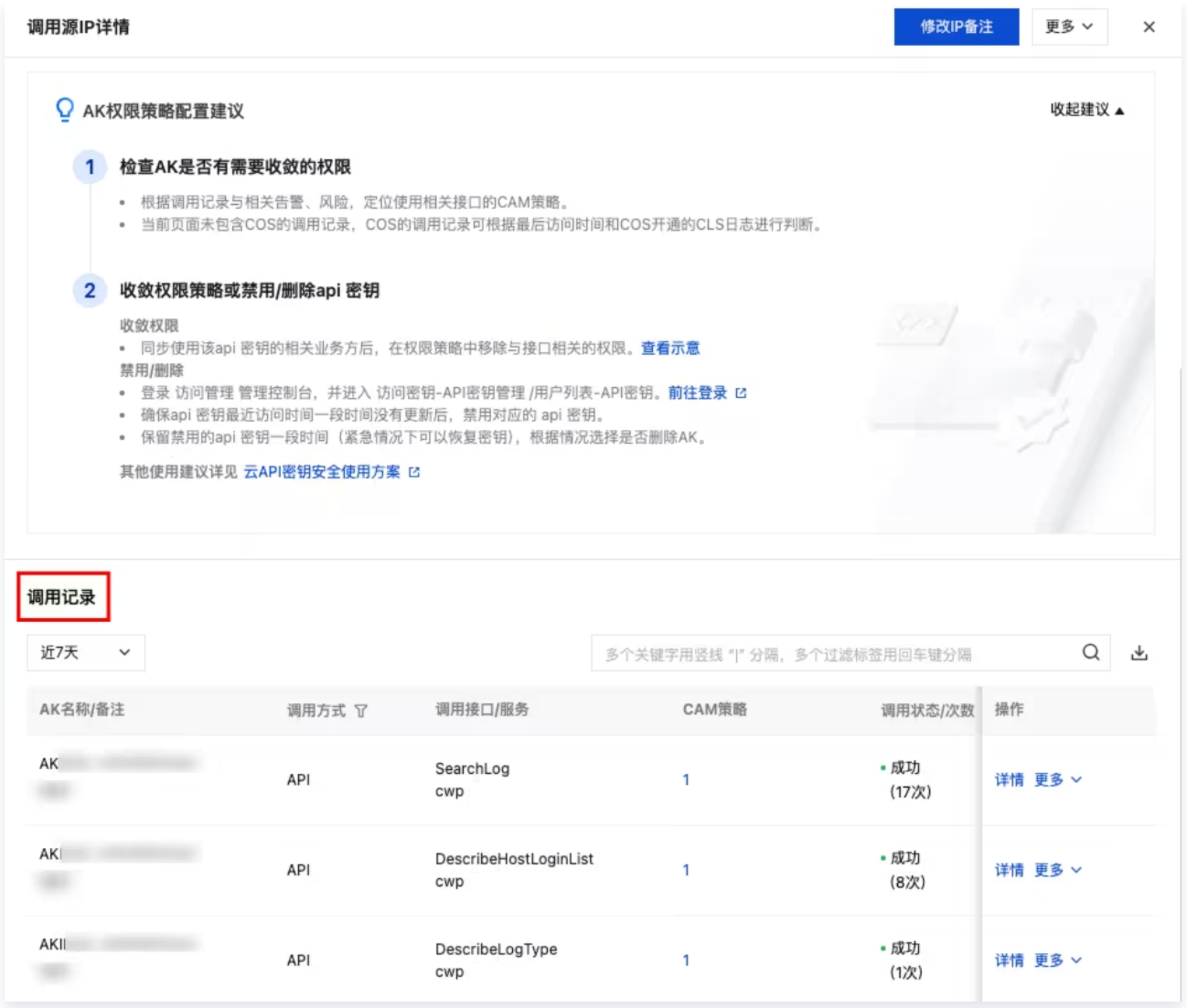
调用源 IP 详情

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 基本信息、关联告警、调用记录与关联资产。
   - 查看 IP 基本信息，IP 基本信息包括：AK 所属账号、账号 ID/APPID、IP 所属资产 ID、IP 所属资产名称以及最近调用时间。

   - 查看该 IP 相关告警信息，默认展示未处理告警，单击**详情**可打开**告警详情抽屉**，相关字段说明请参考 告警 。

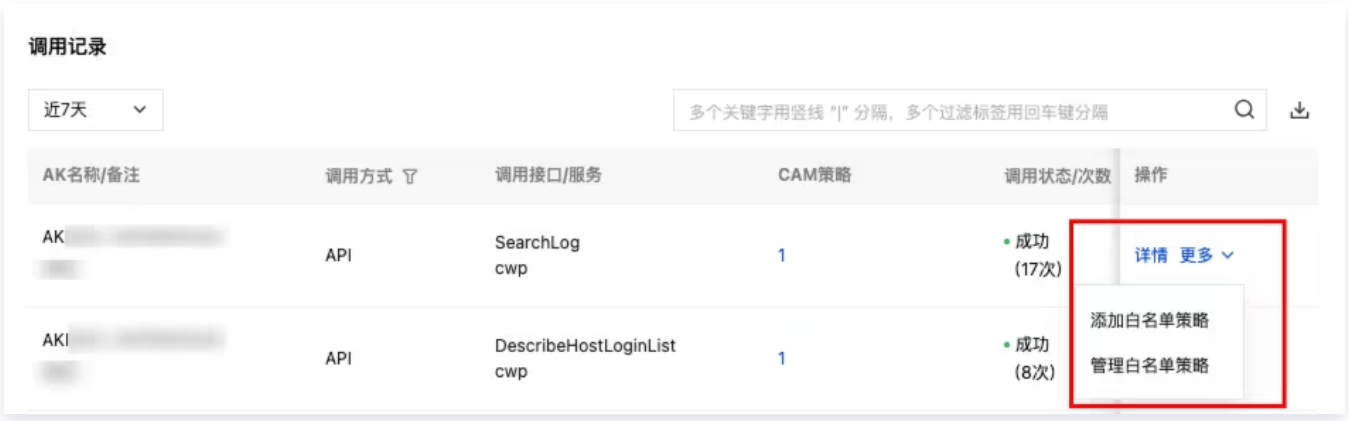
   - 查看调用记录，包括调用该 AK 的 IP 地址、IP 类型、调用方式、服务名称、成功与失败的调用次数、首次/最近调用时间，以及相关的 CAM 策略。



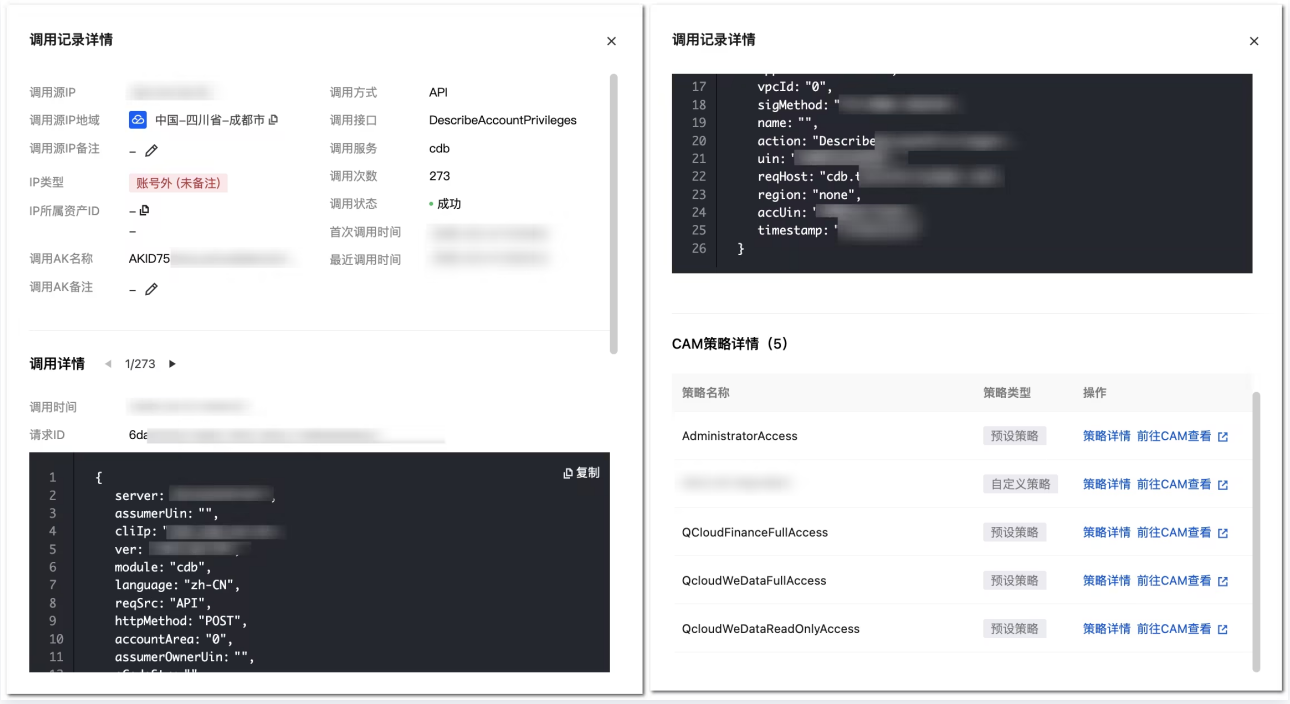
字段名	示例	说明
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 **AK 详情**抽屉。 • 备注可自定义编辑，不超过20字符，若备注为空显示“-”
调用方式	• API • 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。
调用接口/服务	DescribeAccountPrivileges cdb	调用的接口与接口所属服务。
CAM 策略 用户（角色）/策略	1 用户：xxx 策略：1	该 AK 关联的 CAM 策略个数，单击**数字**打开 CAM 策略详情弹窗。 临时密钥由于聚合展示,所以展示用户（角色）。

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。
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**调用源 IP 详情 > 基本信息 > 调用记录**，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**。

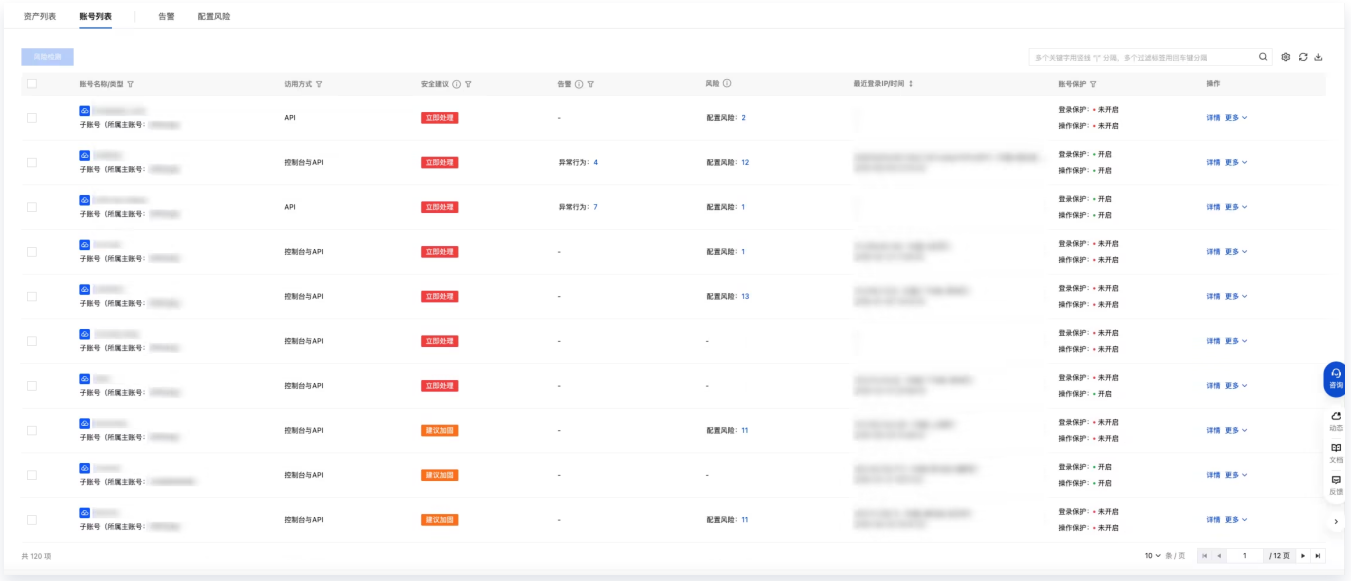
- 更多
  - 添加白名单策略：单击拉起**添加白名单策略**抽屉，填充生效策略、对应 IP、调用方式、AK、接口、返回码，填写说明请参见 策略管理 。
  - 管理白名单策略：单击拉起**策略管理**抽屉，跳转至**策略管理 > 白名单策略**。

账号列表

最近更新时间：2025-09-11 14:33:01

查看账号列表

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. 在账号列表中，基于账号视角，查看账号的基本信息、安全建议、关联告警与风险。



字段名	示例	说明
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。 • 鼠标悬浮查看账号名称、账号 ID与 APPID。
访用方式	• API • 控制台与 API	• 该账号的访问途径。 • 支持筛选 API/控制台与 API。
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	• 异常行为：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	配置风险：x	近期未处理风险，单击拉起 **AK 详情**抽屉，定位到风险页签。

最近登录IP/时间	• 1.x.x.1（中国-广东省-深圳市） • 2025-01-12 18:00:00	• 最近一次登录的IP地址（含地理位置）及登录时间。 • 时间格式：YYYY-MM-DD HH:MM:SS。 • 支持按时间排序。
账号保护	• 登录保护：开启 • 操作保护：开启	• 展示账号的登录保护与操作保护等安全状态的开启情况。 • 支持筛选全部开启/部分开启/未开启。

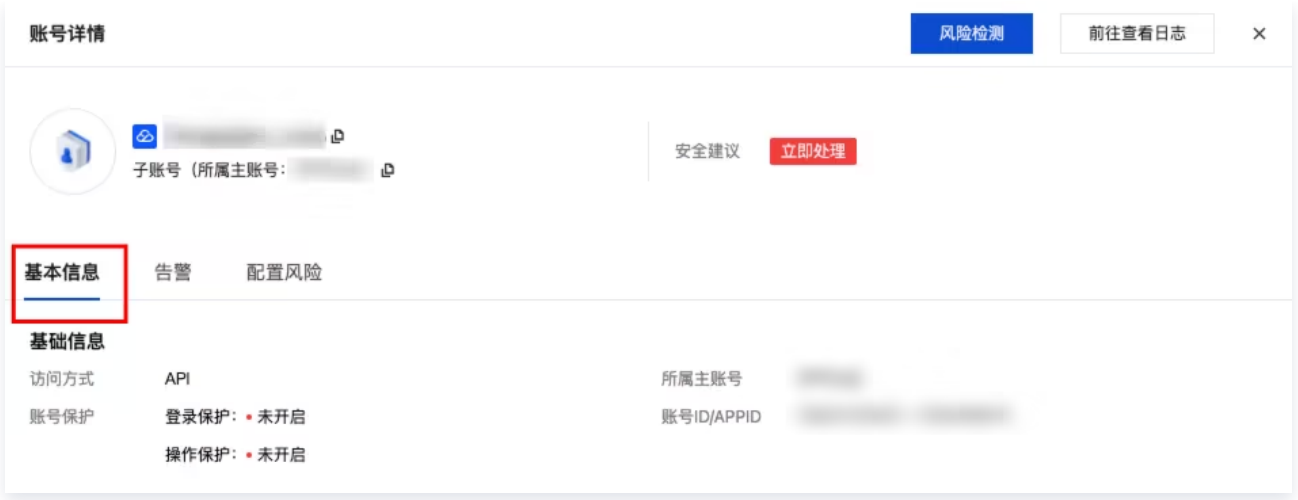
3. 在账号列表中，选择所需账号，单击**详情/更多**。

操作类型		说明
详情		单击拉起**账号详情**抽屉。
更多	风险检测	单击后重新检测该规则。
	前往查看日志	单击跳转至**日志分析 > 增值服务日志检索**。

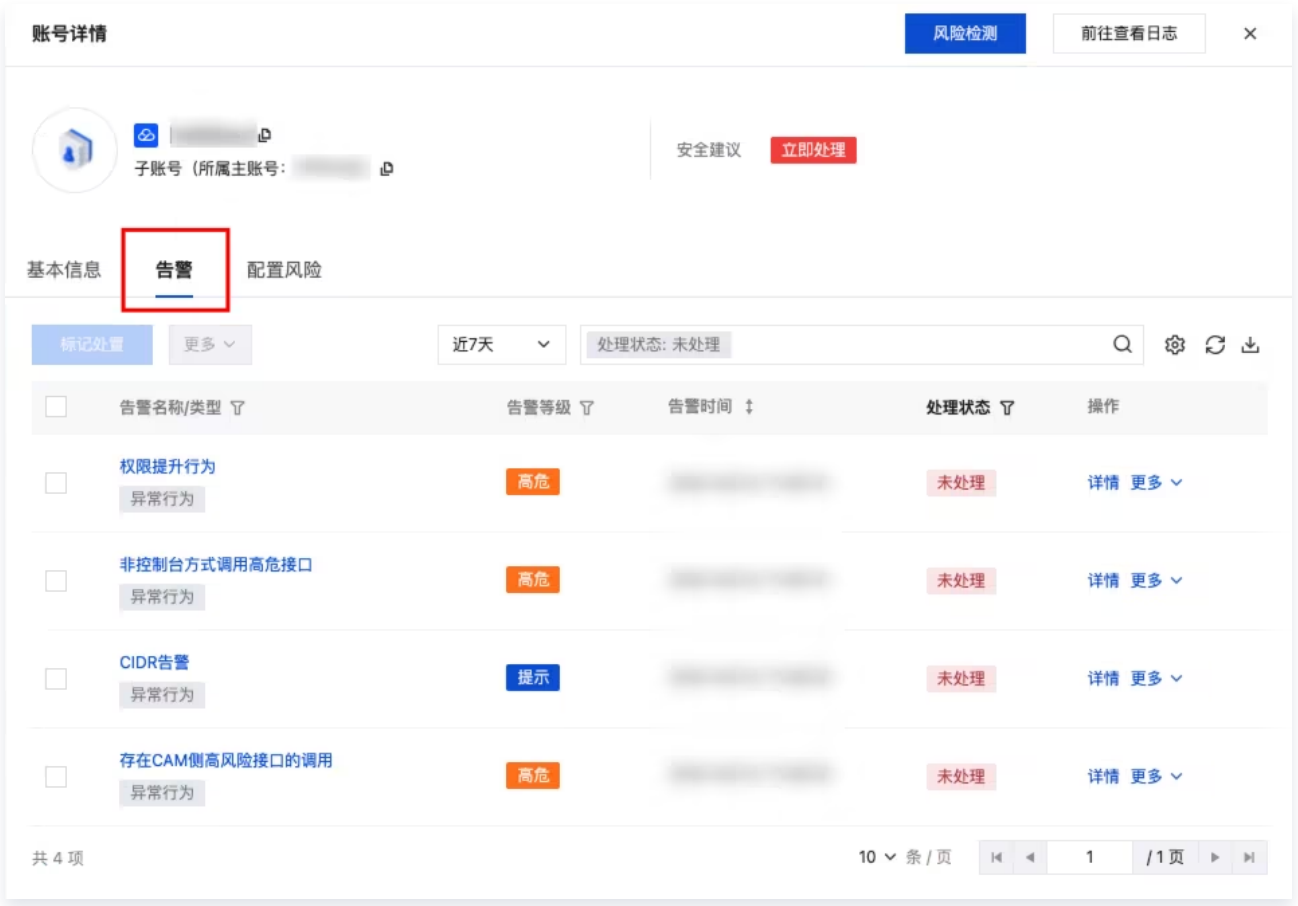
查看账号详情

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. 在账号列表中，选择所需账号，单击**详情**。

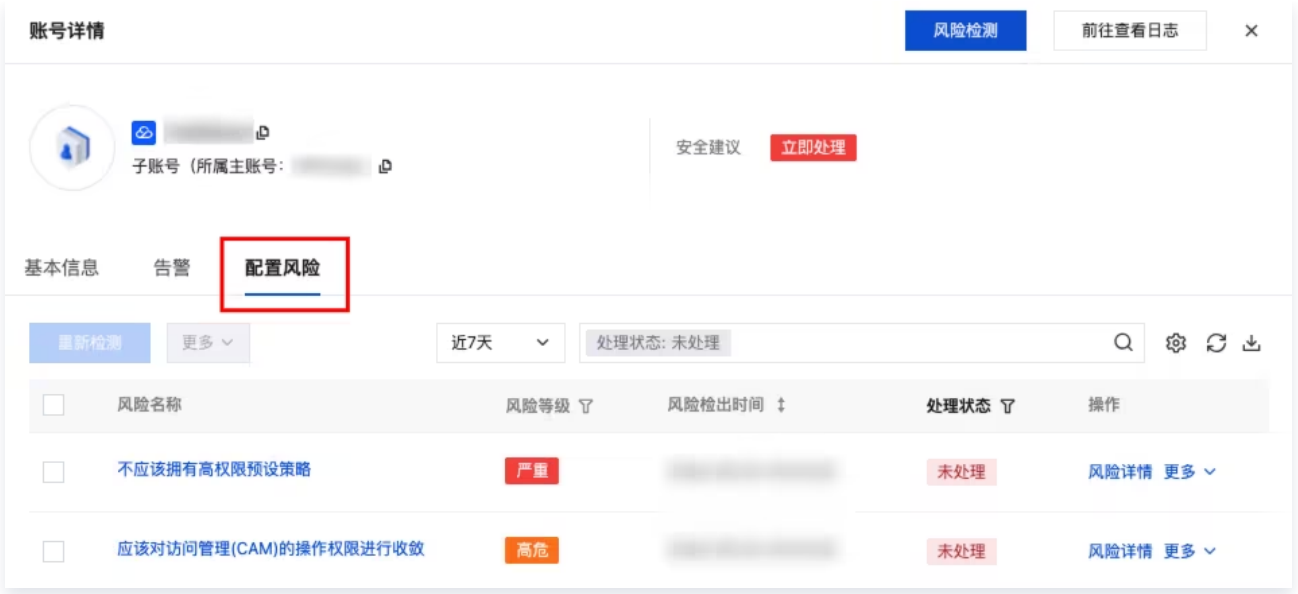
3. 在账号详情页面，查看账号基本信息、关联告警与配置风险、调用记录与关联资产。
   - 查看账号基本信息，账号基本信息包括：访问方式、账号保护状态、所属账号、账号 ID 及 APPID。



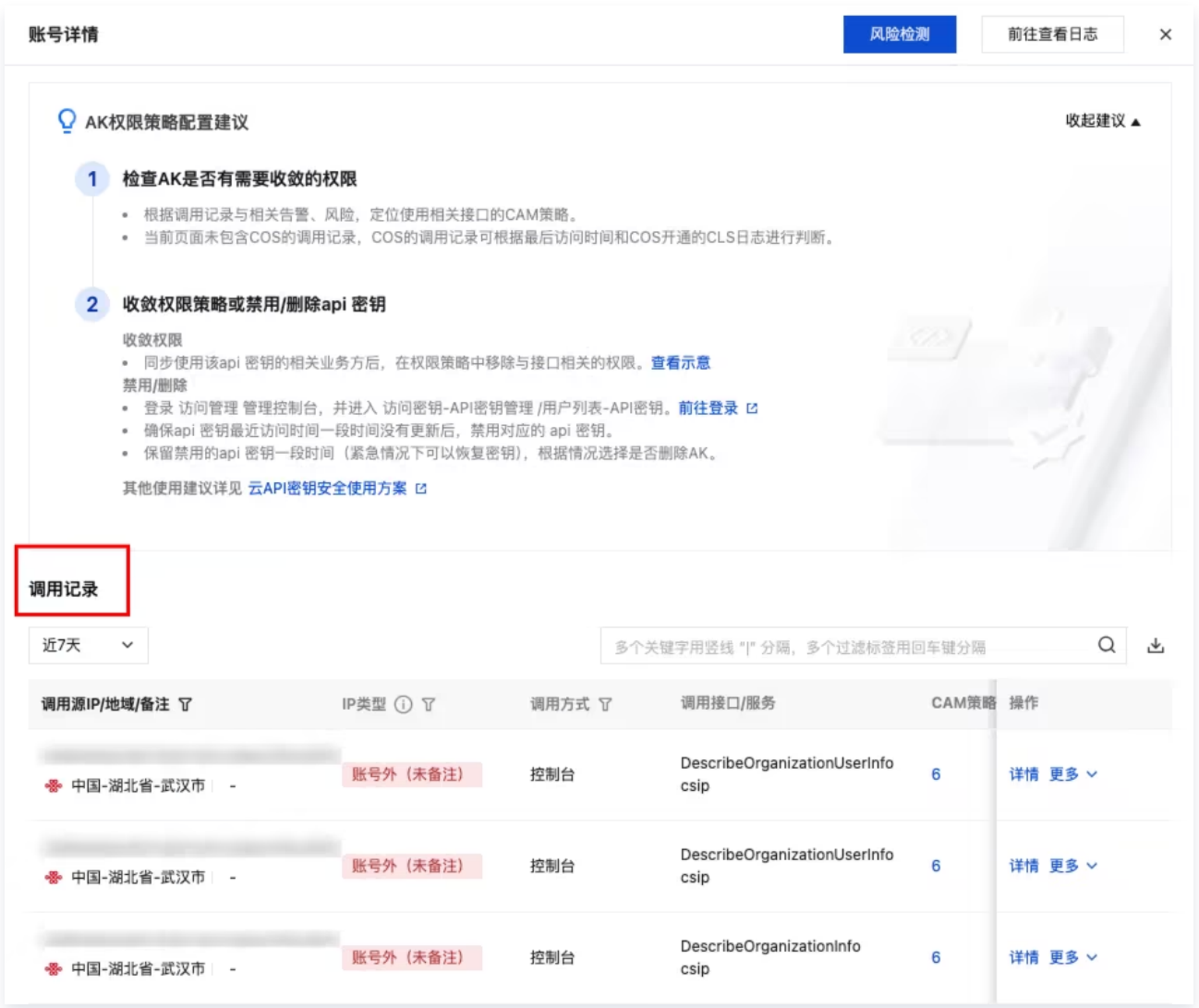
- 查看账号告警信息，默认显示未处理告警。单击**详情**可打开**告警详情抽屉**，相关字段说明请参考 告警 。



- 查看账号风险信息，默认展示未处理风险。单击**详情**可打开**风险详情抽屉**，相关字段说明请参考 配置风险 。



- 查看调用记录，包括调用该 AK 的 IP 地址、IP 类型、调用方式、服务名称、成功与失败的调用次数、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.x.x.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	• 账号内（已备注） • 账号内（未备注） • 账号外（已备注） • 账号外（未备注） • 局域网（已备注） • 局域网（未备注）	• 账号内（已备注）：在云安全中心资产列表中识别到的调用源 IP，有备注。 • 账号内（未备注）：在云安全中心资产列表中识别到的调用源 IP，无备注。 • 账号外（已备注）：非账号内 IP 但有备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 局域网（已备注）：局域网 IP 地址，有备注。 • 局域网（未备注）：局域网 IP 地址，无备注。
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 策略用户（角色）/策略	1 用户：xxx 策略：1	该 AK 关联的 CAM 策略个数，单击**数字**打开 CAM 策略详情弹窗。 临时密钥由于聚合展示,所以展示用户（角色）。
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**账号详情** > **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，跳转至访问管理 > 策略 > 具体策略详情。**

- 更多
  - 添加白名单策略：单击拉起**添加白名单策略**抽屉，填充生效策略、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**。

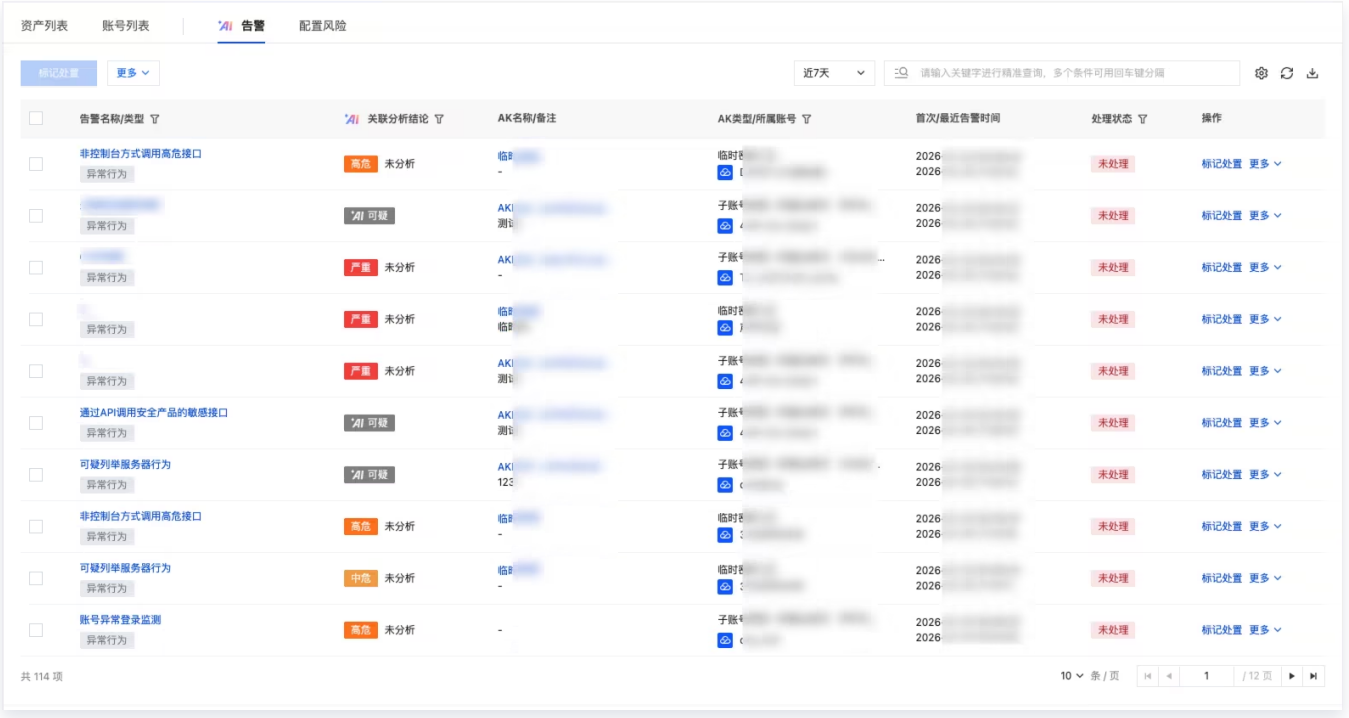
告警

最近更新时间：2026-02-06 16:37:21

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. 告警列表支持从规则视角快速聚焦核心信息：告警内容（泄露、异常调用）、关联分析结论（真实/可疑告警），以及关联的 AK 与异常调用记录。同时，系统提供具体告警处置建议以指导响应。

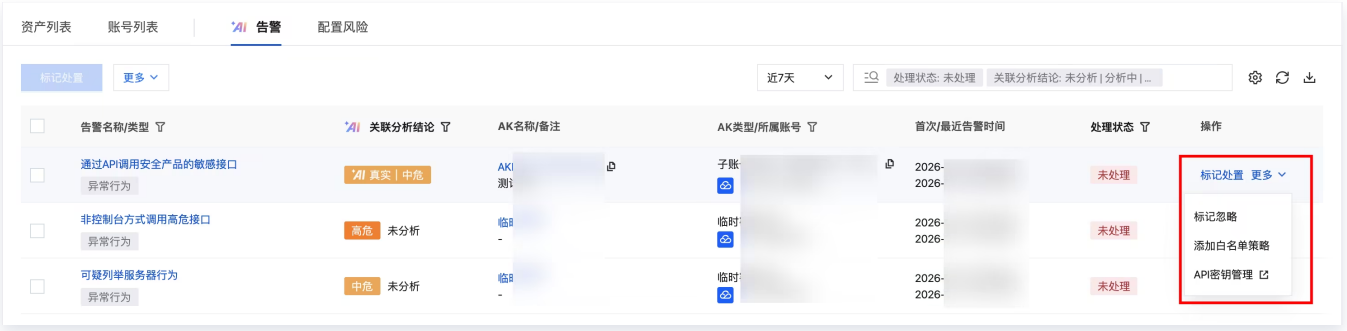
> **说明：**
> AI 研判机制深度融合异常调用记录与安全运营专家思维链，通过多维交叉验证请求源（IP/AK）的可信度、历史行为基线及权限边界，结合 API 调用时序与语义进行风险分析，精准判定真实告警或可疑告警，并输出处置与修复建议，实现闭环安全研判。



字段名	示例	说明
告警名称/类型	可疑列举服务器行为 异常行为	告警名称与所属类型，单击拉起**告警详情**抽屉。 支持筛选异常行为/泄露监测。
关联分析结论	真实 | 高危	结合调用记录以及腾讯云安全专家思维链，评定告警等级并输出分析结论。 支持筛选真实告警/可疑告警/分析中/未分析/分析失败。 • 真实告警：经验证确认存在明确风险，需重点关注并及时处置的告警。

		• 可疑告警：经分析可能为误报，在当前业务场景下暂不视为有效告警，建议进行人工核实。 • 未分析：自定义告警策略不支持分析/临时密钥告警不支持分析。 • 分析失败：AI 分析任务创建失败/AI 分析任务调用失败/AI 分析结果解析失败/AI 分析超时。
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“–”。
AK类型/所属账号	主账号密钥 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。 • 支持筛选主账号密钥/子账号密钥/项目密钥/临时密钥。
首次/最近告警时间	2026-01-12 18:00:00 2026-01-12 18:00:00	首次和最近发生告警的时间。 • 格式：YYYY-MM-DD HH:MM:SS。 • 支持排序。
处理状态	未处理	展示告警处理状态，手动完成标记。 支持筛选未处理/已处置/已忽略。

3. 在告警列表中，选择所需告警，单击**标记处置/更多**。



操作类型		说明
标记处置		单击后处理状态变为“已处置”
更多	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。
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 GitHub AK 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,可以可视化地管理云上 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。

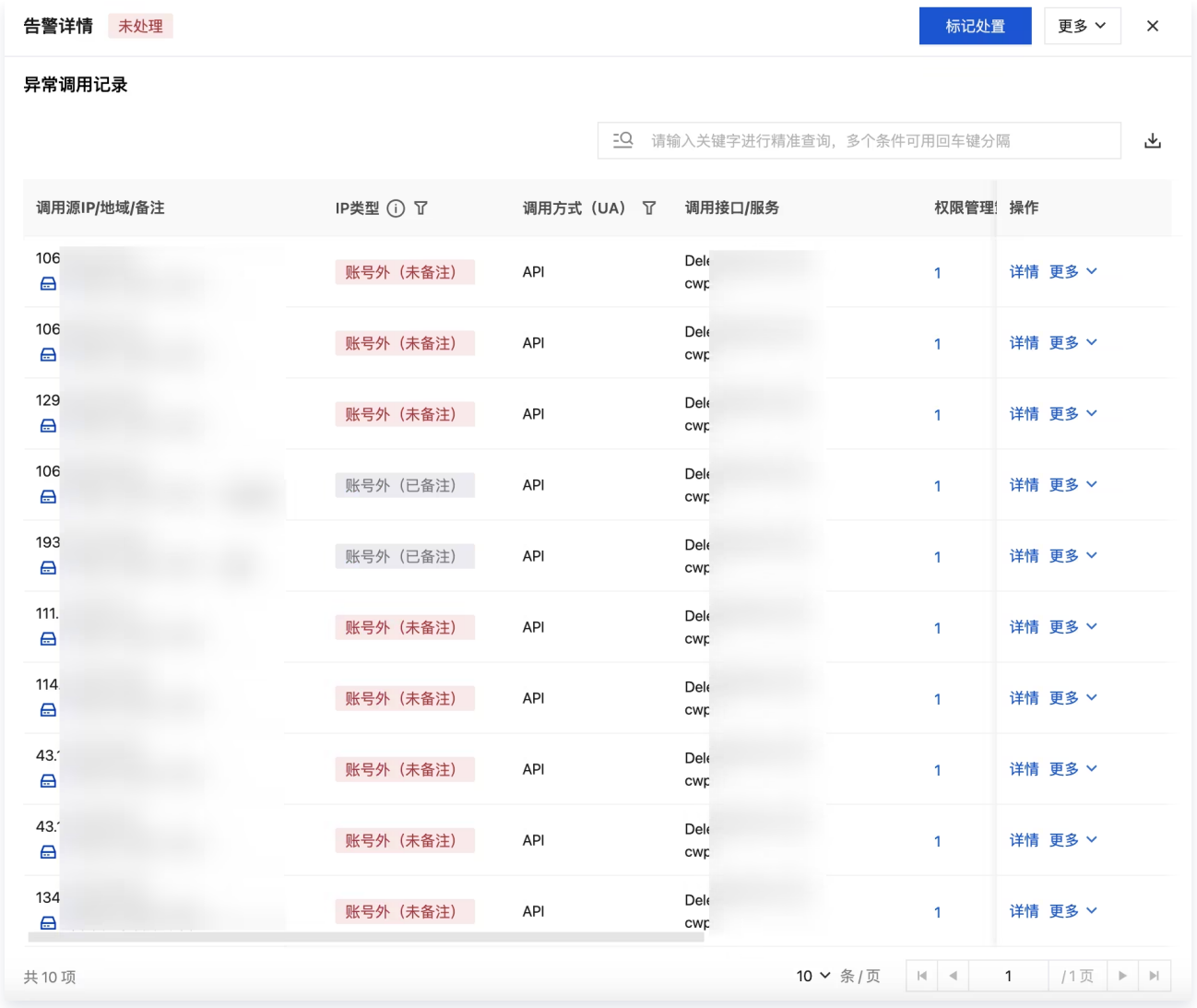
告警详情

1. 在告警列表中，选择所需告警，单击**告警名称**。
2. 在告警详情页面， 查看告警信息、告警关联分析与异常调用记录。

- 查看告警信息。告警信息包括：告警描述/等级/关联分析结论、首次/最近告警时间、AK 名称/备注/类型/关联风险、账号名称以及权限管理策略。

- 查看告警关联分析。告警关联分析包括：结论、研判综述、关键证据链、攻击源与影响面以及处置与加固建议。

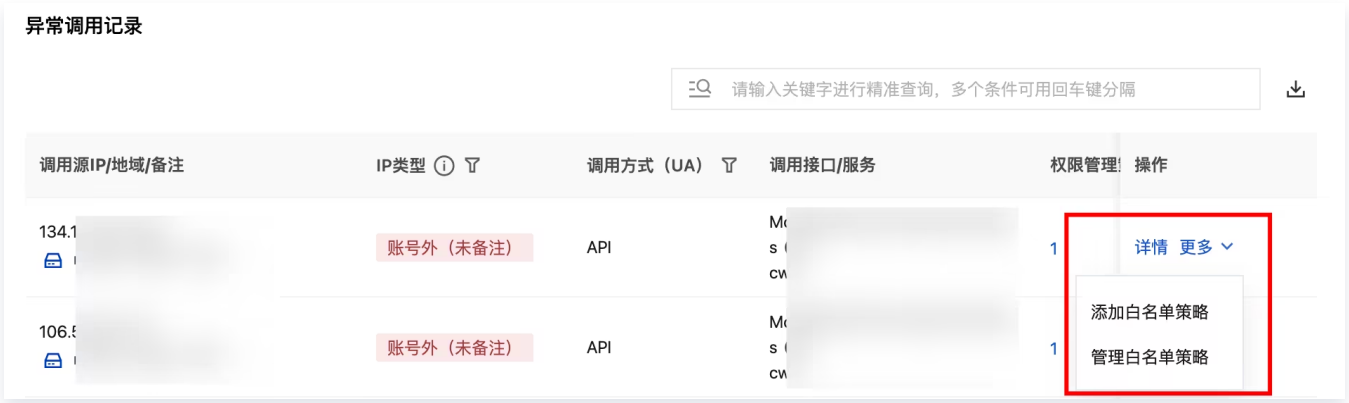
- 查看异常调用记录，包括调用该 AK 的 IP 地址/类型/方式/接口/服务/所属资产、成功与失败的调用次数、首次/最近调用时间，以及权限管理策略。



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	• 账号内（已备注） • 账号内（未备注） • 账号外（已备注） • 账号外（未备注） • 局域网（已备注）	• 账号内（已备注）：在云安全中心资产列表中识别到的调用源 IP，有备注。 • 账号内（未备注）：在云安全中心资产列表中识别到的调用源 IP，无备注。 • 账号外（已备注）：非账号内 IP 但有备注。 • 账号外（未备注）：非账号内 IP 且无备注。 • 局域网（已备注）：局域网IP地址，有备注。 • 局域网（未备注）：局域网IP地址，无备注。

	• 局域网（未备注）	
调用方式（UA）	• 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。
权限管理策略	1	展示该调用关联的权限管理策略个数，单击**数字**打开权限管理策略详情弹窗。
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**。

- 更多
  - 添加白名单策略：单击拉起**添加白名单策略**抽屉，填充生效策略、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**。

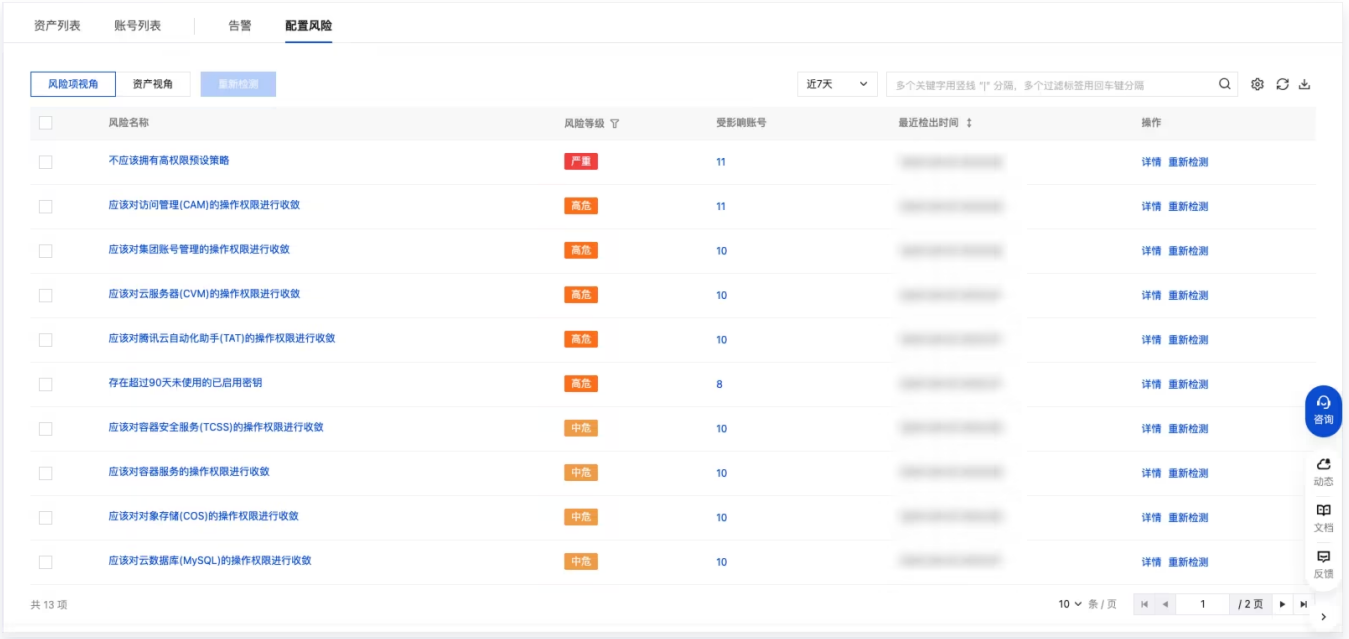
配置风险

最近更新时间：2025-12-11 14:40:12

风险项视角

风险列表

1. 登录 云安全中心控制台，在左侧导航中，单击**云 API 异常监测**。
2. 在**配置风险 > 风险项视角**中，基于风险项视角自动化扫描 AK 权限配置， 识别存在风险的 AK，并直接展示所有受影响的具体账号列表。



字段名	示例	说明
风险名称	不应该拥有高权限预设策略	单击打开**风险项详情**抽屉。
风险等级	• 严重 • 高危 • 中危 • 低危 • 提示	基于腾讯云安全实践评定风险等级。
受影响账号	1	单击数字打开**风险项详情**抽屉。
最近检出时间	2025-01-12 18:00:00	风险检出时间。 格式：YYYY-MM-DD HH:MM:SS。 支持排序。

3. 在风险项视角列表中，选择所需风险，单击**详情/重新检测**。

操作类型	说明
详情	单击打开**风险项详情**抽屉，查看风险描述与关联账号信息，并依据账号当前处理状态执行相应操作。
重新检测	单击后重新检测该规则。

风险项详情

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**配置风险 > 风险项视角**中，选择所需资产，单击**详情**。

3. 在**风险项详情**页面，查看风险项基本信息、受影响账号以及配置建议。
   - 查看风险项基本信息。

   - 查看受影响账号列表，默认显示未处理风险的账号。

字段名	示例	说明
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。 • 鼠标悬浮查看账号名称、账号 ID与 APPID。
账号保护	• 登录保护：开启 • 操作保护：开启	• 展示账号的登录保护与操作保护等安全状态的开启情况。 • 支持筛选全部开启/部分开启/未开启。
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 • 已收敛	展示风险处理状态，手动完成标记，处理状态支持筛选。

	• 已忽略	

4. 在**风险项详情 > 受影响账号**页面，选择所需账号，单击**风险详情/更多**。

操作类型		说明
风险详情		单击打开**风险详情**抽屉，查看风险描述与判定证据。
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**。

风险详情

1. 在**风险项详情 > 受影响账号**页面，选择所需账号，单击**风险详情**。

2. 在**风险详情**页面，查看风险基本信息、风险证据以及描述、风险相关接口调用情况以及配置建议。
   - 查看风险基本信息，风险基本信息包括：所属账号、账号身份、访问方式、账号保护、相关 CAM 策略、关联账号告警以及相关 AK 与关联告警。

- 查看风险描述与证据，该风险详情的证据包括：策略名称、操作、资源以及请求条件。此外还存在另外两类风险证据：AK 名称、创建时间、最近使用时间以及预设策略名称。

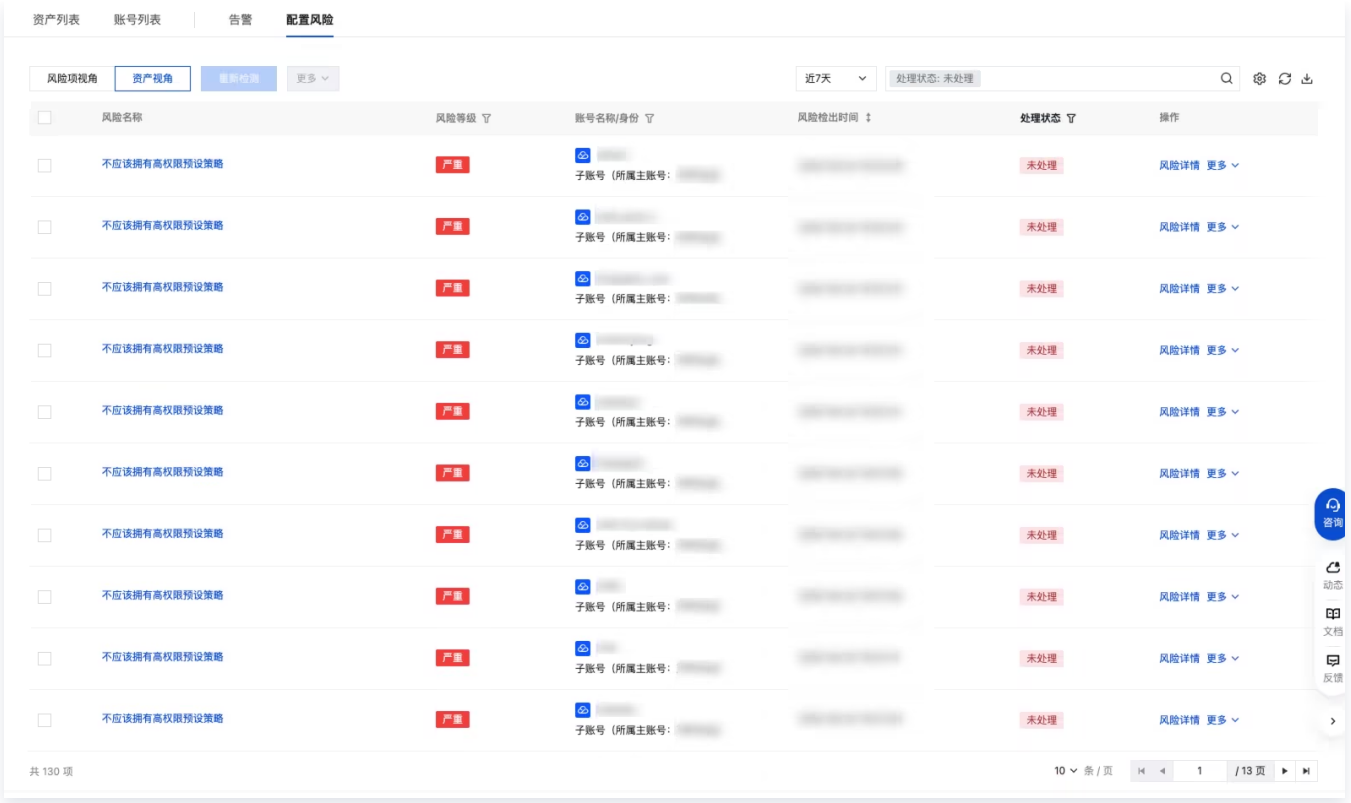
- 查看风险相关接口调用情况以及配置建议。

字段名	示例	说明
接口名称	AddUser	接口的名称，悬浮图标可显示更详细的接口说明。
所属服务	访问管理（cam）	该接口所属的产品或服务模块。
调用次数	1	调用该接口的次数单位。

资产视角

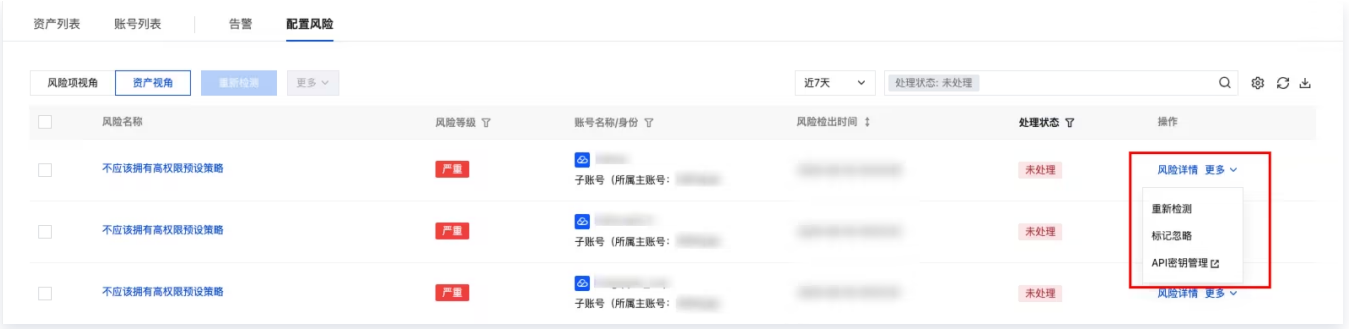
风险列表

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**配置风险** > **资产视角**中，基于资产视角自动化扫描 AK 权限配置， 识别存在风险的 AK，并清晰列出每个风险 AK 对应的受影响账号。



字段名	示例	说明
风险名称	不应该拥有高权限预设策略	单击打开**风险详情**抽屉。
风险等级	• 严重 • 高危 • 中危 • 低危 • 提示	基于腾讯云安全实践评定风险等级。
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 • 已收敛 • 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。

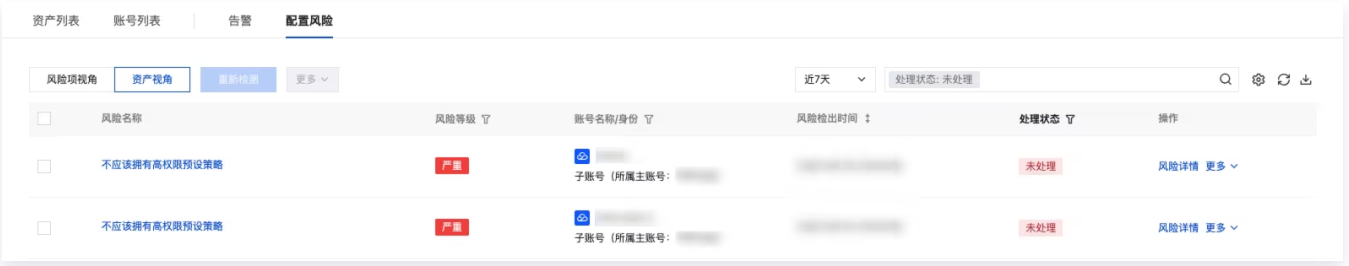
3. 在资产视角列表中，选择所需风险，单击**风险详情/更多**。



操作类型		说明
风险详情		单击打开**风险详情**抽屉，查看风险描述与判定证据。
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**。

风险详情

1. 在**配置风险 > 资产视角**页面，选择所需风险名称，单击**风险详情**。



2. 在**风险详情**页面，查看风险基本信息、风险证据以及描述、风险相关接口调用情况以及配置建议。
   - 查看风险基本信息，风险基本信息包括：所属账号、账号身份、访问方式、账号保护、相关 CAM 策略、关联账号告警以及相关 AK 与关联告警。

- 查看风险描述以及证据。该风险详情的证据包括：策略名称、操作、资源以及请求条件。此外还存在另外两类风险证据：AK名称、创建时间、最近使用时间以及预设策略名称。

- 查看风险相关接口调用情况以及配置建议。

字段名	示例	说明
接口名称	AddUser	接口的名称，悬浮图标可显示更详细的接口说明。
所属服务	访问管理（cam）	该接口所属的产品或服务模块。

调用次数	1	调用该接口的次数单位。

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	应该对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	应该对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	应该对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,

	ModifySecurityGroupPolicies, 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 不应该分配 AdministratorAccess、QCloudResourceFullAccess、QCloudCAMFullAccess、QCloudFinanceFullAccess 高权限预设策略

策略管理

最近更新时间：2025-09-11 14:33:02

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以及添加告警策略、快速定位命中策略的告警。

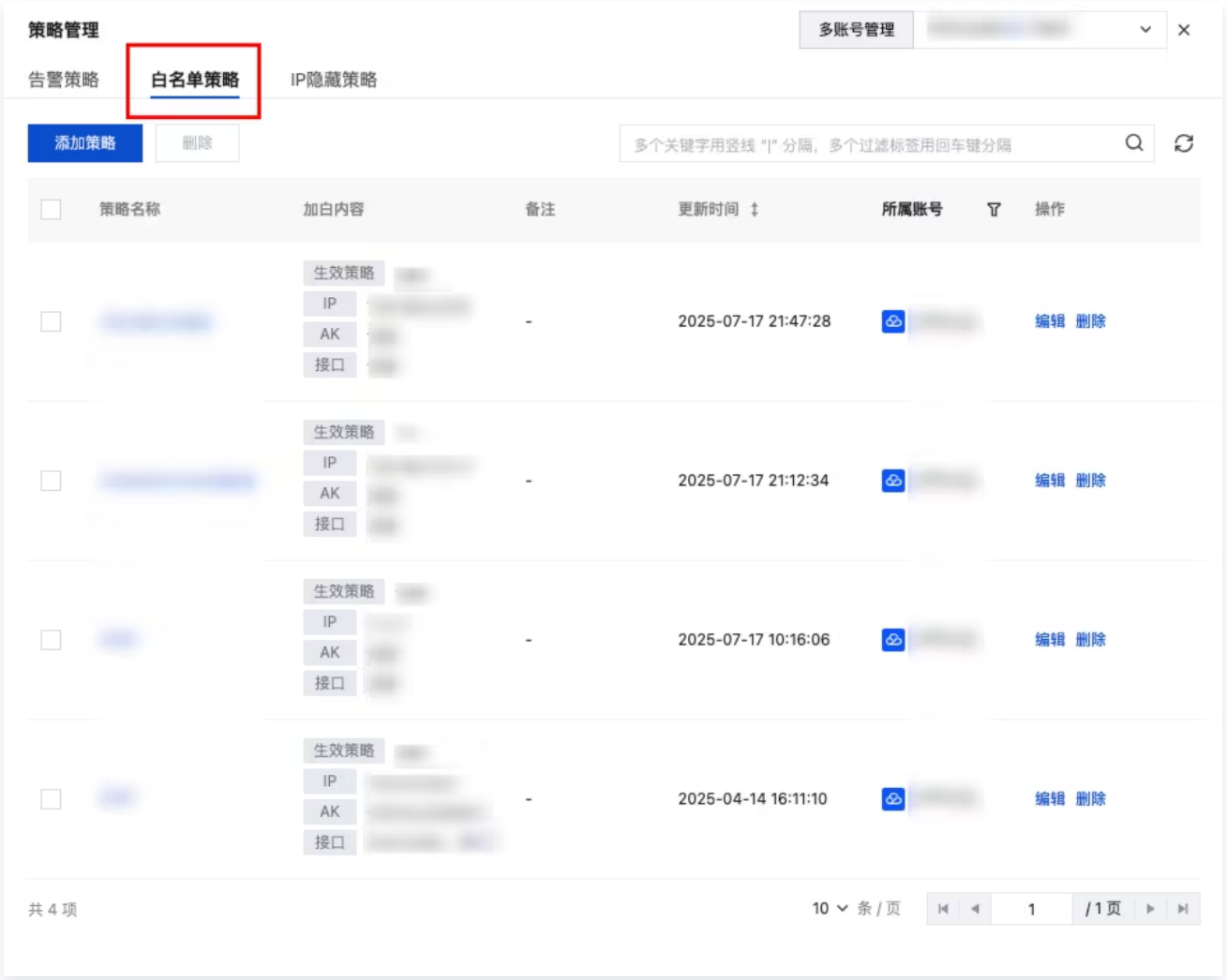
3. 单击**添加策略**，配置相关参数，单击**保存**。

内容名称	说明	示例
生效调用源 IP	支持选择全部源 IP，或按账号内外、局域网、备注状态等类型筛选，也支持手动输入 IP 或网段。多个 IP或类型需换行输入，最多1000行。	1.x.x.1

		x.x.x.x/24
调用方式	可选全部调用方式、控制台或 API，未选择时默认对所有调用方式生效。	-
生效 AK	可选全部 AK，或从现有 AK、长期密钥、临时密钥中选择，也支持手动输入 AK。多个 AK 需换行输入，最多1000行。	AK1 AK2
生效接口	可选全部接口，或手动选择指定接口。未选择时默认对所有接口生效。	-
返回码	选全部返回码，或仅选择成功、失败的返回码。未选择时默认对所有返回码生效。	-

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**。

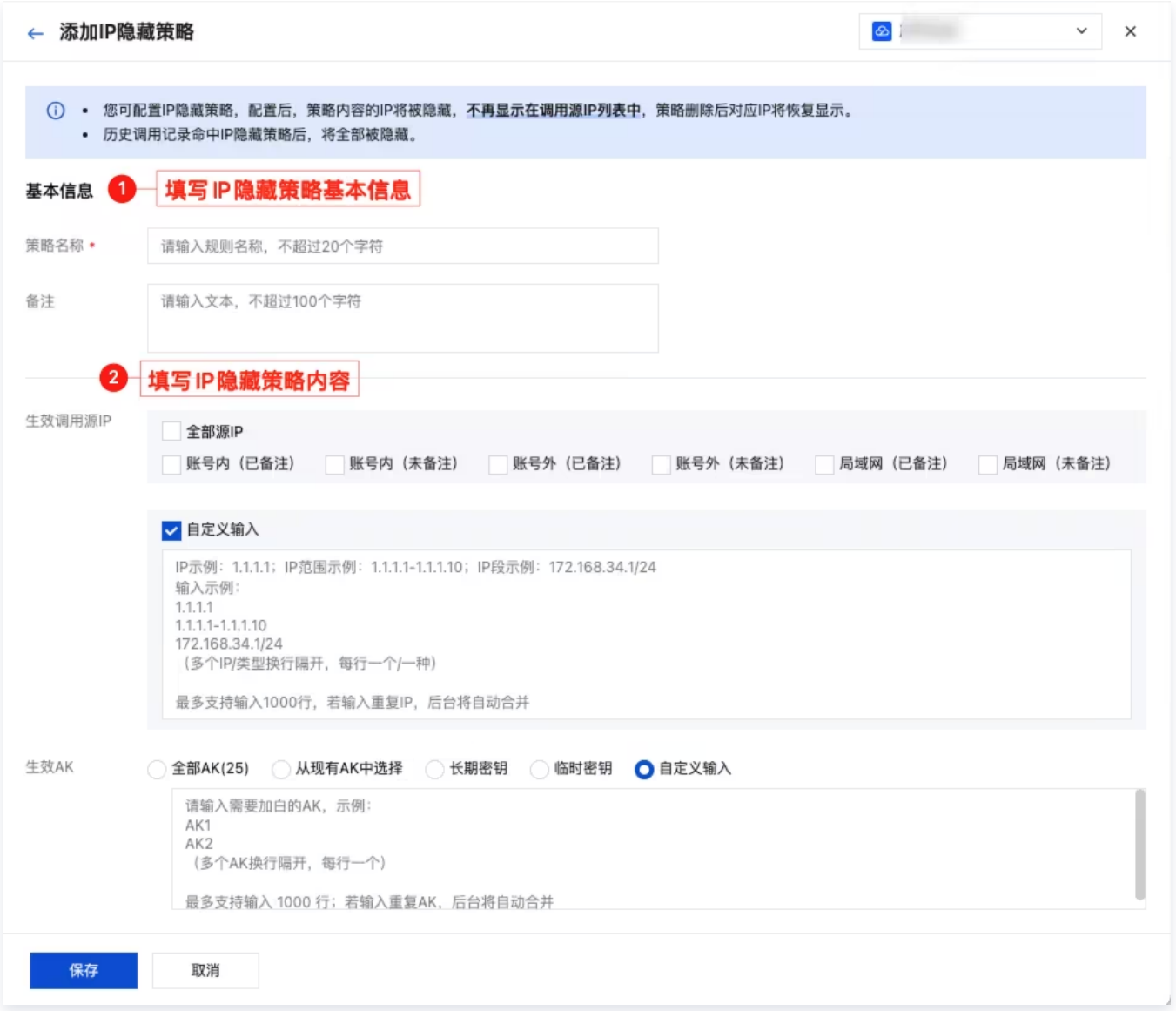
内容名称	说明	示例
生效策略	选择需要加白的告警策略，支持多选；若不选择任何策略，则默认对全部策略生效。	-

生效调用源 IP	支持选择全部源 IP，或按账号内外、局域网、备注状态等类型筛选，也支持手动输入 IP 或网段。多个 IP 或类型需换行输入，最多1000行。	1.x.x.1 x.x.x.x/24
调用方式	可选全部调用方式、控制台或 API，未选择时默认对所有调用方式生效。	-
生效 AK	可选全部 AK，或从现有 AK、长期密钥、临时密钥中选择，也支持手动输入 AK。多个 AK 需换行输入，最多1000行。	AK1 AK2
生效接口	可选全部接口，或手动选择指定接口。未选择时默认对所有接口生效。	-
返回码	选全部返回码，或仅选择成功、失败的返回码。未选择时默认对所有返回码生效。	-

IP隐藏策略

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 > IP隐藏策略**，在此可配置IP隐藏规则，生效后，指定 IP 将不再出现在调用源IP列表中。

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
生效调用源 IP	支持选择全部源 IP，或按账号内外、局域网、备注状态等类型筛选，也支持手动输入 IP 或网段。多个 IP 或类型需换行输入，最多1000行。	1.x.x.1 x.x.x.x/24
生效 AK	可选全部 AK，或从现有 AK、长期密钥、临时密钥中选择，也支持手动输入 AK。多个 AK 需换行输入，最多1000行。	AK1 AK2

接入多云监测

最近更新时间：2025-10-23 16:43:02

多云监测功能目前支持对阿里云的云 API 相关监测，主要功能包括：

- AK 资产与账号接入
- 调用源 IP 梳理
- 异常行为监测
- 配置检查
- 策略管理

步骤1：接入多云多账号

在 多云多账号管理页面，通过 AK 接入方式完成阿里云账号接入，详情请参见 多云多账号管理-多云接入 。

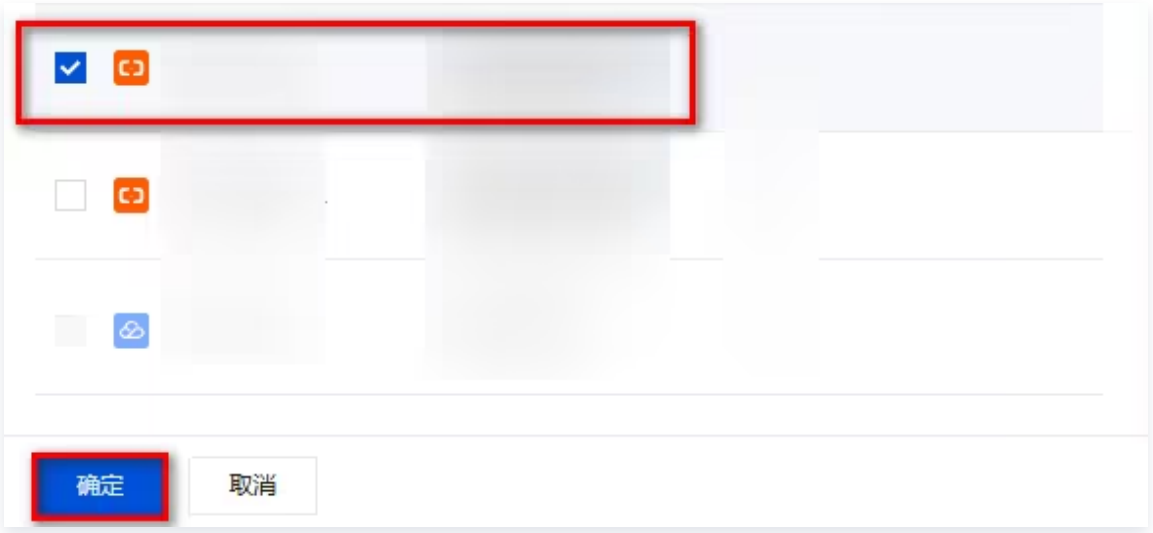
步骤2：将阿里云账号加入云 API 监测账号

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. 在云 API 异常监测页面，单击**监测账号管理**。

3. 在已接入的多云多账号中，单击**编辑**，修改检测账号范围。

> **注意：**
> 取消勾选后，该账号下密钥后续不会继续监测（历史数据保留）。

4. 选择加入云 API 异常监测的账号，单击**确定**保存配置。



步骤3：接入阿里云日志，完成全部接入

将阿里云账号加入云 API 异常监测后，可以完成 AK资产、账号接入与配置检查，若需要进行异常行为监测需要接入阿里云日志。

1. 在 云 API 异常监测页面，单击**监测账号管理**。
2. 在监测账号详情中，找到已加入监测的阿里云账号，单击**接入日志源**。

3. 在日志源接入窗口中，选择阿里云对象存储 OSS 的跟踪集，单击**确定**完成接入。接入完成后，您可以在 云 API 异常监测页面 进行阿里云调用源 IP 梳理、异常行为监测和策略管理。

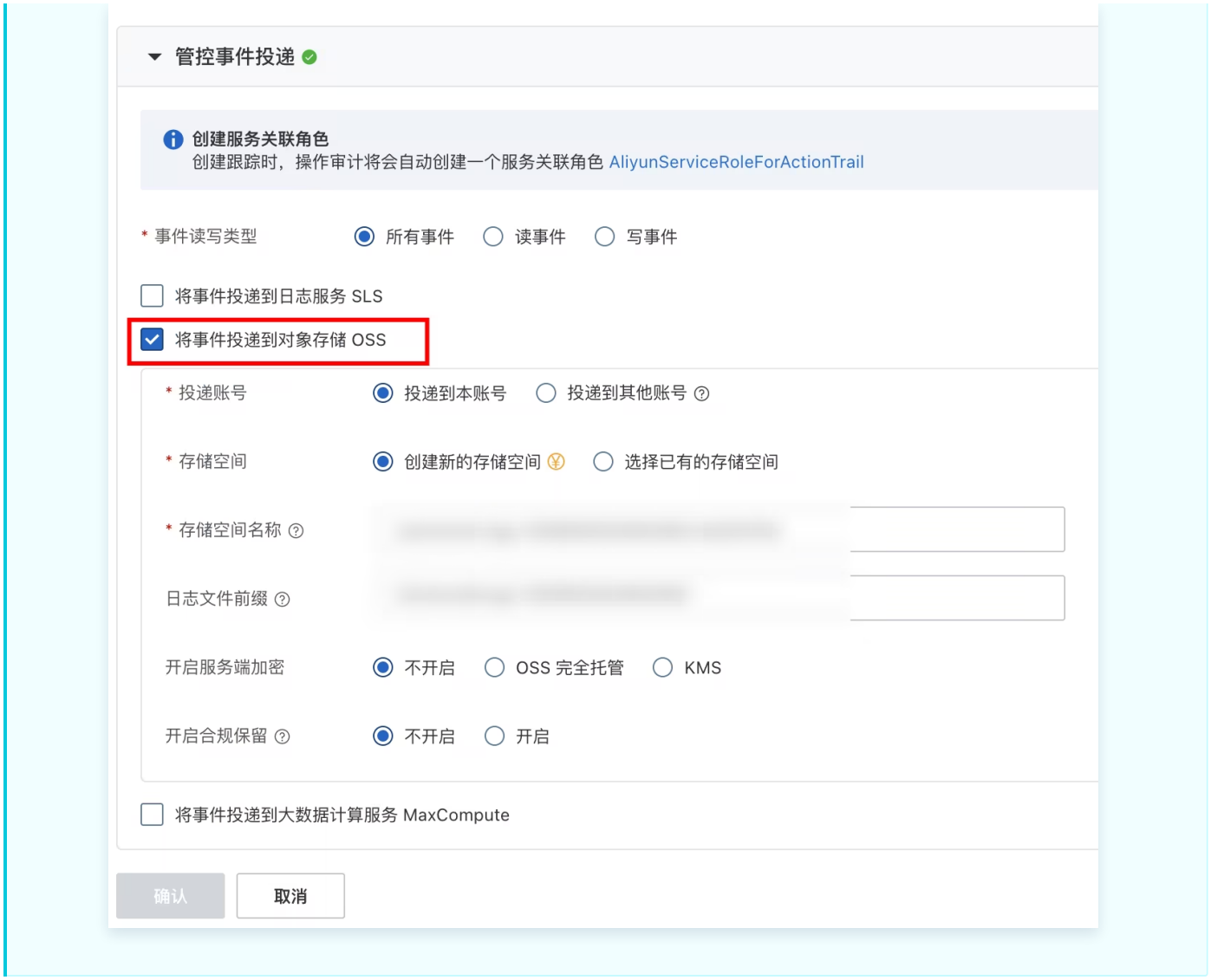
> **说明：**
> 当前阿里云日志接入存在10分钟左右延迟，调用源 IP 梳理、异常行为监测将受到对应影响。

注意：

跟踪集仅展示可用且存储到阿里云OSS的跟踪集，如未创建，请先前往阿里云操作审计 创建跟踪 。

1. 登录阿里云控制台，前往 操作审计 > 跟踪 ，单击**创建跟踪**。

2. 填写基本信息，并在管控事件投递中选择**将事件投递到对象存储 OSS**，单击**确认**完成创建。


管控事件投递
创建服务关联角色
创建跟踪时，操作审计将会自动创建一个服务关联角色 AliyunServiceRoleForActionTrail
* 事件读写类型
所有事件
读事件
写事件
将事件投递到日志服务 SLS
将事件投递到对象存储 OSS
* 投递账号
投递到本账号
投递到其他账号
* 存储空间
创建新的存储空间
选择已有的存储空间
* 存储空间名称
日志文件前缀
开启服务端加密
不开启
OSS 完全托管
KMS
开启合规保留
不开启
开启
将事件投递到大数据计算服务 MaxCompute
确认
取消

数据安全态势管理
对象存储异常监测
功能简介

最近更新时间：2026-01-29 14:57:01

云安全中心通过实时监测对象存储（COS）AccessKey 相关信息，梳理 COS 权限配置与调用路径，并基于腾讯云丰富情报识别**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 COS 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 COS 的权限失控、配置错误、泄露事件响应慢、异常调用难溯源等问题，更好地对 COS 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

功能版块		功能点	解决问题	操作指引
统计面板		快速了解对象存储资产情况，定位建议关注的异常 COS、待处理告警、待处理风险等。	定位高优问题，了解有多少 COS 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	对象存储资产	基于对象存储资产视角，查看基本信息、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。	
	关联 AK	基于对象存储关联 AK 的视角，查看 AK 关联的对象存储资产与资产告警详情。	明确每个 AK 对应的对象存储资产范围，快速定位该 AK 关联资产的安全告警，评估 AK 的影响面与风险程度。	
告警列表			• 实时告警泄露事件，全面分析并溯源异常调用；	告警

		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。	• 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。	
风险列表	风险项视角	基于风险项视角，查看风险详情、受影响存储桶与风险等级、及处置建议。	梳理当前存在的风险项类型与数量，明确每个风险的触发原因、影响范围和严重程度，辅助评估风险优先级并推动处置。	风险
	资产视角	基于资产视角，查看该资产关联的所有风险项、风险证据&描述、风险接口情况及风险处置状态。	定位特定资产存在的风险，明确风险对资产安全的影响，跟踪风险的发现与处置全流程，保障资产安全。	
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。		
	IP 隐藏策略	通过为指定 AK 配置调用源 IP 加白策略，该 AK 后续所有访问 IP 将自动隐藏，不在调用源 IP 列表展示。		

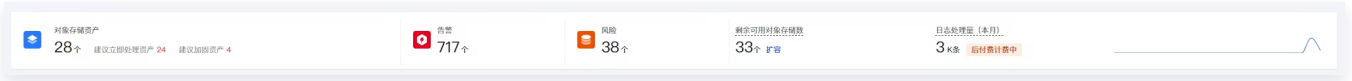
统计面板

最近更新时间：2026-01-29 14:57:01

1. 登录 云安全中心控制台 ，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，将显示当前资产概览、告警概览、风险概览，您可以通过统计面板了解当前对象存储资产安全态势。
   - **对象存储资产：**统计当前已进行同步的对象存储资产数量和不同安全建议的对象存储资产数量。

安全建议	建议说明
建议立即处理	基于当前存储桶的全部待处理告警、风险，为您提供综合的安全等级，请立即关注并处理。
建议立即加固	基于当前存储桶的全部待处理告警、风险，为您提供综合的安全等级，建议进行关注并收敛权限，完成加固。

   - **告警：**统计**全部**待处理的告警。
   - **风险：**统计**全部**待处理的风险。
   - **剩余可用对象存储数：**显示已购买的对象存储资产数以及剩余可用的对象存储资产存储数。
   - **日志处理量：**每天0点更新前一天数据，仅展示当前登录账号所属订单日志处理数据。
3. 单击各概览项中的**数字**，可直接跳转至对应模块的详情页面（如单击 “告警” 跳转至告警列表）。



资产列表

最近更新时间：2026-01-29 14:57:01

对象存储资产

对象存储资产列表

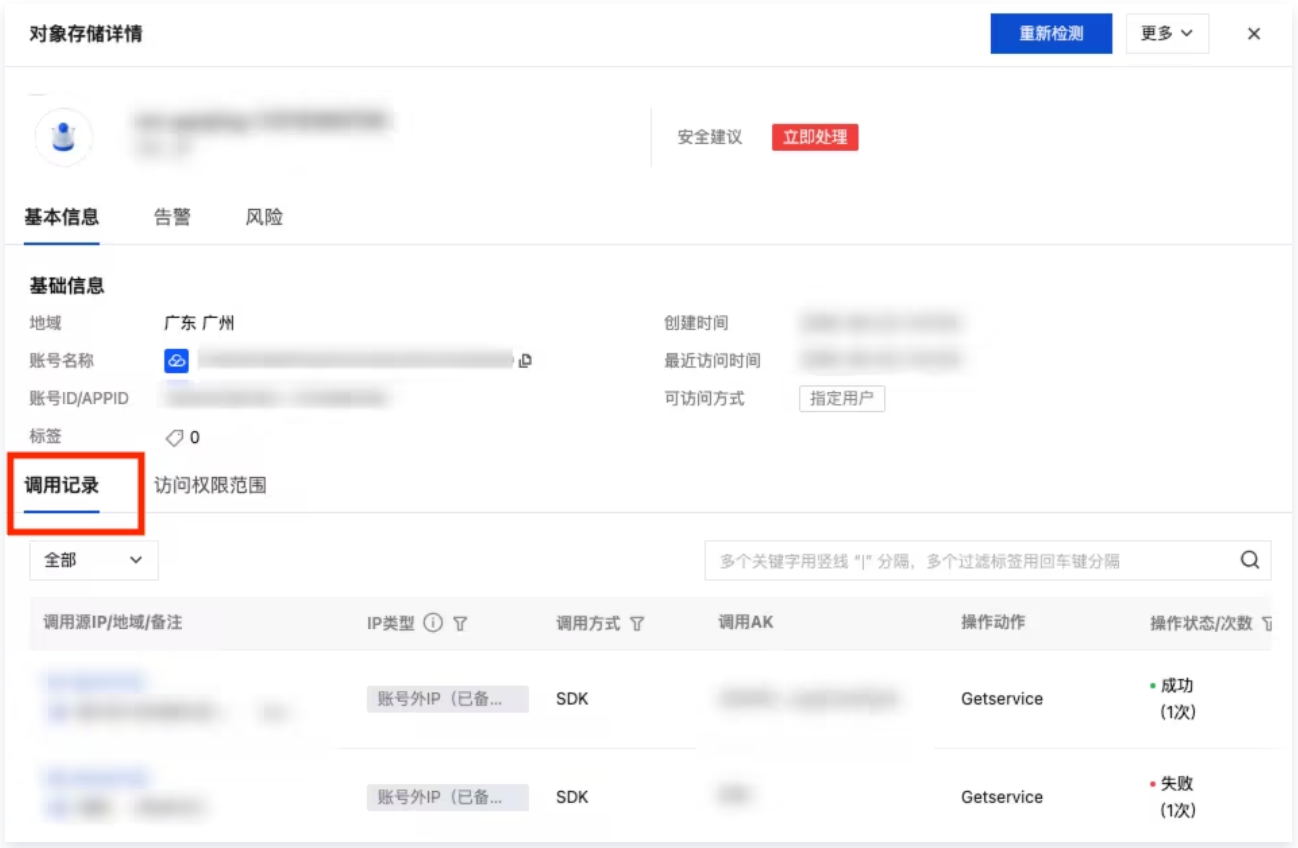
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，**单击资产列表 > 对象存储资产**。
3. 在对象存储资产页中，基于对象存储资产视角，查看存储桶基本信息、安全建议、关联告警与风险。

对象存储详情

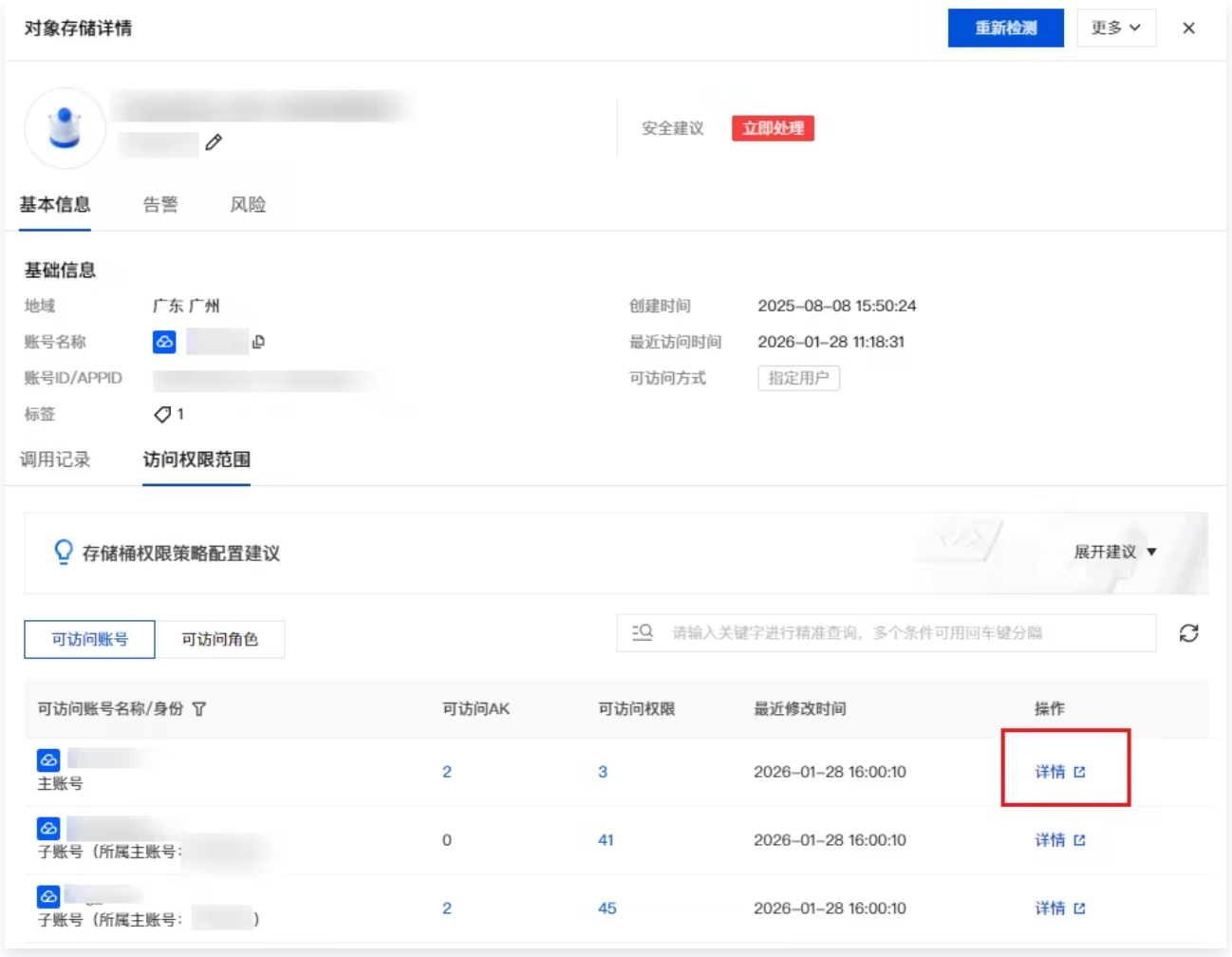
1. 在对象存储资产页中，选择所需资产，单击**详情**。

2. 在对象存储详情页面，您可以查看当前对象存储资产的基本信息、调用记录、访问权限范围以及关联的告警风险详情。通过该页面，您可以针对性地进行数据安全治理。
3. 在对象存储详情页面，单击**基本信息**，可查看存储桶基本信息，包括地域、账号名称、账号 ID/APPID、标签、创建时间、最近访问时间、可访问方式。

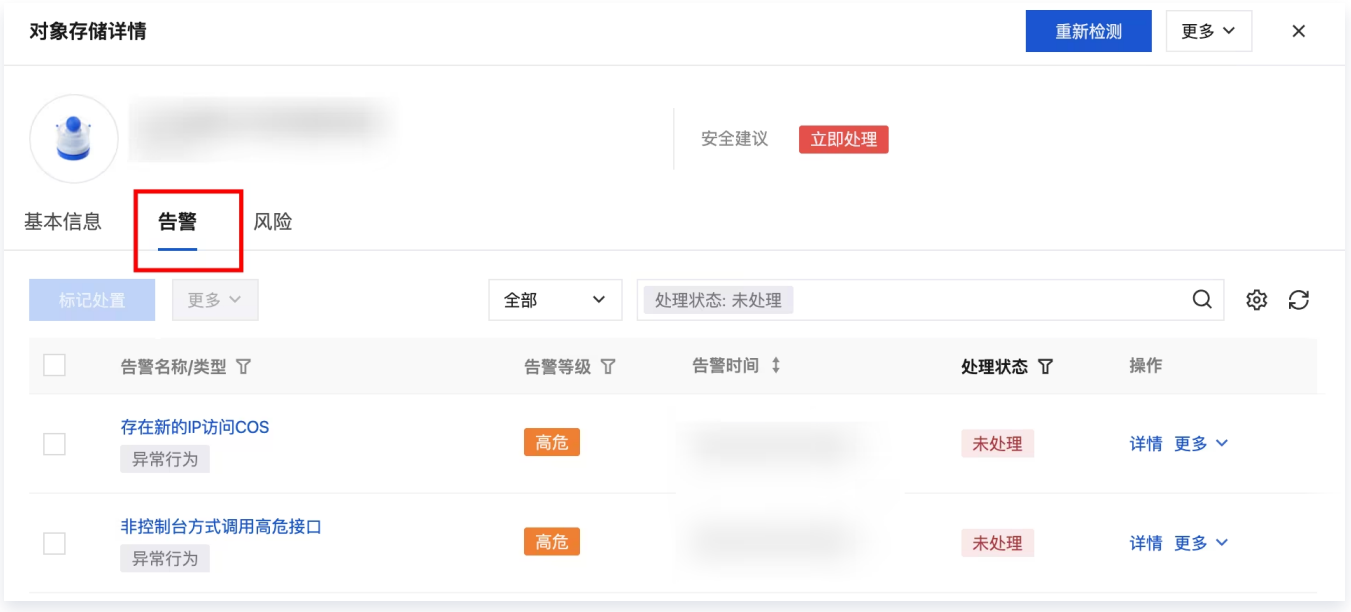
- 在对象存储详情页面，单击**基本信息** > **调用记录**，可查看当前对象存储资产的调用记录，包括：调用源 IP/地域/备注、IP 类型、调用方式、调用 AK、操作动作、操作状态/次数、首次/最近调用时间。



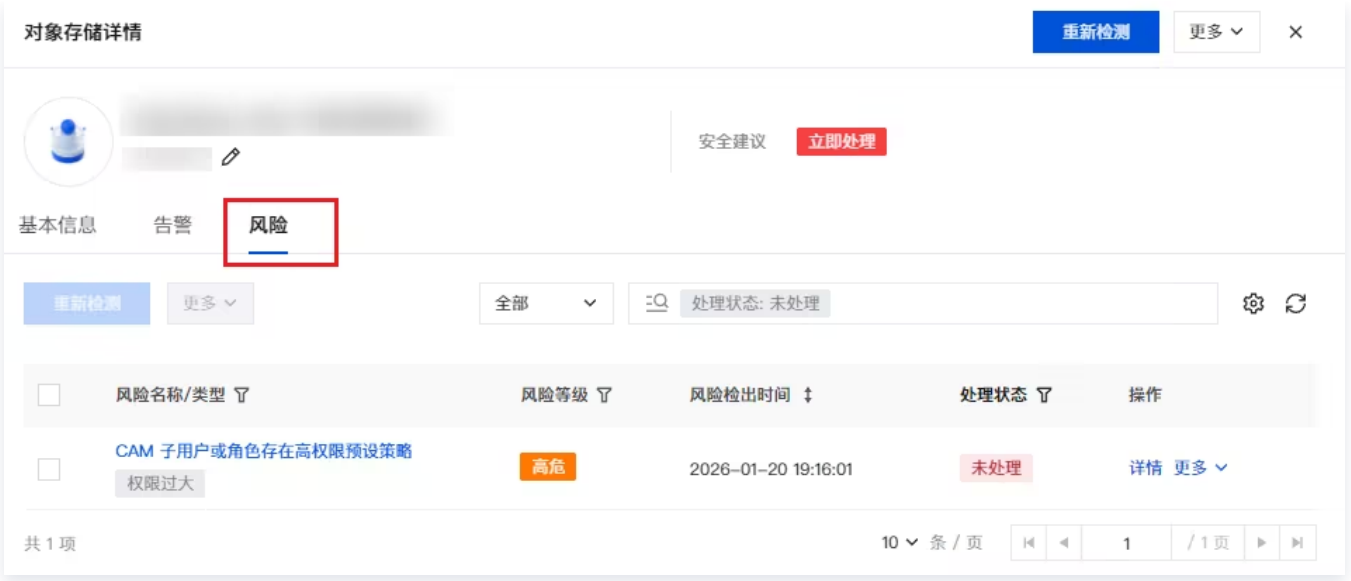
- 在对象存储详情页面，单击**基本信息** > **访问权限范围**，可通过访问账号和访问角色视角查看当前对象存储资产的访问权限范围。



4. 在对象存储详情页面，单击**告警**，可查看当前对象存储资产的告警信息，默认展示未处理告警，单击**详情**可打开**告警详情**。



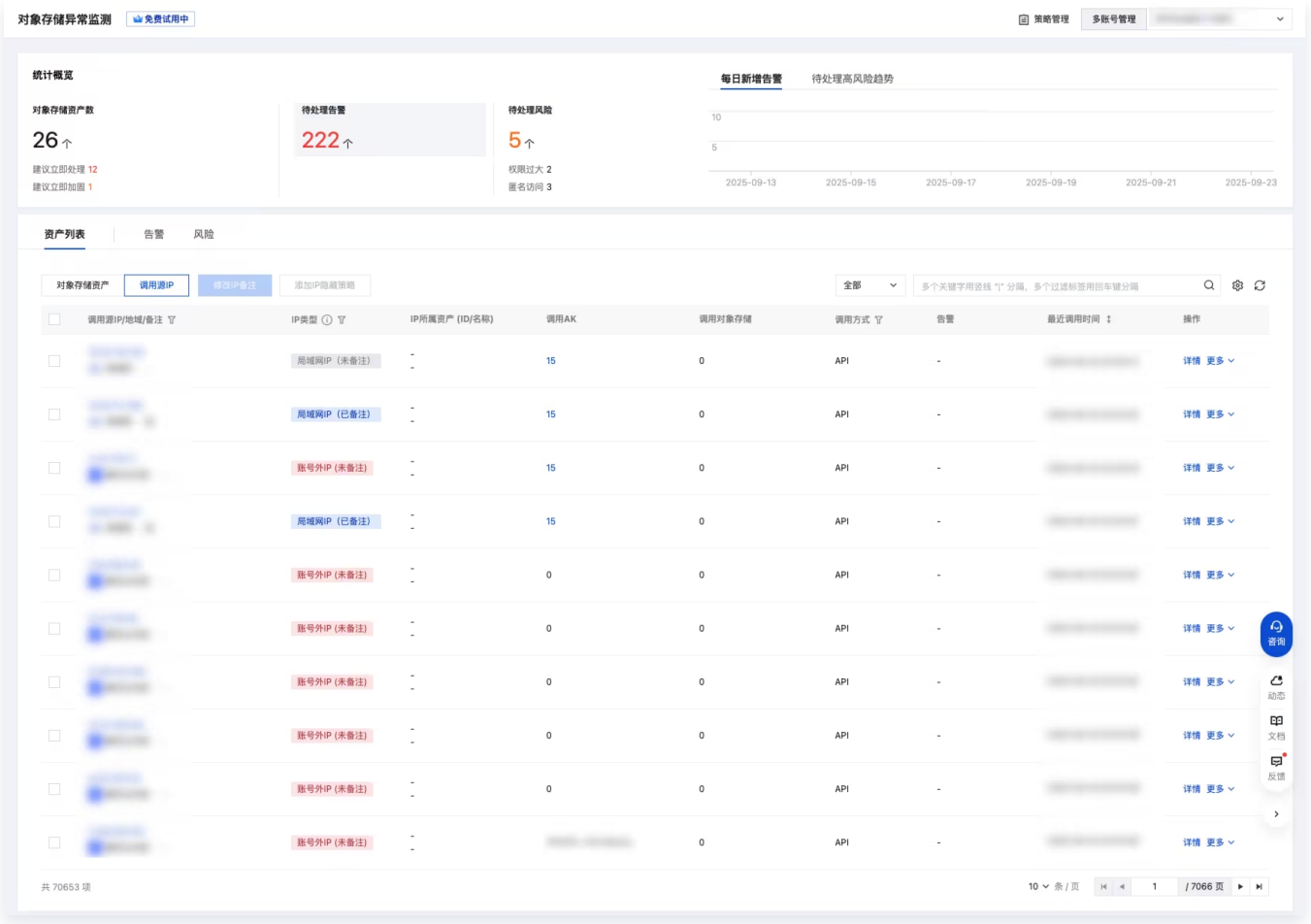
5. 在对象存储详情页面，单击**风险**，可查看存储桶风险信息，默认展示未处理风险，单击**详情**可打开**风险详情**。



调用源 IP

调用源 IP 列表

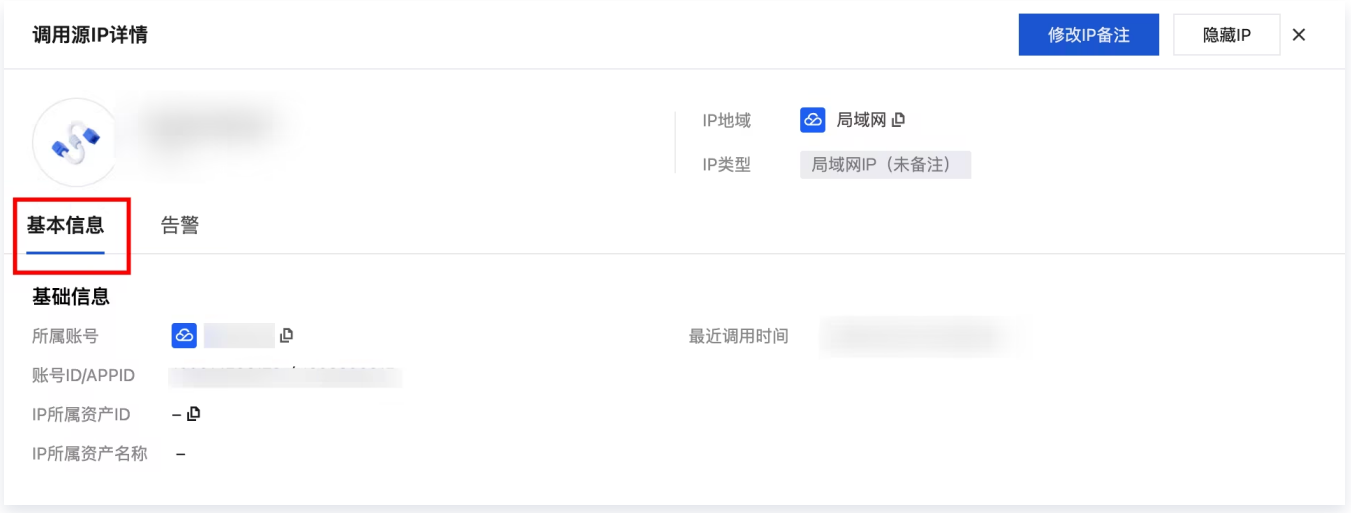
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，**单击资产列表 > 调用源 IP**。
3. 在调用源 IP 页面中，基于调用源 IP 视角，可查看调用源 IP 信息、调用 AK、调用对象存储、关联告警、调用方式以及调用时间。



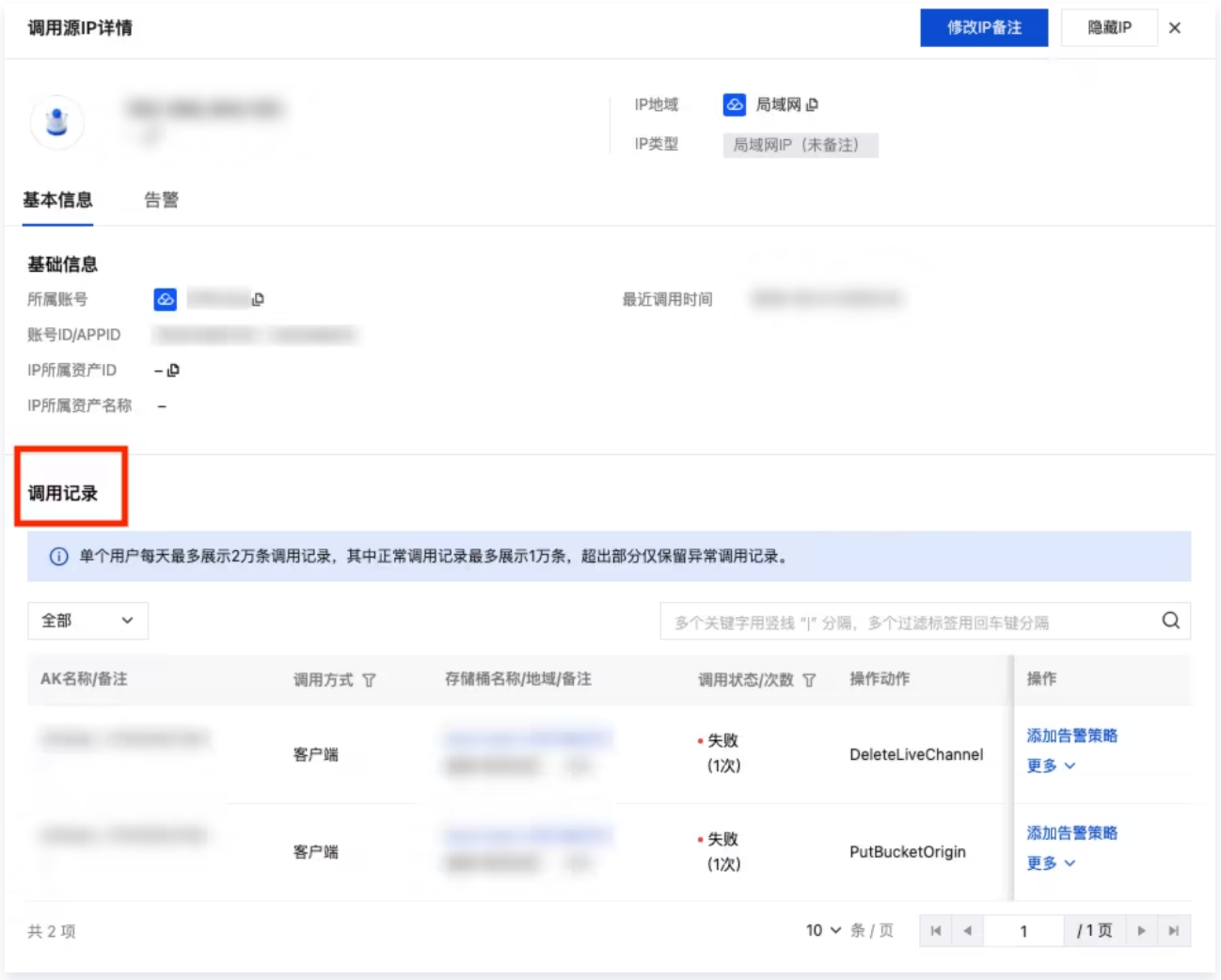
> **说明：**
> 仅展示被永久密钥访问过的IP。

调用源 IP 详情

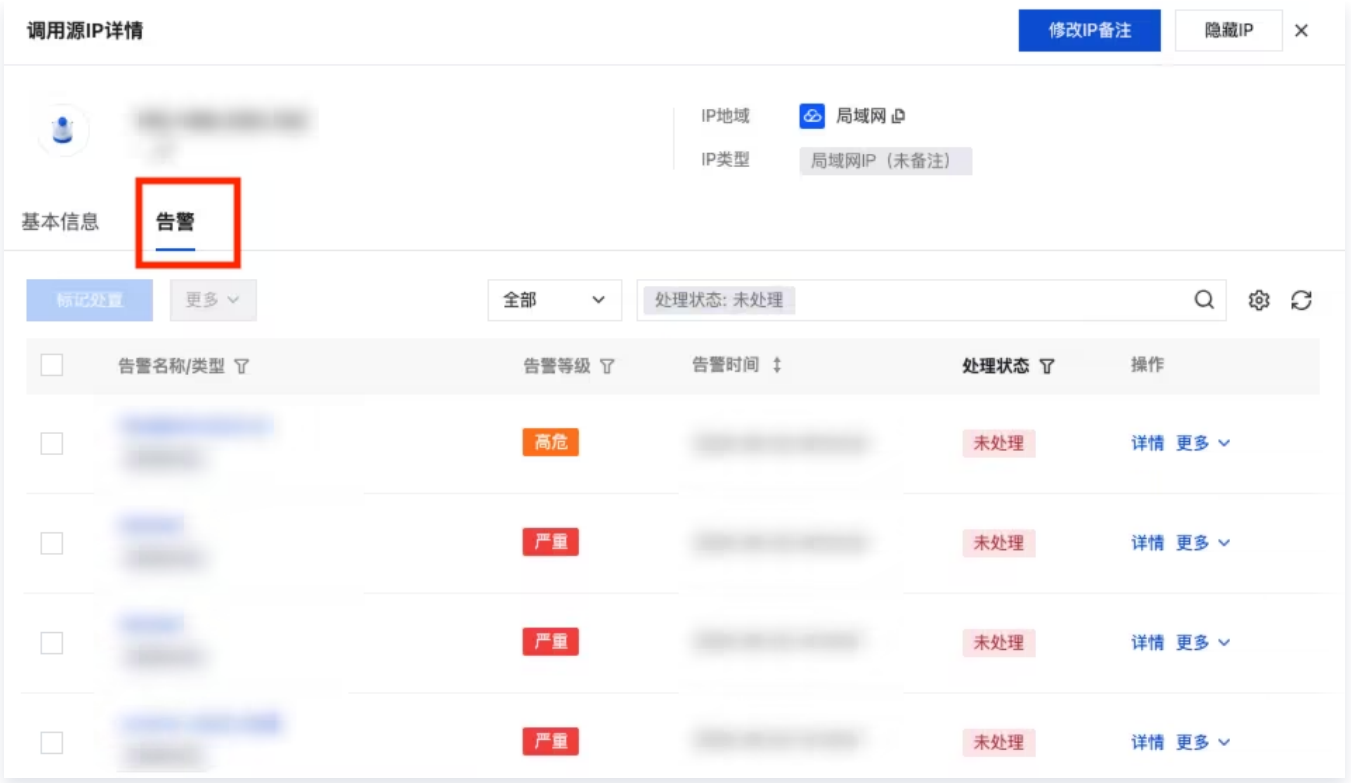
1. 在调用源 IP 页面中，选择所需调用源 IP，单击**详情**。
2. 在调用源 IP 详情页面，单击**基本信息**，可查看当前 IP 的基本信息，包括所属账号、账号 ID/APPID、IP 所属资产 ID、IP 所属资产名称、最近调用时间。



- 在调用源 IP 详情页面，单击**基本信息** > **调用记录**，可查看调用记录，包括 AK 名称/备注、调用方式、存储桶名称/地域/备注、调用状态/次数、操作动作、最近调用时间。



3. 在调用源 IP 详情页面，单击**告警**，可查看该 IP 相关告警信息，默认展示未处理告警，单击**详情**可查看**告警详情**。



关联 AK

> **说明：**
> 关联 AK 仅展示对象存储相关的 AK 资产 ，查看更多完整 AK 资产，或进一步配置策略、管理白名单、查看&处置风险，可前往 云 API 异常监测 。

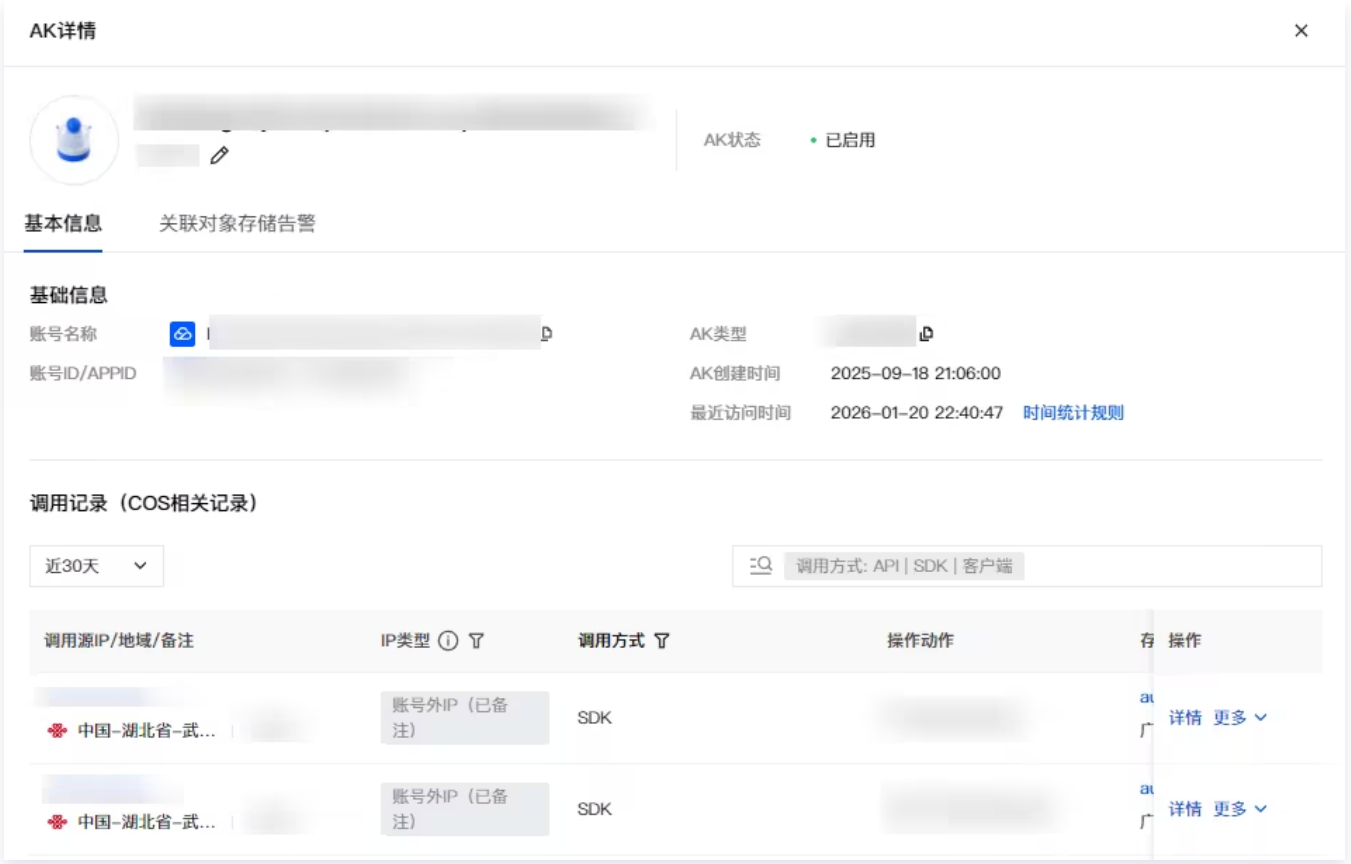
关联 AK 列表将展示对象存储相关的 AK 资产，可通过 AK 视角查看其关联的对象存储资产，以及所关联的对象存储资产告警详情。

AK 详情

登录 云安全中心控制台 ，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。

1. 在对象存储异常监测页面，**单击资产列表 > 关联 AK**。
2. 在关联 AK 页面中，选择所需查看的 AK ，单击**详情**。

3. 在 AK 详情页面，将展示当前 AK 详情、AK 调用详情、AK 所关联的对象存储告警。

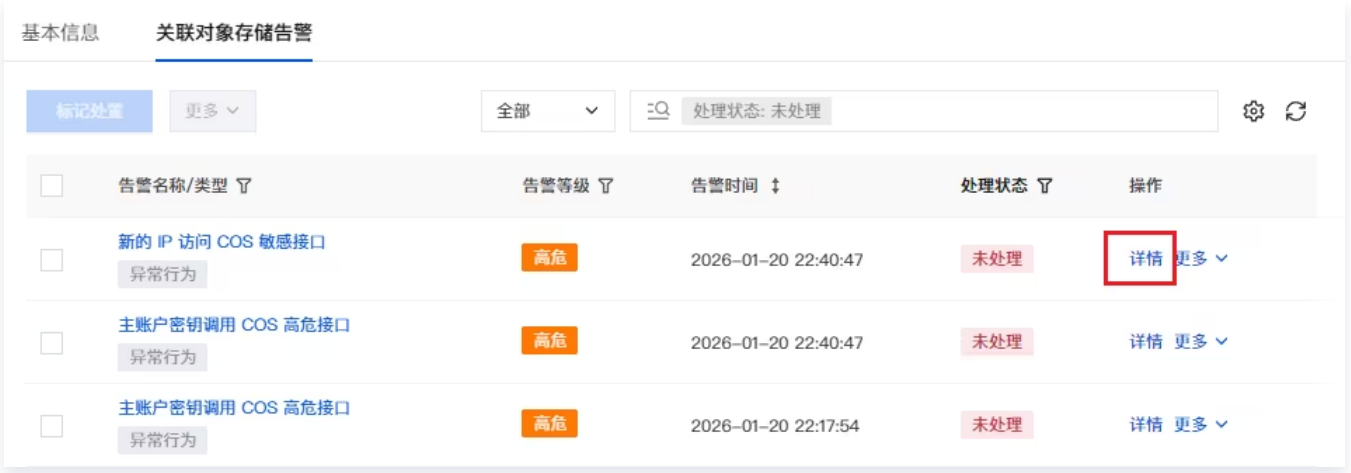


AK 调用记录

1. 在 AK 详情页面，单击**基本信息**。
2. 选择需要查看的 AK 调用记录，单击**详情**，可查看该 AK 的调用详情。

AK 所关联的对象存储告警

1. 在 AK 详情页面，单击**关联对象存储告警**。
2. 在关联对象存储告警页面，将展示当前 AK 所关联的对象存储资产所有的告警信息。
3. 选择需要查看告警详情的告警，单击**详情**，即可查看该告警详情信息。


基本信息
关联对象存储告警
标记处置
更多
全部
处理状态: 未处理
告警名称/类型
告警等级
告警时间
处理状态
操作
新的 IP 访问 COS 敏感接口
异常行为
高危
2026-01-20 22:40:47
未处理
详情
更多
主账户密钥调用 COS 高危接口
异常行为
高危
2026-01-20 22:40:47
未处理
详情
更多
主账户密钥调用 COS 高危接口
异常行为
高危
2026-01-20 22:17:54
未处理
详情
更多

告警

最近更新时间：2026-01-29 14:57:01

告警列表

1. 登录 云安全中心控制台 ，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，单击**告警**。
3. 在告警列表中，基于告警规则视角，查看告警信息、存储桶信息以及账号信息，并提供权限策略配置建议。

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，告警信息包括：告警策略、策略描述、对象存储名称、对象存储备注、标签、地域、账号名称、账号身份、账号ID/APPID、访问方式。

- 查看异常调用记录，调用记录包括：调用源IP/地域/备注、IP 类型、调用方式、调用AK、操作动作、操作状态/次数、首次/最近调用时间。

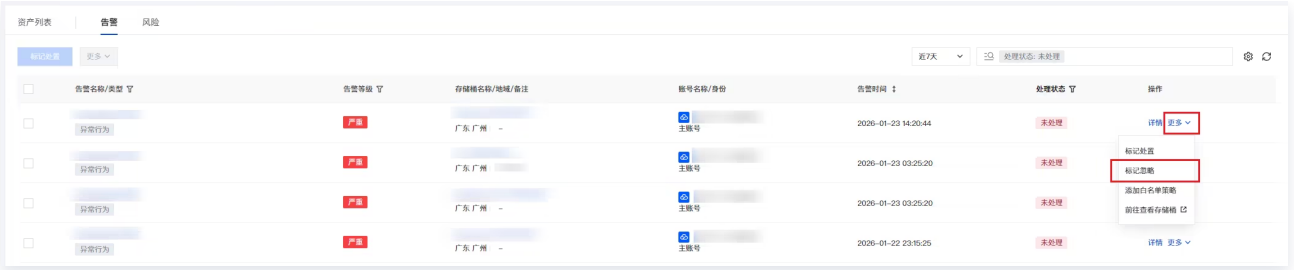
告警处置

标记忽略

对误报或无需处理的告警进行状态标记，排除风险统计干扰。

> **说明：**
> 告警处理状态标记为已忽略，则该风险将不会纳入风险统计中。

1. 在告警标签页面，支持单个或者批量处理目标告警：
   - **单个处置：**单击目标告警操作列的**更多 > 标记忽略**。



- **批量处置：**选择多个目标告警，单击**更多 > 标记忽略**。

2. 在二次确认中，单击**确定**，即可将告警标记为已忽略。

添加白名单

对于需要长期放行的行为，可以将该告警所触发的策略添加至规则白名单中。

1. 在告警标签页面，单击目标告警操作列的**更多 > 添加白名单策略**。

2. 在添加白名单窗口策略中，查看白名单策略内容，确认无误后单击**确定**，即可将该告警所触发的策略信息添加至白名单。

> **说明：**
> 告警白名单策略规则生效后，该行为不再触发告警。

标记已处理

对已完成应急响应的告警进行状态更新，实现处置闭环。

1. 在告警标签页面，选择单个或多个目标告警，单击**标记处置**。

2. 在确认窗口中，核查告警信息，确认无误后，单击**确定**，即可将该告警标记为已处理。

> **说明：**
> 告警处理状态标记已处理后，该告警将不会纳入风险统计中。

风险

最近更新时间：2026-01-29 14:57:01

从风险项与资产双视角，全面呈现风险详情、关联的资产与告警信息、风险等级及处置状态，辅助安全团队评估风险优先级并跟踪风险处置过程。

风险项视角

从风险项视角聚焦风险详情及关联受影响的存储桶资产，可按风险项维度精准定位并处置对应受影响的存储资产，提升风险处置的针对性与效率。

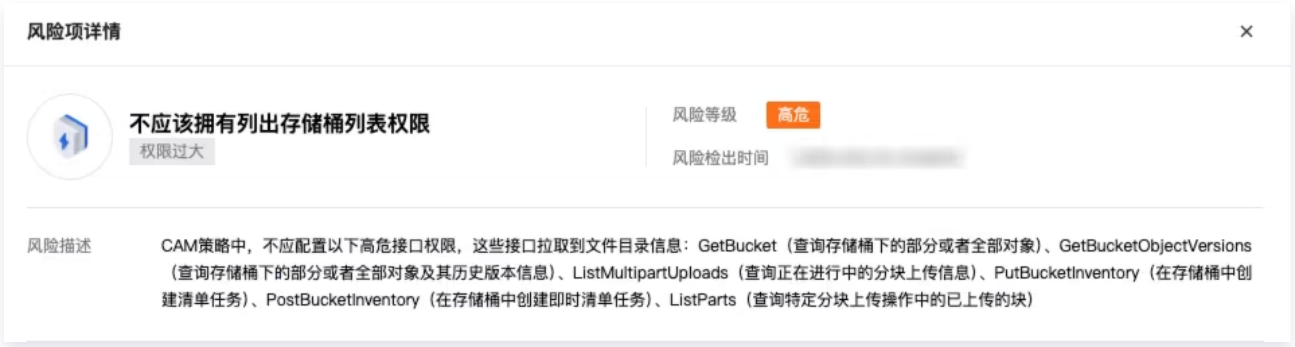
风险列表

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知** > **对象存储异常监测**。
2. 在对象存储异常监测页面，单击**风险**。
3. 在**风险** > **风险项视角**中，基于风险项视角自动化扫描存储桶权限配置，识别存在风险的存储桶，并展示风险检出时间以及风险等级。

风险项详情

1. 在**风险** > **风险项视角**中，选择所需资产，单击**详情**。

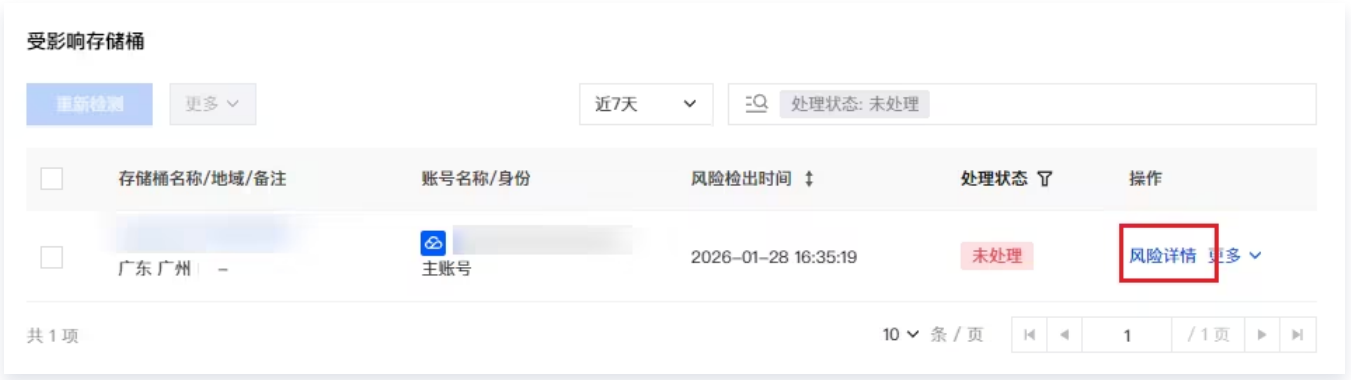
2. 在**风险项详情**页面，查看风险项基本信息、受影响存储桶以及配置建议。
   - 查看风险项基本信息。



   - 查看受影响存储桶列表，默认显示未处理风险的存储桶。

风险详情

1. 在**风险项详情 > 受影响存储桶**页面，选择所需账号，单击**风险详情**。



2. 在**风险详情**页面，查看风险基本信息、风险证据以及描述、风险相关接口调用情况以及配置建议。
   - 查看风险基本信息，风险基本信息包括：受影响存储桶名称、存储桶地域、存储桶备注、标签、账号名称、APPID。

   - 查看风险描述与证据，该风险详情的证据包括：权限来源/内容、策略 ID /授权策略名称、授权资源、授权操作。

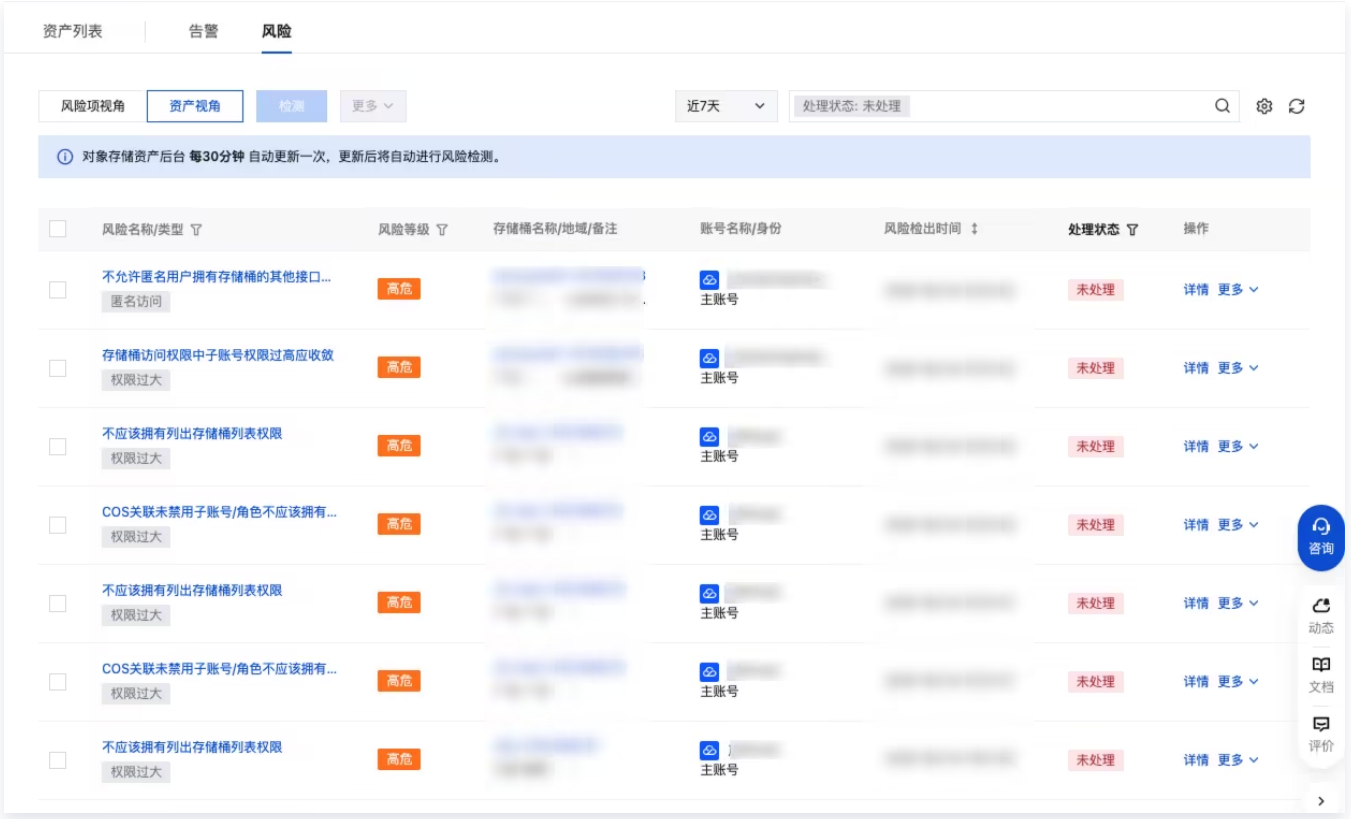
   - 查看风险相关接口调用情况以及配置建议。

资产视角

从资产视角聚焦单存储资产所触发的所有风险项、及处置状态，实现对单资产风险的处置跟踪，精准评估风险对资产安全的影响，支撑资产安全的持续保障。

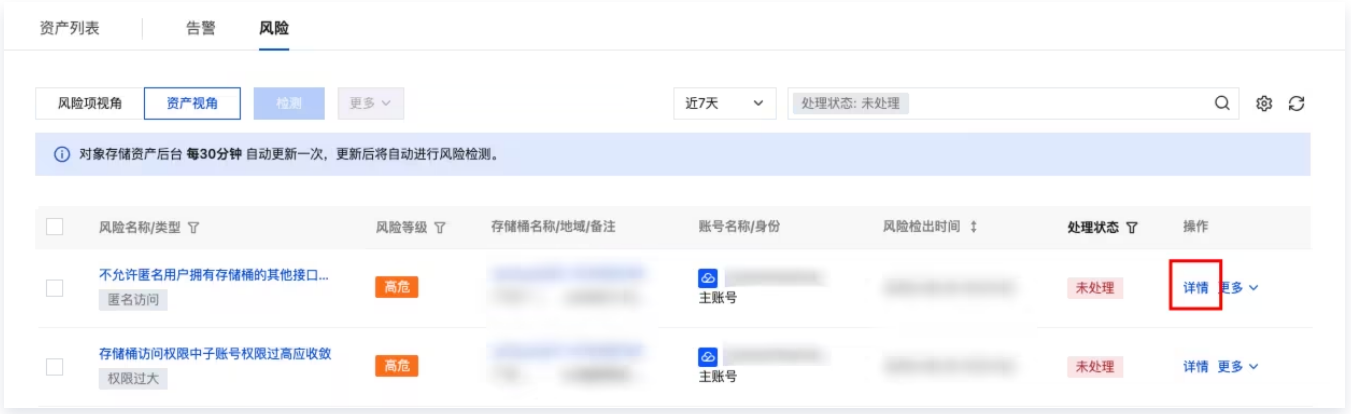
风险列表

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，单击**风险**。
3. 在**风险 > 资产视角**中，基于资产视角自动化扫描 AK 权限配置， 识别存在风险的存储桶，并清晰列出每项风险对应的受影响账号。



风险详情

1. 在**风险 > 资产视角**页面，选择所需风险名称，单击**详情**。



2. 在**风险详情**页面，查看风险基本信息、风险证据以及描述、风险相关接口调用情况以及配置建议。
   - 查看风险基本信息，风险基本信息包括：受影响存储桶名称、存储桶地域、存储桶备注、标签、账号名称、APPID。

- 查看风险描述与证据，该风险详情的证据包括：权限来源/内容、策略 ID/授权策略名称、授权资源、授权操作。

- 查看风险相关接口调用情况以及配置建议。

风险处置

标记忽略

1. 在**风险 > 资产视角**，支持单个或者批量处理目标风险：
   - **单个处置：**单击目标风险操作列中的**更多 > 标记忽略**。

   - **批量处置：**在风险页面，选择多个目标风险，单击**更多 > 标记忽略**。

2. 在二次确认中，单击**确定**，即可将该风险标记为已忽略。

策略管理

最近更新时间：2026-01-29 14:57:01

告警策略

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，单击右上角**策略管理**。
3. 在策略管理窗口中，单击**告警策略**标签。对告警策略进行管理，目前支持开启/关闭具体的告警策略以及添加告警策略、快速定位命中策略的告警。

4. 在告警策略标签页面，单击**添加策略**。
5. 在添加策略窗口，按需配置相关参数，配置完成后，单击**保存**即可。

内容名称	说明	示例
生效调用源 IP	• 支持选择全部源 IP，或按账号内外、局域网等类型筛选，也支持手动输入 IP 或网段； • 多个 IP 或类型需换行输入，最多150行； • 若输入重复 IP，后台将自动合并； • 未选择时默认对全部调用 IP 生效。	1.x.x.1 x.x.x.x/24
调用 UA	• 支持选择全部调用 UA，或自定义调用 UA； • 多个 UA 需换行输入，最多20行； • 若输入重复 UA，后台将自动合并； • 未选择时默认对全部调用 UA 生效。	cos-xx-xx-v5.3.0 custom-xx
生效 AK	• 可选全部 AK，或从现有 AK、长期密钥、临时密钥、匿名访问中选择，也支持手动输入 AK； • 多个 AK 需换行输入，最多150行； • 若输入重复 AK，后台将自动合并； • 未选择时默认对全部 AK 生效。	AK1 AK2
生效域名	• 可选全部域名，或自定义域名； • 多个域名需换行输入，最多150行； • 若输入重复域名，后台将自动合并； • 未选择时默认对全部域名生效。	example0.com example1.com
生效存储桶	• 可选全部存储桶，或从现有存储桶中选择； • 未选择时默认对全部存储桶生效。	-
生效文件路径	• 可选全部文件路径，或自定义文件路径； • 多个文件路径需换行输入，最多150行； • 若输入重复文件路径，后台将自动合并； • 未选择时默认对全部文件路径生效。	bucket1/logs/ydeyes.yaml
生效接口	• 可选全部接口，或手动选择指定接口； • 未选择时默认对所有接口生效。	-
返回码	• 选全部返回码，或仅选择成功、失败的返回码。 • 未选择时默认对所有返回码生效。	-

白名单策略

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，单击右上角**策略管理**。
3. 在策略管理窗口中，单击**白名单策略**标签。对白名单策略进行管理，支持基于调用源 IP、调用 UA、域名、存储桶、文件路径、AK、接口、返回码进行加白，并指定生效范围。

4. 在白名单策略标签页面，单击**添加策略**。
5. 在添加策略窗口，按需配置相关参数，配置完成后，单击**保存**即可。

内容名称	说明	示例
生效调用源 IP	• 支持选择全部源 IP，或按账号内外、局域网等类型筛选，也支持手动输入 IP 或网段； • 多个 IP 或类型需换行输入，最多150行； • 若输入重复 IP，后台将自动合并； • 未选择时默认对全部调用 IP 生效。	1.x.x.1 x.x.x.x/24
调用 UA	• 支持选择全部调用 UA，或自定义调用 UA； • 多个 UA 需换行输入，最多20行； • 若输入重复 UA，后台将自动合并； • 未选择时默认对全部调用 UA 生效。	cos-xx-xx-v5.3.0 custom-xx
生效 AK	• 可选全部 AK，或从现有 AK、长期密钥、临时密钥、匿名访问中选择，也支持手动输入 AK； • 多个 AK 需换行输入，最多150行； • 若输入重复 AK，后台将自动合并； • 未选择时默认对全部 AK 生效。	AK1 AK2

生效域名	• 可选全部域名，或自定义域名； • 多个域名需换行输入，最多150行； • 若输入重复域名，后台将自动合并； • 未选择时默认对全部域名生效。	example0.com example1.com
生效存储桶	• 可选全部存储桶，或从现有存储桶中选择； • 未选择时默认对全部存储桶生效。	-
生效文件路径	• 可选全部文件路径，或自定义文件路径； • 多个文件路径需换行输入，最多150行； • 若输入重复文件路径，后台将自动合并； • 未选择时默认对全部文件路径生效。	bucket1/logs/ydeyes.yaml
生效接口	• 可选全部接口，或手动选择指定接口； • 未选择时默认对所有接口生效。	-
返回码	• 选全部返回码，或仅选择成功、失败的返回码。 • 未选择时默认对所有返回码生效。	-

IP 隐藏策略

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，单击右上角**策略管理**。
3. 在策略管理窗口中，单击 **IP 隐藏策略**标签。在此可配置IP隐藏规则，生效后，指定 IP 将不再出现在调用源 IP 列表中。

4. 在 IP 隐藏策略标签页面，单击**添加策略**。

5. 在添加策略窗口，按需配置相关参数，配置完成后，单击**保存**即可。

内容名称	说明	示例
生效调用源 IP	• 支持选择全部源 IP，或按账号内外、局域网等类型筛选，也支持手动输入 IP 或网段； • 多个 IP 或类型需换行输入，最多150行； • 若输入重复 IP，后台将自动合并； • 未选择时默认对全部调用 IP 生效。	1.x.x.1 x.x.x.x/24
生效 AK	• 可选全部 AK，或从现有 AK、长期密钥、临时密钥、匿名访问中选择，也支持手动输入 AK； • 多个 AK 需换行输入，最多150行； • 若输入重复 AK，后台将自动合并； • 未选择时默认对全部 AK 生效。	AK1 AK2
生效存储桶	• 可选全部存储桶，或从现有存储桶中选择； • 未选择时默认对全部存储桶生效。	–

说明：

- IP 隐藏策略配置后，策略内容的 IP 将被隐藏， 不再显示在调用源 IP 列表中，策略删除后对应 IP 将恢复显示。
- 历史调用记录命中 IP 隐藏策略后，将全部被隐藏。
- 策略配置后预计 10 分钟左右生效。

数据库风险监测
功能简介

最近更新时间：2026-01-26 17:41:22

数据库风险监测专注于数据库风险监测与数据安全治理，通过资产梳理、风险识别、行为分析、权限管控、操作审计的全链路能力，帮助企业实现云上数据库的 “看得见、管得住、防得准”，有效防范数据泄露风险，保障业务持续稳定运行。

前提条件

已购买 数据安全态势管理（数据库风险异常监测）。

功能点梳理

模块名称	核心定位	实践价值	操作指引
统计面板	聚合核心安全指标，提供全局安全态势视图，支撑快速决策与优先级排序。	解决“多模块分散查询效率低、安全态势不直观”等问题。	统计面板
数据资产	数据库风险监测的基石，实现资产从录入到防护的闭环管理，确保“资产清晰”“权责明确”“数据安全”。	解决“资产不清、权责不明、敏感数据失控”痛点，确保每台资产有人管、每份敏感数据有防护，支撑资产盘点与合规治理。	数据资产
访问管理	数据库访问双向管控体系，从双视角实现访问行为治理，管理异常访问入口。	解决“访问控制粗放、异常访问难追溯”等问题，实现“谁能访问、从哪访问、安全管控”的精细化治理，守住安全第一道防线。	访问管理
告警模块	安全事件实时监测与响应体系，实现违规行为精准识别与闭环处理。	解决“安全事件发现不及时、处理无闭环”等问题，将事件响应时间从小时级压缩至分钟级。	告警
风险模块	实现风险前置治理，降低安全事件发生概率，从被动应对转向主动防御。	解决数据安全风险隐患等问题，降低安全事件发生概率，实现风险前置治理。	风险
审计日志	数据库操作行为全量记录，为数据库安全事件的溯源提供支持。	解决“操作无记录、事件溯源难”等问题，有效还原数据库安全信息。	审计日志

统计面板

最近更新时间：2026-01-26 17:32:12

数据库风险监测统计面板模块，将展示数据库资产安全全局态势，包括资产概览、安全概览、待处理风险统计及趋势变化，可通过此模块快速掌握核心安全状态。

操作步骤

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，将显示当前资产概览、安全概览、告警趋势、风险趋势，您可以通过统计面板了解当前资产安全态势。
   - **资产数：**统计当前已进行同步的数据库资产数量和不同安全建议的数据库资产数量。

安全建议	建议说明
立即处理	该数据库资产存在异常行为告警，请立即关注并处理。
立即加固	该数据库资产存在风险，建议进行关注并收敛权限，完成加固。

   - **待处理告警：**统计近七天数据安全资产待处理告警数；
   - **待处理风险：**统计近七天数据安全资产待处理风险数；
   - **告警趋势图：**统计**近七天数据资产安全告警数的变化趋势；**
   - **风险趋势图：**统计**近七天数据安全资产风险数变化趋势。**
3. 单击各概览项中的**数字**，可直接跳转至对应模块的详情页面（如单击 “待处理告警数” 跳转至告警列表）。

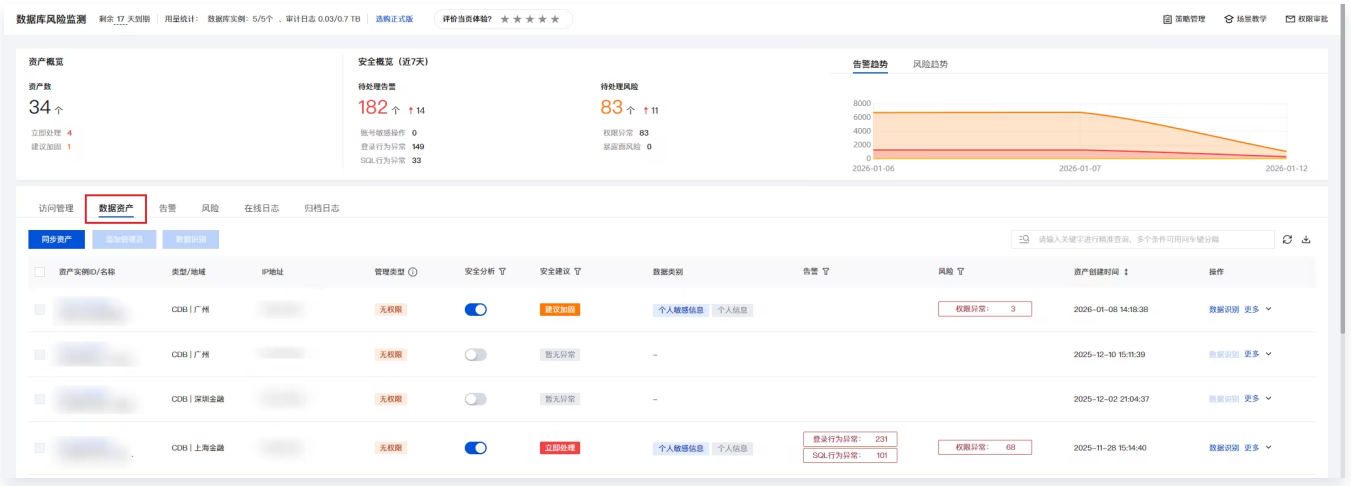
数据资产

最近更新时间：2026-01-26 17:32:12

数据库风险监测数据资产模块，从资产同步到权限分配、敏感数据识别，覆盖资产合规盘点、敏感数据专项防护、权限合规整改等核心场景。

数据资产列表

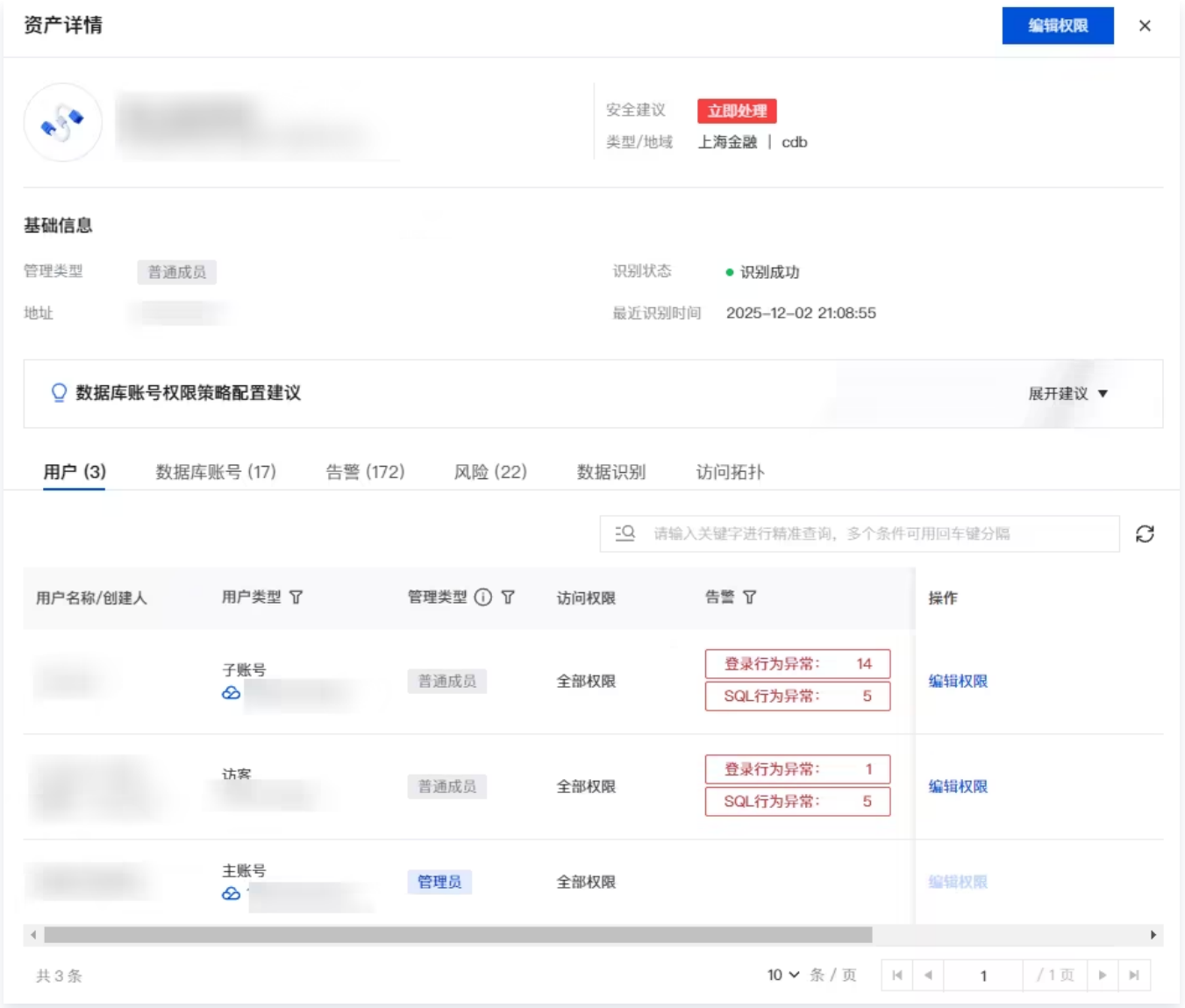
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**数据资产**标签。
3. 在数据资产标签页面，将显示已同步的数据库资产。



数据资产详情

1. 在数据资产标签页面，选择目标数据库资产，单击**资产实例 ID**。

2. 在资产详情页面，将会显示当前数据库资产基础信息、用户信息、数据库账号信息、告警信息、风险信息、敏感数据识别详情、访问拓扑。



同步数据资产

在数据资产标签页，单击**同步资产**，即可同步当前账号下的数据库资产。

开启安全监测

1. 在数据资产标签页中，选择目标数据库资产，单击**安全分析**列的**开关**，开启数据安全监测。

2. 开启后，系统将实时监测该资产的安全状态（如访问、违规操作）。

敏感数据识别

对敏感数据进行差异化防护，提升防护精准度。

1. 在数据资产标签页中，选择目标数据库资产，单击操作列中的**数据识别**。

2. 在数据识别配置窗口中，可选择立即识别，或选择周期识别，配置完成后，单击**确定**。
3. 识别成功后将自动刷新数据库资产库表详情，同时新增数据资产内容标签。

访问管理

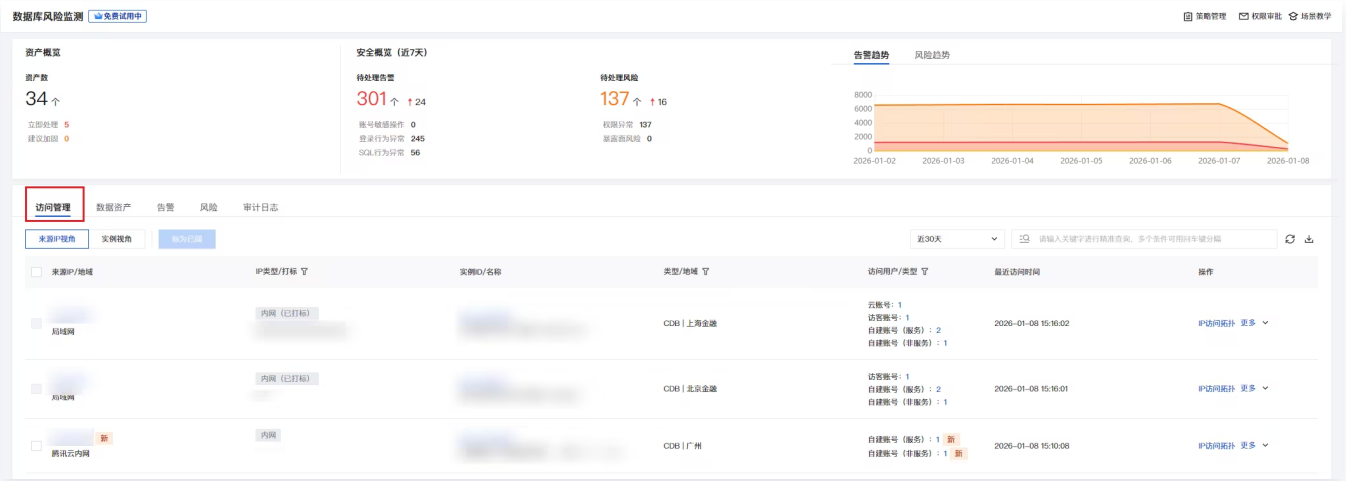
最近更新时间：2026-01-26 17:32:12

数据库风险监测访问管理模块，通过 “来源 IP 视角” 与 “实例视角” 的双维度互补治理，实现对数据库访问行为的精细化管控。支持访问行为的可视化展示（如访问拓扑图）、IP / 账号打标操作，实现精细化访问控制。从 “来源 IP” 和 “实例” 双维度管控访问行为，解决 “谁能访问、从哪访问、访问什么” 的核心问题，避免粗放式访问控制导致的安全漏洞。

管控视角	描述	适用场景
来源 IP 视角	以访问发起端的来源 IP 为核心管控维度，整合该 IP 对数据库实例的访问数据，提供访问拓扑可视化、IP / 账号精准打标及安全组策略快速调整能力，实现对访问发起端的集中精细化管控。	排查单一 IP 的跨实例访问风险、批量标记某类访问端。
实例视角	以访问目标端的数据库实例为核心资源维度，整合来源 IP 对该实例的访问数据，提供资产访问拓扑可视化、IP / 账号精准打标及安全组策略快速调整能力，实现对访问目标端的集中精细化管控。	梳理单一实例的全量访问来源、针对核心实例做专项管控。

来源 IP 视角

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**访问管理 > 来源 IP 视角**标签。
3. 在来源 IP 视角标签页面，可以查看来源 IP / 地域、IP 类型 / 打标、实例 ID / 名称、数据库类型 / 地域、访问用户 / 类型、最近访问时间等信息。



IP 访问拓扑

以可视化图谱的形式，直观展示单个来源 IP 与所有关联账号、数据库实例之间的访问关系、访问频率及安全状态。在来源 IP 视角列表，单击目标 IP 对应操作列的 **IP 访问拓扑**，可查看该 IP 与关联数据库实例的访问关系图谱。

IP 打标

为目标来源 IP 添加预设或自定义标签，实现对 IP 的分类管控，便于后续风险监测时进行差异化判定。

1. 在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 来源 IP 打标**。

2. 在来源 IP 打标窗口，编辑来源 IP 备注，单击**确定**完成标记。

> **说明：**
> 来源 IP 视角和实例视角的打标操作是相互联动的，在来源 IP 视角为某 IP 打标后，在实例视角查看该 IP 时，打标状态会同步更新；反之亦然。

账号打标

为目标来源 IP 访问数据库时使用的账号添加预设或自定义标签，实现对访问账号的分类管控，便于后续审计和风险排查。

1. 在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 账号打标**。

2. 在账号打标窗口，选择账号类型，编辑账号备注信息，单击**确定**完成标记。

> **说明：**
> 可以编辑类型为“自建账号”的访问账号类型，若当前访问账号为云主账号/子账号，系统将自动识别，无需手动编辑。

修改安全组策略

快速跳转至目标 IP 关联的数据库实例资产页面，直接修改安全组策略，实现对该 IP 访问权限的快速管控（允许 / 拒绝访问）。
在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 修改安全组策略**，可前往数据库实例资产页面修改安全组策略。

实例视角

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**访问管理 > 实例视角**。
3. 在实例视角页面，可查看实例 ID / 名称、数据库类型 / 地域、访问用户 / 类型、来源 IP / 类型、最近访问时间等信息。

资产访问拓扑

以可视化图谱的形式，直观展示单个数据库实例的所有访问来源 IP、关联访问账号之间的访问关系、访问频率及风险状态。
在实例视角列表，单击目标实例对应操作列的**资产访问拓扑**，可查看该实例的所有访问来源 IP、关联账号的拓扑关系。

IP打标

为访问目标实例的指定来源 IP 添加预设或自定义标签，实现对该实例访问 IP 的精准分类管控，便于后续风险监测和审计。
1. 在实例视角列表，单击目标实例对应操作列的**更多 > 来源 IP 打标**。

2. 在来源 IP 打标窗口，编辑来源 IP 备注，单击**确定**完成标记。

> **说明：**
> 来源 IP 视角和实例视角的打标操作是相互联动的，在来源 IP 视角为某 IP 打标后，在实例视角查看该 IP 时，打标状态会同步更新；反之亦然。

账号打标

为访问目标实例的指定账号添加预设或自定义标签，实现对该实例访问账号的精准分类管控，便于后续风险排查和权限审计。

1. 在实例视角列表，单击目标实例对应操作列的**更多** > **账号打标**。

2. 在账号打标窗口，选择账号类型，编辑账号备注信息，单击**确定**完成标记。

> **说明：**
> 可以编辑类型为“自建账号”的访问账号类型，若当前访问账号为云主账号/子账号，系统将自动识别，无需手动编辑。

修改安全组策略

快速跳转至目标数据库实例的资产页面，直接修改安全组策略，实现对该实例所有访问来源 IP 的管控。

在实例视角列表，单击目标实例对应操作列的**更多** > **修改安全组策略**，可前往数据库实例资产页面修改安全组策略。

告警

最近更新时间：2026-01-26 17:32:12

数据库风险监测告警模块，通过对数据库资产的安全事件实时监测与响应体系，实现违规行为精准识别与闭环处理。

告警列表

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知** > **数据库风险监测**。
2. 在数据库风险监测页面，单击**告警**标签。
3. 在告警标签页面，您可查看当前数据库资产的相关告警信息。告警列表将展示告警名称/类型、告警等级、资产实例ID /名称、数据库账号、所属用户/类型、告警检出时间、处理状态；

查看告警详情

在告警标签页面，单击目标告警操作列的**详情**，查看告警触发原因、违规操作详情（SQL 语句、来源 IP）、关联资产等信息。

告警处理操作

标记忽略

对误报或无需处理的告警进行状态标记，排除风险统计干扰。

> **说明：**
> 告警处理状态标记为已忽略，则该风险将不会纳入风险统计中。

1. 在告警标签页面，支持单个或者批量处理目标告警：
   - **单个处置：**单击目标告警操作列的**更多 > 标记忽略**。

   - **批量处置：**选择多个目标告警，单击**标记忽略**。

2. 在二次确认中，单击**确定**，即可将告警标记为已忽略。

添加白名单

对于需要长期放行的行为，可以将该告警所触发的策略添加至规则白名单中。

1. 在告警标签页面，单击目标告警操作列的**更多** > **添加白名单**。

2. 在添加白名单窗口中，查看白名单策略内容，确认无误后单击**确定**，即可将该告警所触发的策略信息添加至白名单。

> **说明：**
> 告警白名单策略规则生效后，该行为不再触发告警；

标记已处理

对已完成应急响应的告警进行状态更新，实现处置闭环。

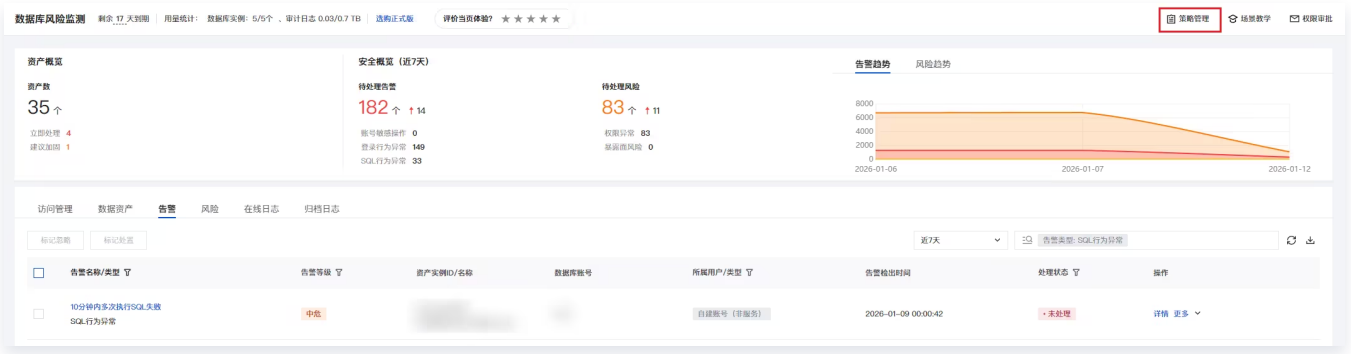
1. 在告警标签页面，选择单个或多个目标告警，单击**标记处置**。

2. 在确认窗口中，核查告警信息，确认无误后，单击**确定**，即可将该告警标记为已处理。

> **说明：**
> 告警处理状态标记已处理后，该告警将不会纳入风险统计中。

告警策略配置

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击右上角**策略管理**。



3. 在策略管理窗口中，单击**告警策略**标签。
4. 在告警策略标签页面中，将显示所有内置的预设告警策略。您可以在该标签页面中对告警策略进行开启/关闭、调整策略等级、修改策略内容等操作。

开启/关闭告警策略

在告警策略标签页面，选择目标告警策略，单击策略开关列的**开关**，开启或关闭告警策略。

编辑告警策略

1. 在告警策略标签页面，选择目标告警策略，单击操作列的**编辑**。

2. 在编辑策略窗口，可以对策略等级、策略内容（非服务账号）进行修改。

告警白名单管理

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击右上角**策略管理**。
3. 在策略管理窗口中，单击**告警白名单策略**标签。

4. 在告警白名单策略标签页面，将显示所有已添加的告警白名单策略
5. 在告警白名单策略标签页面，可定期查看白名单列表，单击 “编辑” 修改规则，或 “删除” 过期 / 无效规则。

风险

最近更新时间：2026-01-26 17:32:12

数据库风险监测模块，聚焦未触发风险但存在长期安全隐患的行为。覆盖权限合规整改、暴露面安全加固、账号安全优化等核心场景，降低安全事件发生概率。

策略名称	策略内容	处置操作建议
操作权限范围过大	基于账号近 7 天使用权限计算权限使用率（使用权限/授权权限），当小于配置的比例时，触发风险	• 风险忽略 • 风险加白 • 一键处置
绕过 DSPM 修改账号权限	当前检测到账号的权限与 DSPM 设置的权限不一致时，触发风险	一键处置
未管控账号	数据库自建的账号，且未设置为服务账号	一键处置
绕过 DSPM 删除账号	当检测到绕过 DSPM 删除账号时，触发风险	一键处置
暴露公网访问入口	数据库实例启用公网地址时，触发风险	一键处置

风险列表

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**风险**标签。

3. 在风险页面，将展示已触发风险策略的数据安全风险，包括风险名称/类型、风险等级、资产实例 ID/名称、数据库账号、所属用户/类型、风险检出时间、处理状态等信息。

风险详情

在风险页面，选择目标风险，单击操作列的**详情**，查看风险详情。

风险处置

标记忽略

对**操作权限范围过大的风险项**进行状态标记，排除风险统计干扰。

> **说明：**
> 风险处理状态标记为已忽略，则该风险将不会纳入风险统计中。

1. 在风险标签页面，支持单个或者批量处理目标风险：
   - **单个处置：**单击风险名称为**操作权限范围过大**的风险操作列中的**更多 > 标记忽略**。

   - **批量处置：**在风险页面，选择风险名称为**操作权限范围过大**的风险，单击**标记忽略**。

2. 在二次确认中，单击**确定**，即可将该风险标记为已忽略。

添加白名单

1. 在风险标签页面，单击风险名称为**操作权限范围过大**的风险操作列中的**更多 > 添加白名单**。

2. 在添加白名单窗口中，查看白名单策略内容，确认无误后单击**确定**，即可将该风险所触发的策略信息添加至白名单。

> **说明：**

> 风险白名单策略规则生效后，该行为不再触发风险；

标记已处置

对已完成应急响应的风险进行状态更新，实现处置闭环。

1. 在风险标签页面，选择单个或多个目标风险，单击**标记处置**。

2. 在确认窗口中，核查风险信息，确认无误后，单击**确定**，即可将该风险标记为已处理。

> **说明：**
> 风险处理状态标记已处理后，该风险将不会纳入风险统计中。

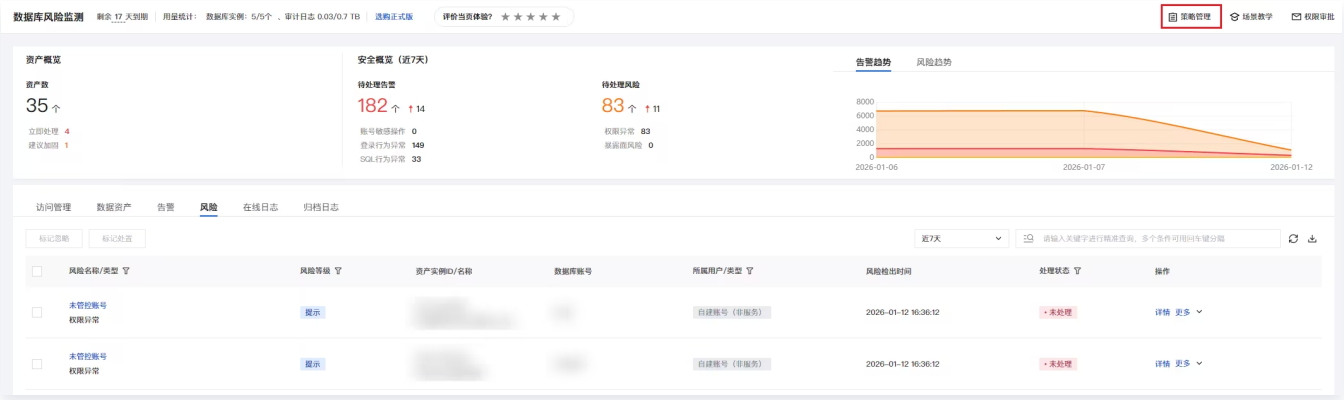
一键处置

针对不同的风险项，可以通过一键处置进行风险的处置操作。

在风险标签页面，选择目标风险，单击操作列中的**更多 > 一键处置**。可通过系统预设的处置操作进行风险处置。

风险策略配置

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击右上角**策略管理**。



3. 在策略管理窗口中，单击**风险策略**标签。

4. 在风险策略标签页面中，将显示所有内置的预设风险策略。您可以在该标签页面中对风险策略进行开启/关闭、调整策略等级、修改策略内容等操作。

开启/关闭风险策略

在风险策略标签页面，选择目标风险策略，单击策略开关列中的**开关**，开启或关闭风险策略。

编辑风险策略

1. 在风险策略标签页面，选择目标风险策略，单击操作列中的**编辑**。

2. 在编辑策略窗口，可以对策略等级、策略内容（非服务账号）进行修改。

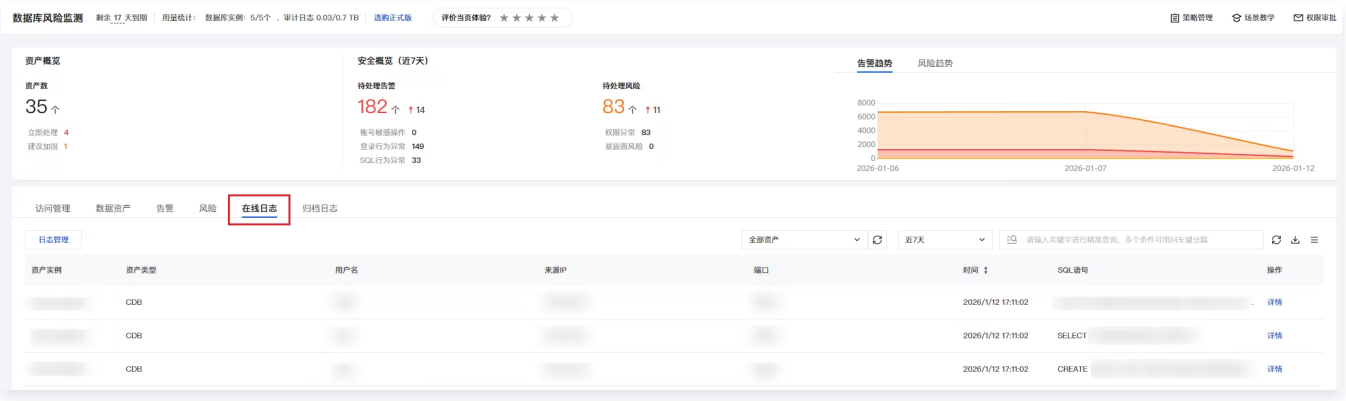
审计日志

最近更新时间：2026-01-26 17:32:12

数据库风险监测审计日志模块，全面记录数据库操作全量行为，包含 SQL 语句、操作人员、来源 IP、时间戳等关键溯源信息，支持多维度精准检索与详情查看，为数据库操作行为提供全程可追溯能力。

在线日志

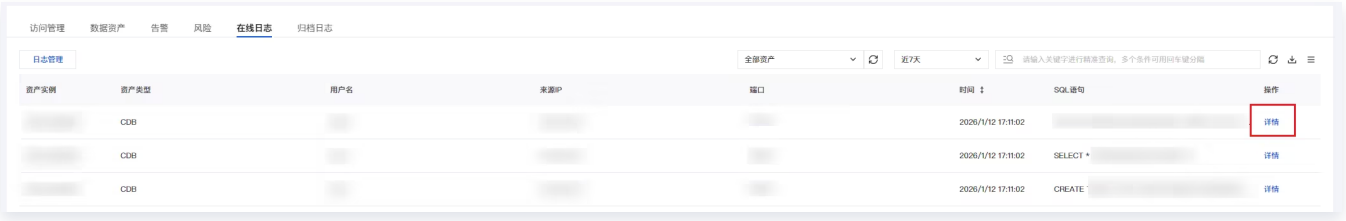
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**在线日志**标签。
3. 在在线日志页面中，显示已同步数据库资产的操作记录。



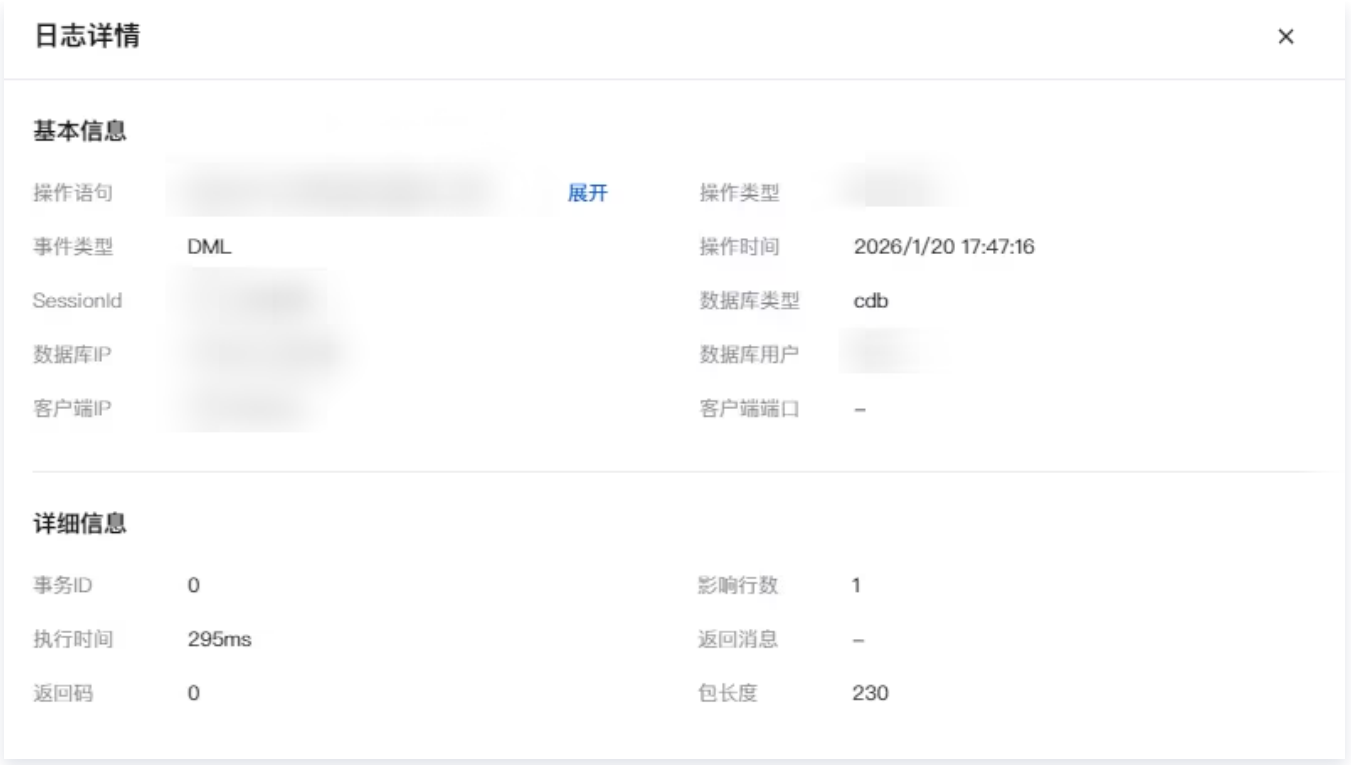
4. 在在线日志页面中，可通过资产实例、时间范围、用户名、来源 IP、端口和 SQL 语句进行日志检索。

在线日志详情

1. 在审计日志标签页面中，单击目标日志操作列的**详情**。

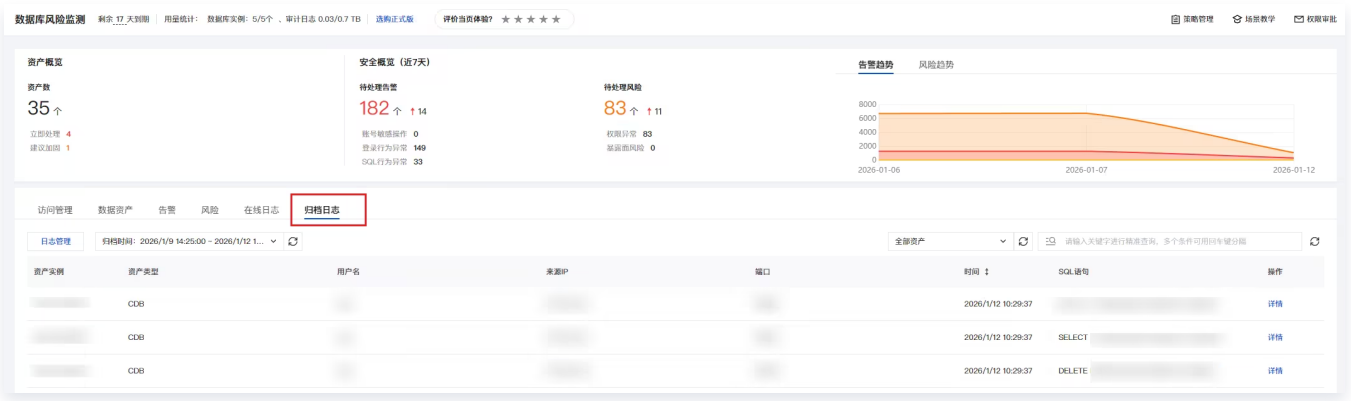


2. 在日志详情页，您可查看完整操作信息：操作语句、操作类型、事件类型、操作时间、数据库类型、数据库 IP、数据库用户、客户端 IP、客户端端口、返回消息、执行时间、返回码等信息。



归档日志

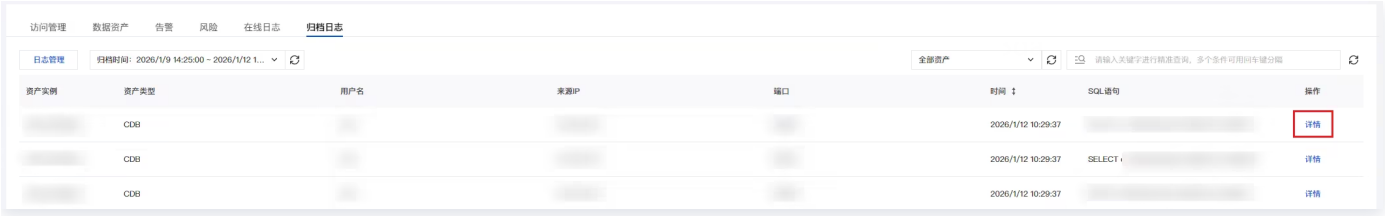
1. 登录 **云安全中心控制台**，在左侧导览中，单击**数据安全态势感知 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**归档日志**标签。
3. 在归档日志页面中，显示已归档的审计日志。



4. 在归档日志页面中，可通过资产实例、用户名、来源 IP、端口和 SQL 语句进行日志检索。

在线日志详情

在审计日志标签页面中，单击目标日志操作列的**详情**，查看完整操作信息：操作语句、操作类型、事件类型、操作时间、数据库 db、数据库 IP、数据库用户、客户端 IP、客户端端口、返回消息、执行时间、返回码等信息。



日志管理

日志存储设置

> **说明：**
> - 当启用日志归档后，**在线日志达到 2.4 亿条或在线日志存储时间达到 7 天时**，将自动以文件形式归档较早的日志；
> - 日志归档成功后，其对应的在线日志将删除，归档的日志需恢复后查看。

1. 在在线日志标签页面中，单击**日志管理**。
2. 在日志管理窗口，单击**日志存储设置**标签页面，可开启/关闭归档日志存储，以及对在线日志存储时间、恢复日志保留时间、日志生命周期进行调整。

归档日志管理

> **说明：**
> - 最多支持恢复 500 GB 日志；
> - 同一时间只能进行一个恢复任务；
> - 在线日志和归档日志会占用存储空间，恢复日志不占用存储空间。

1. 在归档日志标签页面中，单击**日志管理**。
2. 在日志管理窗口，单击**归档日志管理**标签页面。

3. 在归档日志管理标签页面，将显示所有已归档的审计日志，您可以对已归档的日志进行删除或恢复（恢复为在线日志）操作。

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

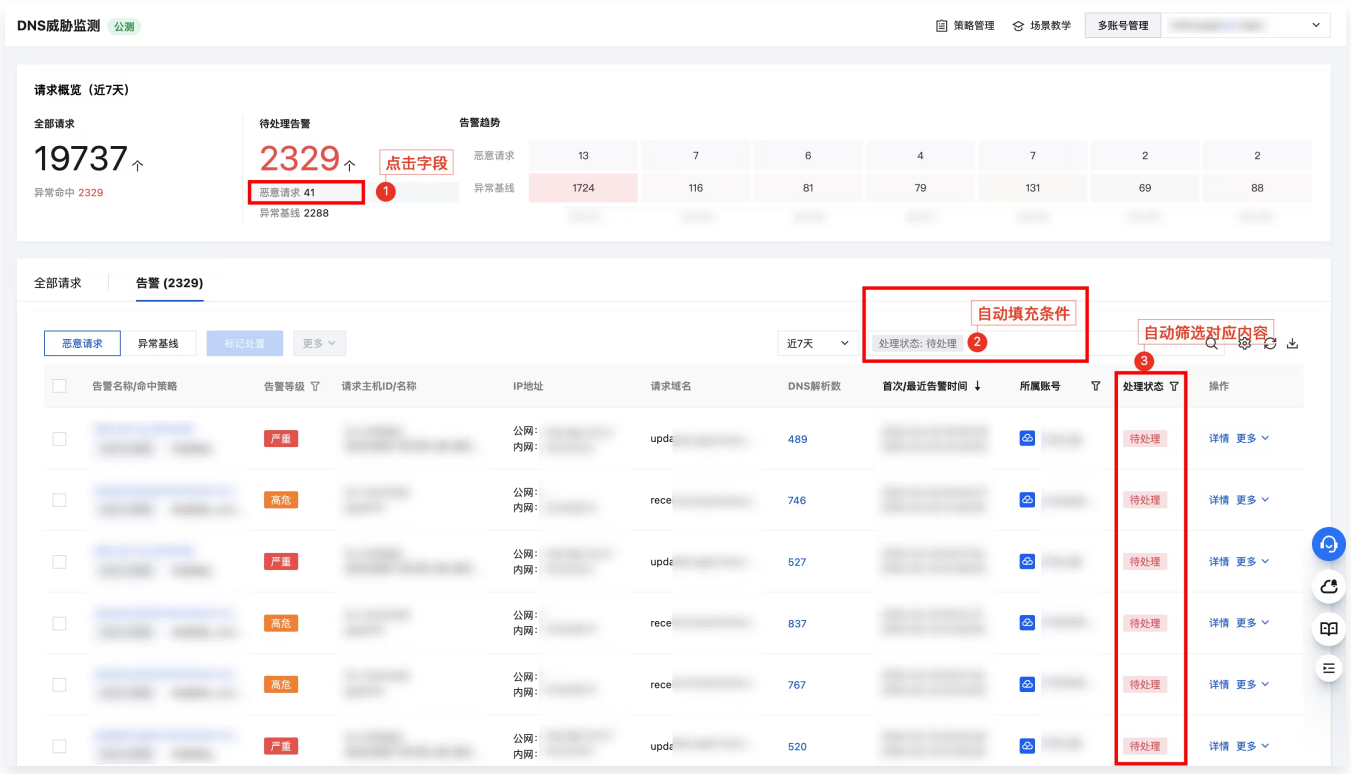
功能板块		功能点	解决问题	操作指引
统计面板-请求概览		快速了解请求情况、待处理的恶意请求与异常基线告警等。	了解请求情况与异常占比，待处理的问题有多少，近期安全运营趋势怎样。	统计面板
全部请求		查看全部域名请求情况、关联异常分析。	梳理有多少主机请求了哪些域名，是否有命中异常。 关键时期可以进行历史全量域名请求记录的回溯，协助进行溯源排查。	全部请求
告警列表	恶意请求	实时监控恶意域名请求，基于系统与自定义告警规则视角，查看告警内容、机器详细信息，并提供说明&修复方案。	识别矿池挖掘、远控木马、恶意C2、远程桌面工具等，配合主机/容器安全定位进程，引导处置	恶意请求
	异常基线	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：2025-11-28 16:17:12

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的全部请求。
   - **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**，下方列表的搜索框中自动添加条件并筛选出对应内容。



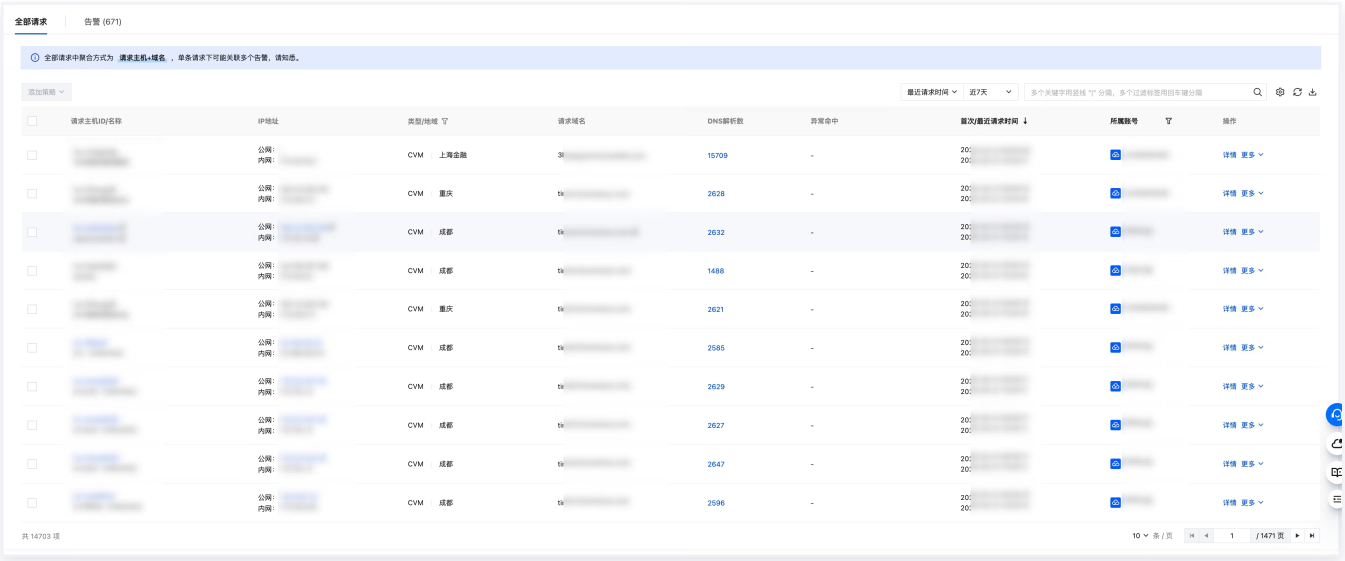
全部请求

最近更新时间：2025-12-11 14:40:12

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	请求是否有命中相关告警策略
首次/最近请求时间	2025-01-01 18:00:00	• 格式：YYYY-MM-DD HH:MM:SS

	2025-01-12 18:00:00	• 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**。

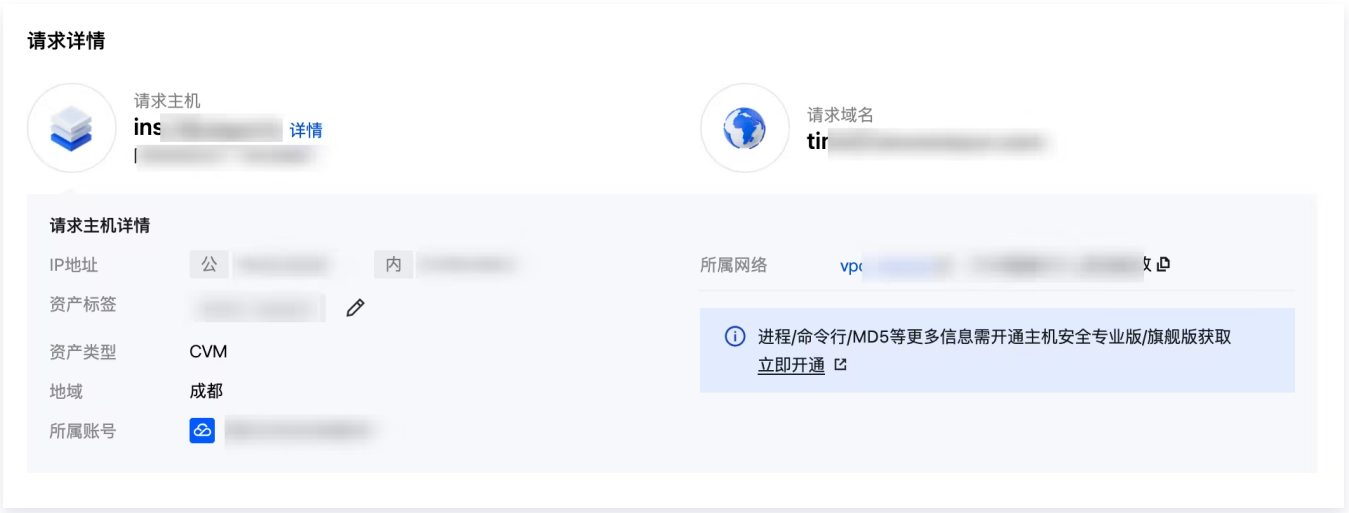
操作类型		说明
详情		单击拉起 请求详情 抽屉。
更多	添加恶意请求策略	单击打开**添加恶意请求策略**弹窗，并填充对应内容。添加后若命中该策略将产生恶意请求告警。
	加入行为基线策略	单击打开**加入行为基线策略**弹窗，并填充对应内容。加入后当发生行为基线策略范围外的请求时，产生异常基线告警。

请求详情

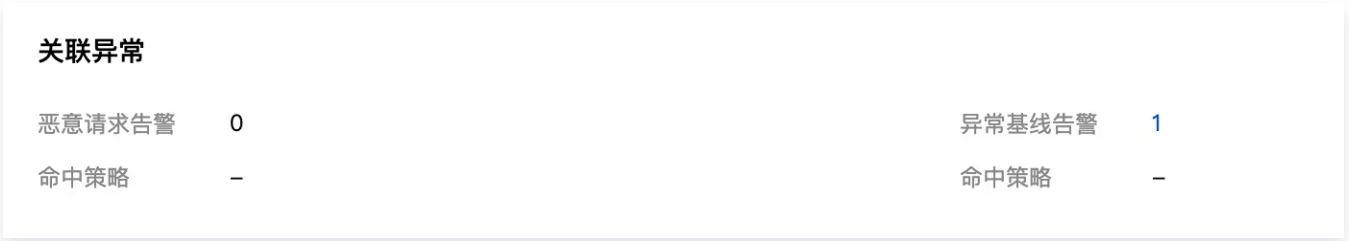
在请求详情抽屉页面，查看请求信息、请求详情与关联异常情况。

- 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。**



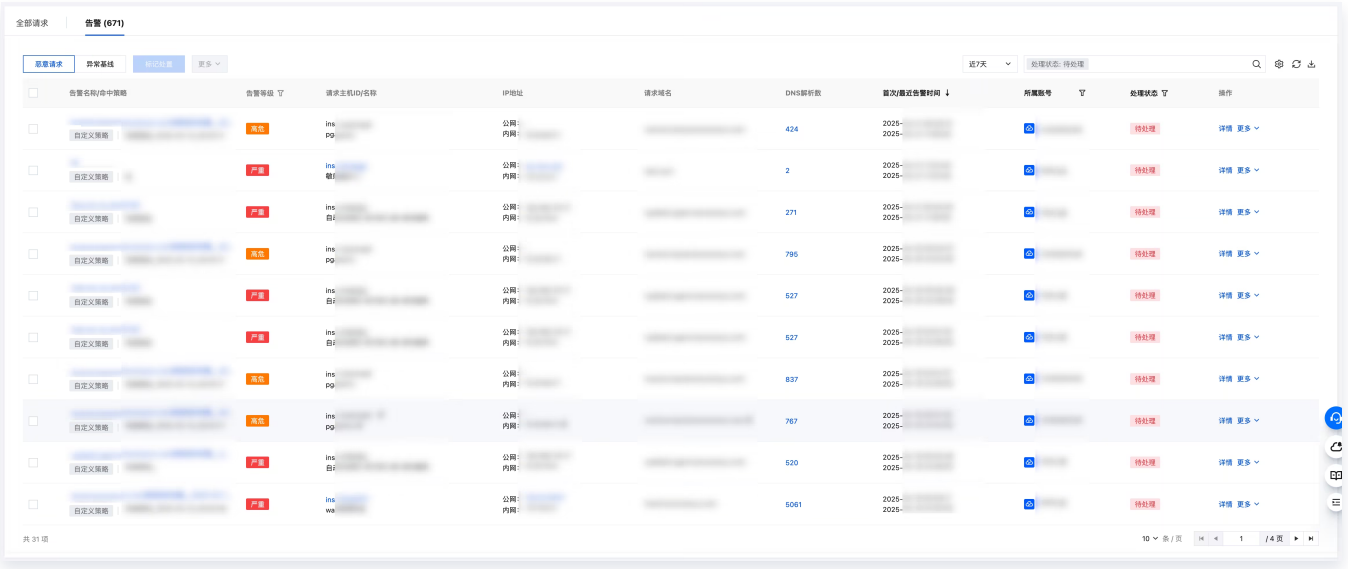
恶意请求

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**。

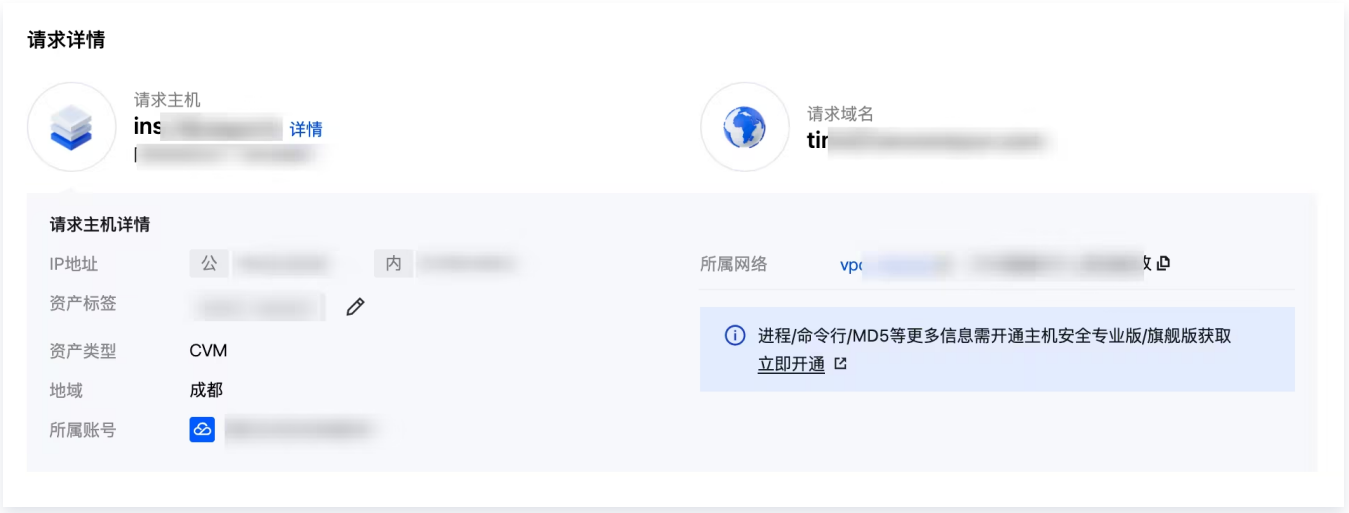
操作类型		说明
详情		单击拉起 告警详情 抽屉。
更多	标记处置	单击后处理状态变为“已处置”。
	标记忽略	单击后处理状态变为“已忽略”。
	添加白名单策略	单击拉起**添加白名单策略**抽屉，并填充对应 AK。

恶意请求详情

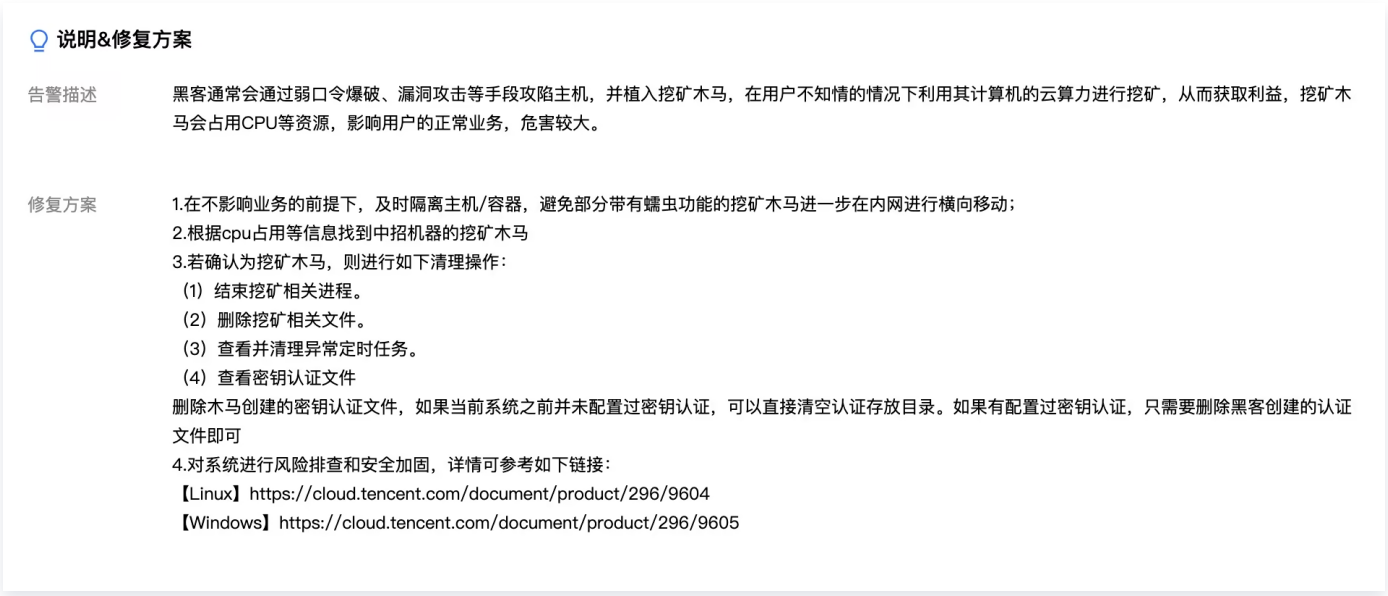
在告警详情抽屉页面，查看告警信息、请求详情与说明&修复方案。

- 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。**



说明&修复方案

告警描述	黑客通常会通过弱口令爆破、漏洞攻击等手段攻陷主机，并植入挖矿木马，在用户不知情的情况下利用其计算机的云算力进行挖矿，从而获取利益，挖矿木马会占用CPU等资源，影响用户的正常业务，危害较大。
修复方案	1.在不影响业务的前提下，及时隔离主机/容器，避免部分带有蠕虫功能的挖矿木马进一步在内网进行横向移动； 2.根据cpu占用等信息找到中招机器的挖矿木马 3.若确认为挖矿木马，则进行如下清理操作： （1）结束挖矿相关进程。 （2）删除挖矿相关文件。 （3）查看并清理异常定时任务。 （4）查看密钥认证文件 删除木马创建的密钥认证文件，如果当前系统之前并未配置过密钥认证，可以直接清空认证存放目录。如果有配置过密钥认证，只需要删除黑客创建的认证文件即可 4.对系统进行风险排查和安全加固，详情可参考如下链接： 【Linux】https://cloud.tencent.com/document/product/296/9604 【Windows】https://cloud.tencent.com/document/product/296/9605

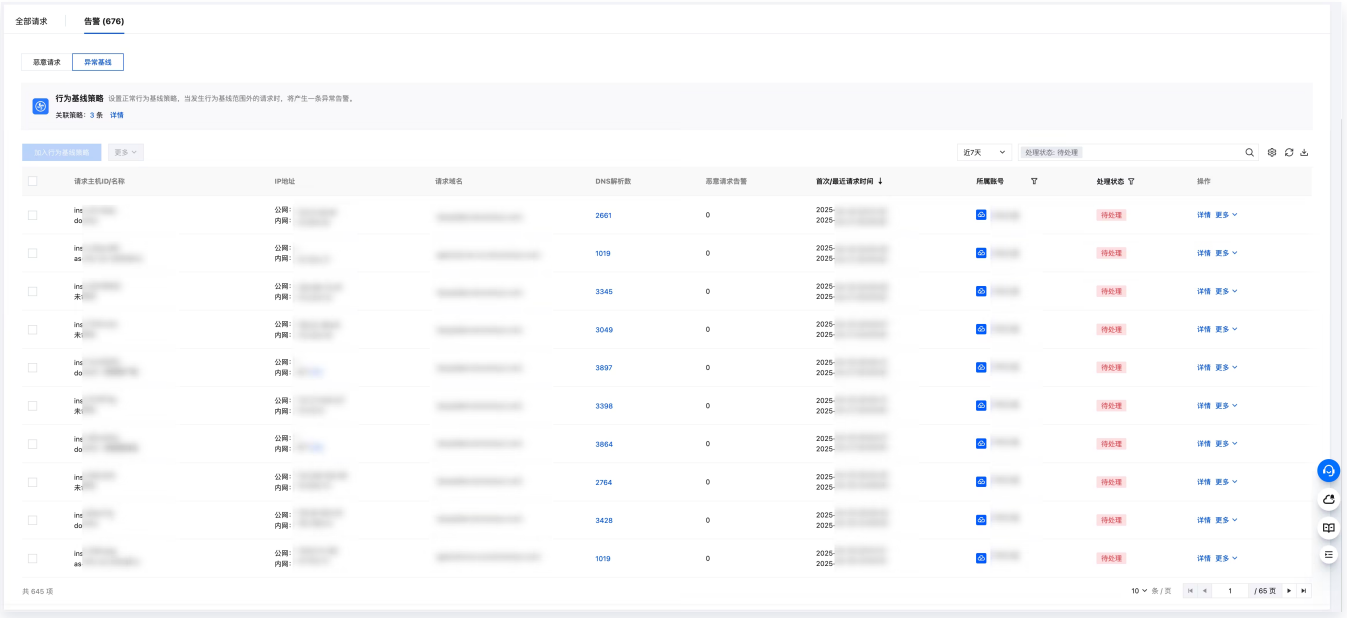
异常基线

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**。

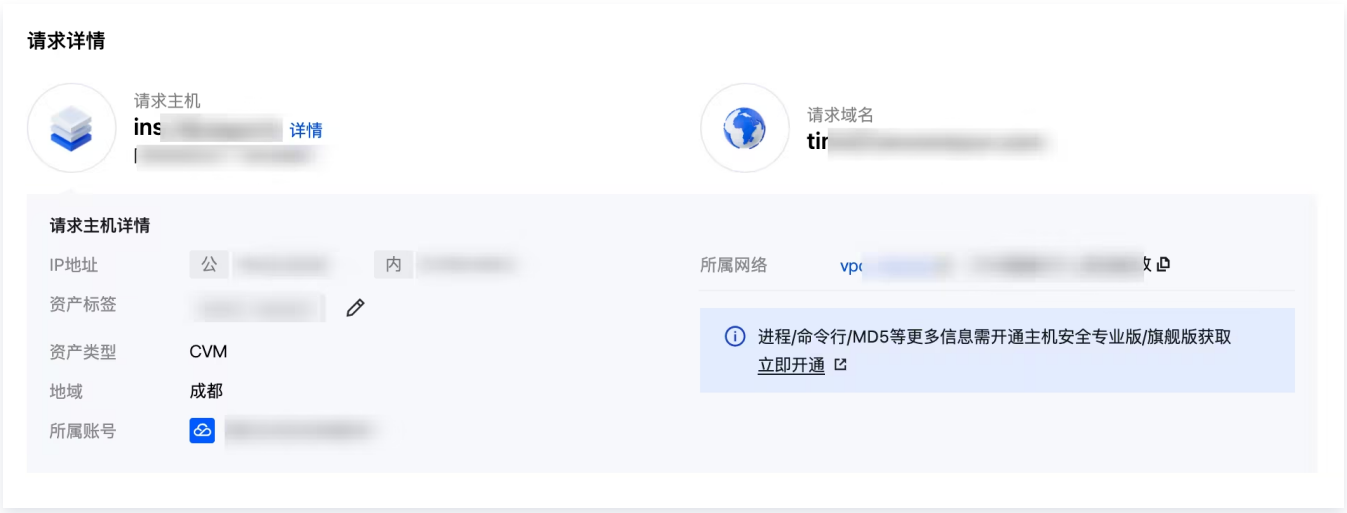
操作类型		说明
详情		单击拉起 告警详情 抽屉。
更多	加入行为基线策略	单击打开**加入行为基线策略**弹窗，并填充对应内容。加入后当发生行为基线策略范围外的请求时，产生异常基线告警。
	标记处置	单击后处理状态变为“已处置”。
	标记忽略	单击后处理状态变为“已忽略”。
	创建告警策略	单击拉起**添加策略-恶意请求**抽屉，并填充生效主机、生效域名。添加后若命中该策略将产生恶意请求告警。

异常基线详情

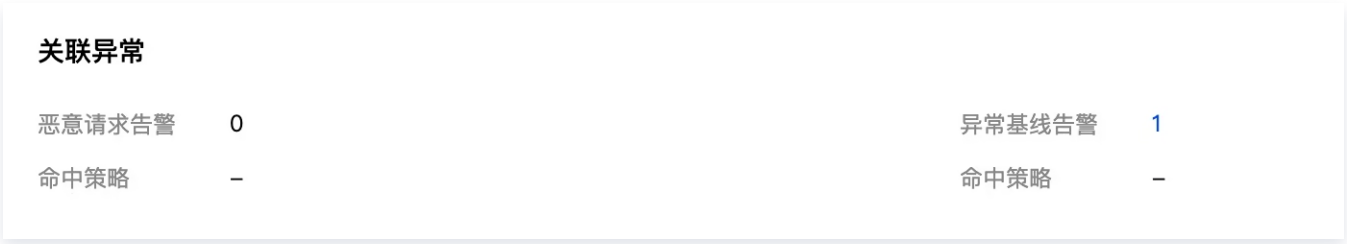
在请求详情抽屉页面，查看请求信息、请求详情与关联异常情况。

- 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：2025-08-26 18:08:52

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。

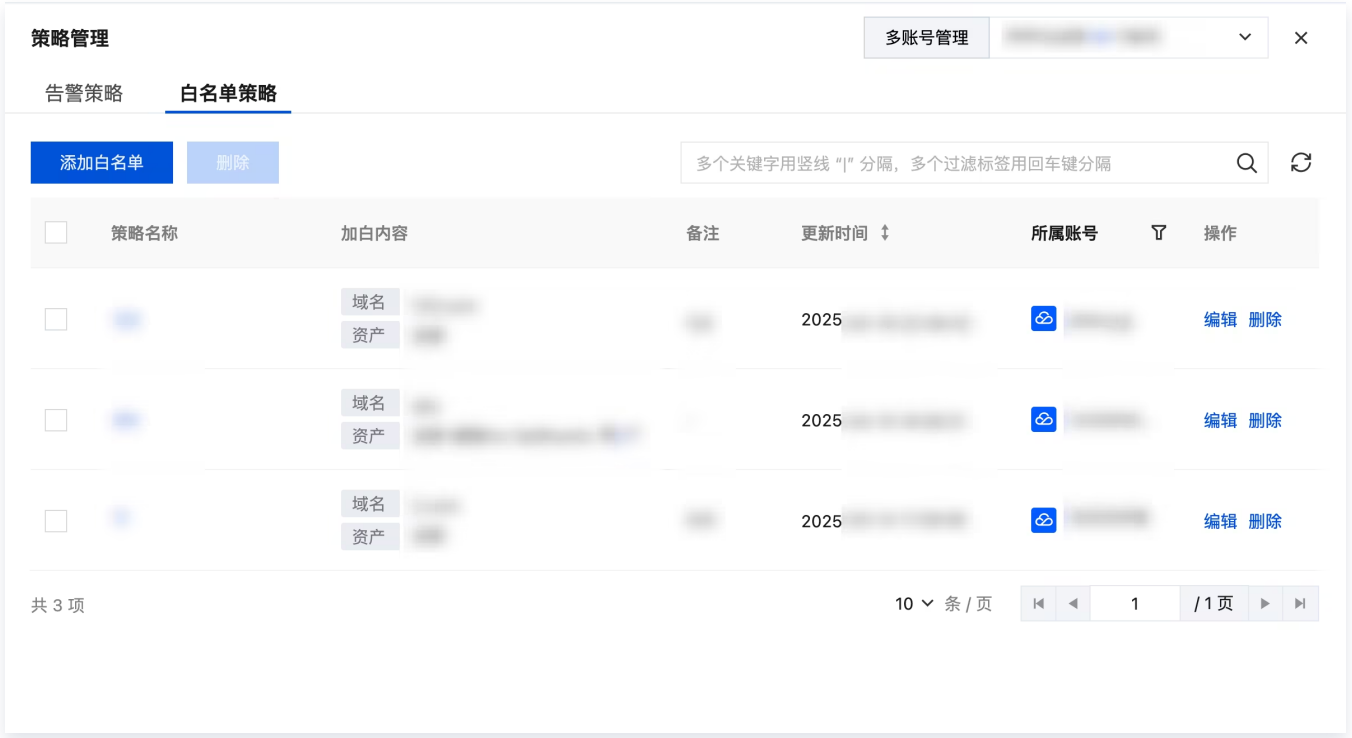
4. 在异常基线页签，单击行为基线策略的 ，修改生效主机/域名，单击**保存**。

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. 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 > 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**。


添加策略-白名单策略
基本信息
填写策略基本信息
1
策略名称 *
请输入策略名称，不超过20个字符
备注
请输入备注信息，不超过20个字符
策略内容
您可以在下方放通 请求的主机及域名 ，后续当检测到对应请求时，将不再生成告警。
生效主机
全部主机 (103) 剔除资产(0)
自选主机
选择加白策略生效的主机和域名范围
2
生效域名
自定义域名
请输入域名/泛域名（如：www.12345.com、*.tencent.com等，暂不支持URL），多个内容以换行分隔
编辑策略-白名单策略
基本信息
策略名称 *
策略1
备注
业务A加白
策略内容
您可以在下方放通 请求的主机及域名 ，后续当检测到对应请求时，将不再生成告警。
生效主机
全部主机 (0) 剔除资产(0)
自选主机
生效域名
自定义域名
2.com
3.com

用户行为分析（UEBA）

最近更新时间：2025-08-26 18:08:52

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**。

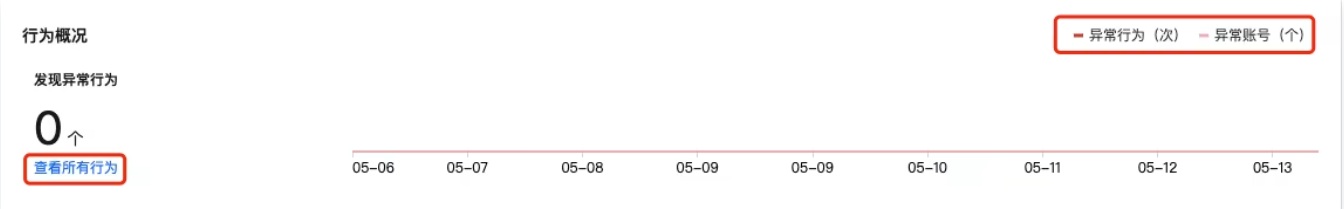
3. 在接入日志源对话框中，日志来源可选择操作和自定义日志来源。

> **说明：**
> 如果在日志分析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 JSON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天的策略命中记录。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。

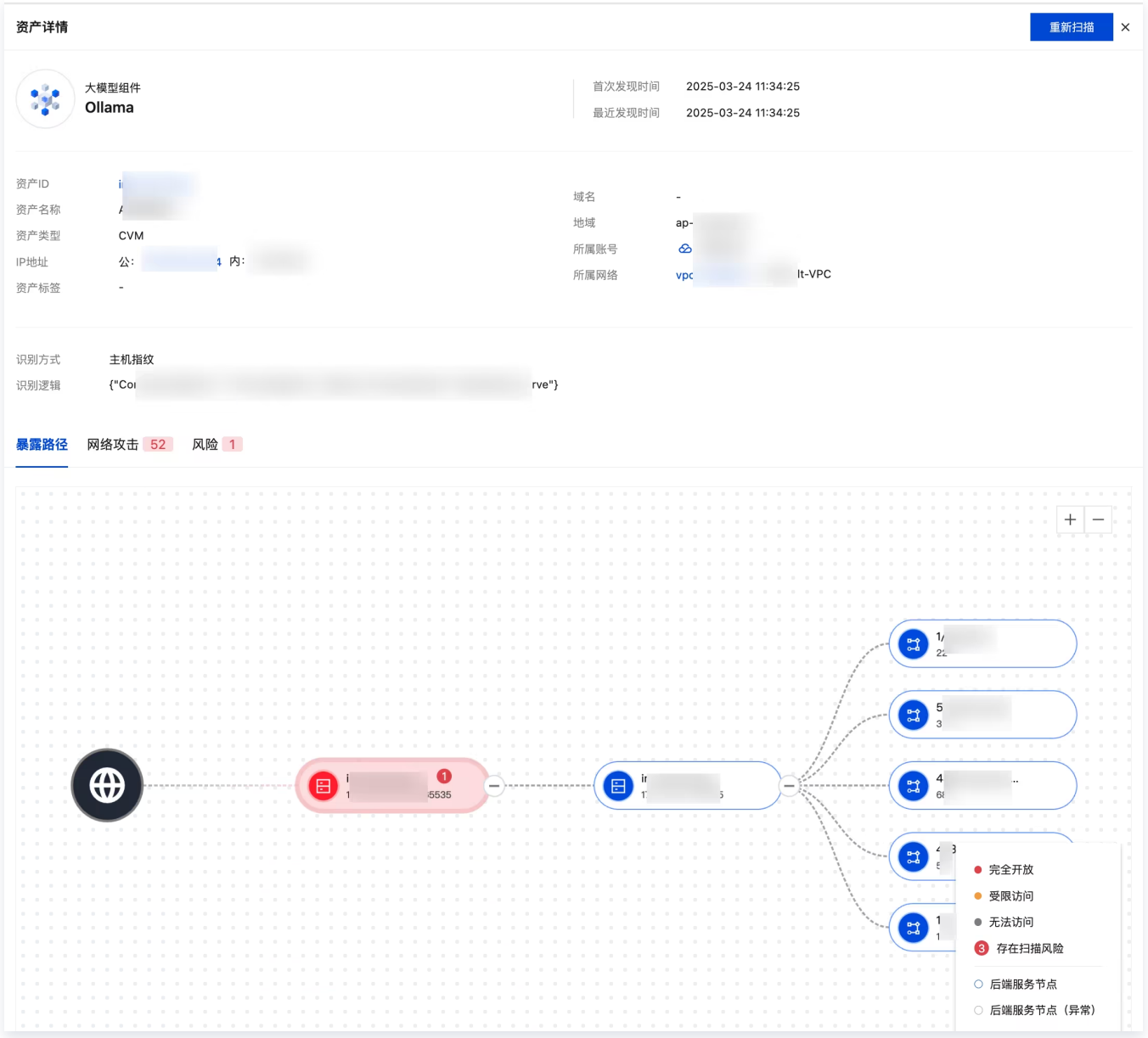
前提条件

已购买 云安全中心高级版 。

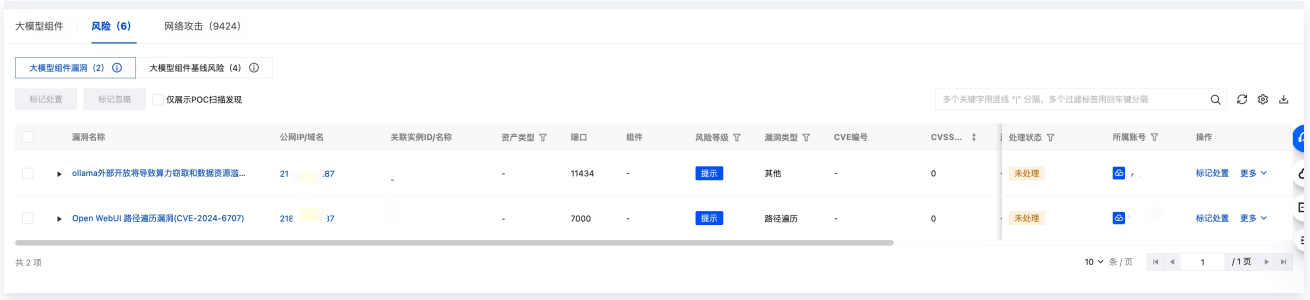
查看功能

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**。

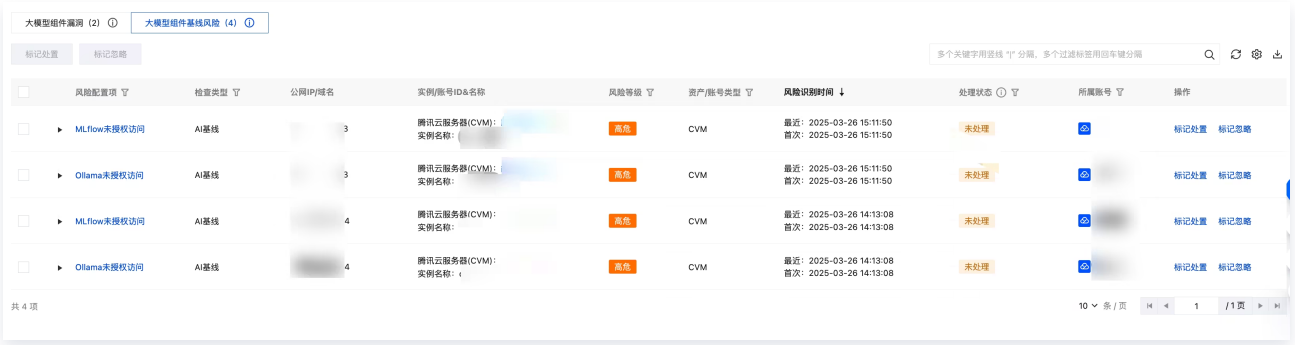
3. 在**大模型资产**列表中，您可以查看已识别的组件信息、资产实例信息、识别方式等。选择您关心的数据，单击**详情**可查看具体的组件识别原因、暴露路径 、网络攻击、风险等。



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）
标记处置
标记忽略
全部攻击状态
请选择时间
请选择时间
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
资产ID/名称
IP地址
目标端口
攻击来源IP/地址
大模型组件
漏洞名称
攻击状态
攻击次数
处理状态
所属账号
操作
公网：
内网：
80
Ollama
dirk1983/chatgpt 服务器端请求伪造 (SSRF) ...
尝试攻击
1
未处理
详情
更多
公网：-
内网：-
ChatGPT-Next-Web服务器端请求伪造 (SSRF...
8080


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
nginx: m
ginx
异常行为
-
攻击数据包
GET
cf-
ustom-
User
影响主机
大模型资产
Ollama
资产类型
CVM
地域
广州
域名
-
所属账号
IP地址
公：1
内：
所属网络
vp
资产标签
-
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

云合规审计

最近更新时间：2025-11-28 16:17:12

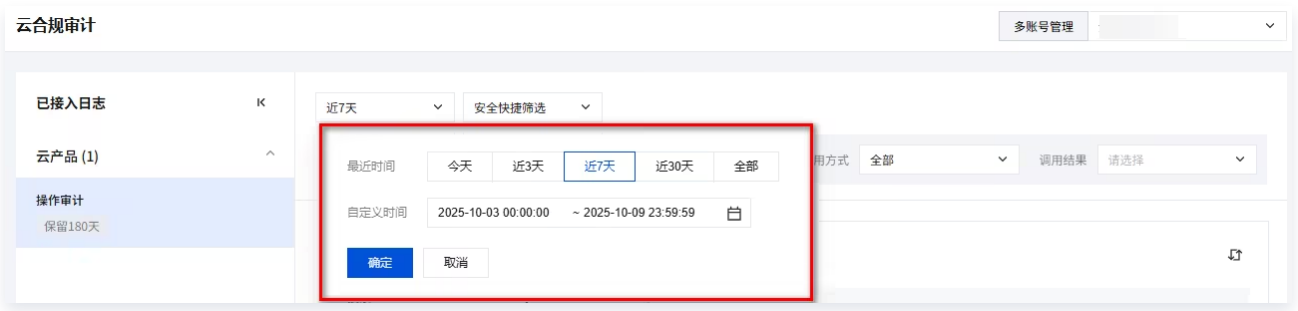
云合规审计模块是基于日志服务构建的统一云产品日志管理平台，该功能专注于云产品日志的原生接入、集中存储与智能分析，实现对云上操作行为的全面记录与审计追踪。通过多维的查询能力，我们为您提供覆盖异常访问识别、安全规则/告警关联等日志审计服务，助力企业落实内部安全管控与外部合规要求，有效降低云上安全风险。

> **注意：**
> **云合规审计模块目前公测中**，相关策略如下：
> - 公测期间将**不再允许新购/扩容**云安全中心日志分析模块的“日志分析量”。
> - 原日志分析模块**存量的“日志分析量”将1:1转化为云合规审计模块的“日志存储量”，云产品及云安全中心相关的日志将占用存储量（公测期间，“操作审计”日志将默认存储且不占用日志存储量，公测结束后将恢复正常占用），其他安全产品的日志将不在云安全中心存储，仅跟随各产品已存储日志提供查询能力。**

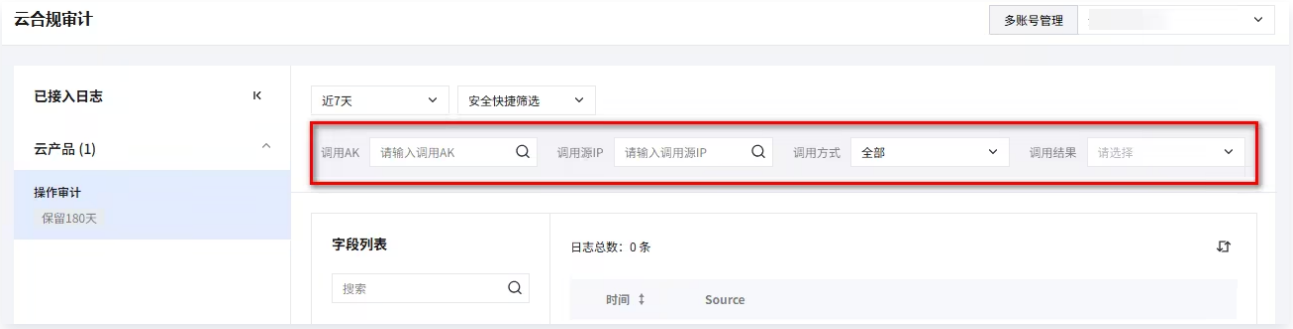
安全快捷筛选

1. 登录 云安全中心控制台，在左侧导览中，单击**云合规审计**。
2. 在云合规审计页面，选择**安全快捷筛选**。

3. **安全快捷筛选：**针对不同云产品日志，基于其相关特性提供快捷筛选功能，可快速筛选重点字段对应的日志结果。
   - 按时间筛选：支持按最近时间或自定义时间范围进行检索。



- 按字段检索：支持按字段进行输入/选择，进行精准检索。

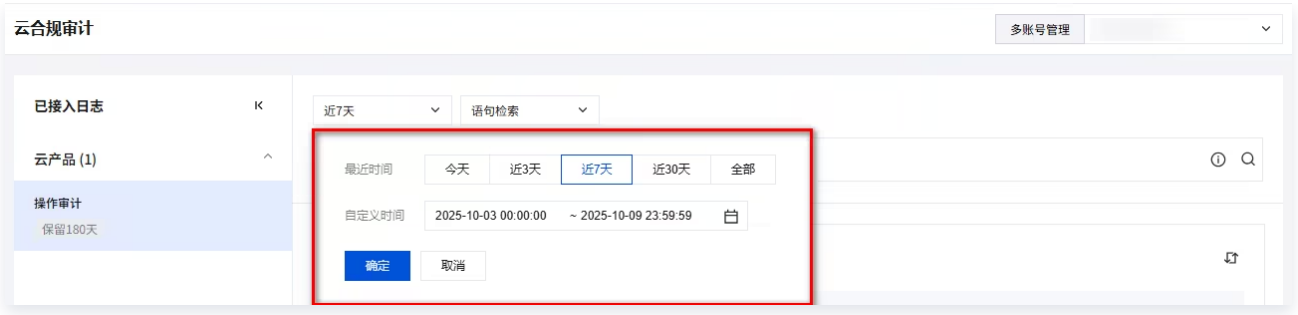


日志类型	字段名	示例
操作审计	调用 AK	AKID75XXX
	调用源 IP	119.x.x.x
	调用方式	• API调用 • 控制台调用 • 外网调用 • 局域网调用
	调用结果	• 未授权的 API 调用 • 返回错误的调用

语句检索

1. 登录 云安全中心控制台，在左侧导览中，单击**云合规审计**。
2. 在云合规审计页面，选择**语句检索**。

3. **语句检索：**通过日志查询语句进行日志检索。
   - 按时间筛选：支持筛选最近时间/自定义时间范围进行检索。



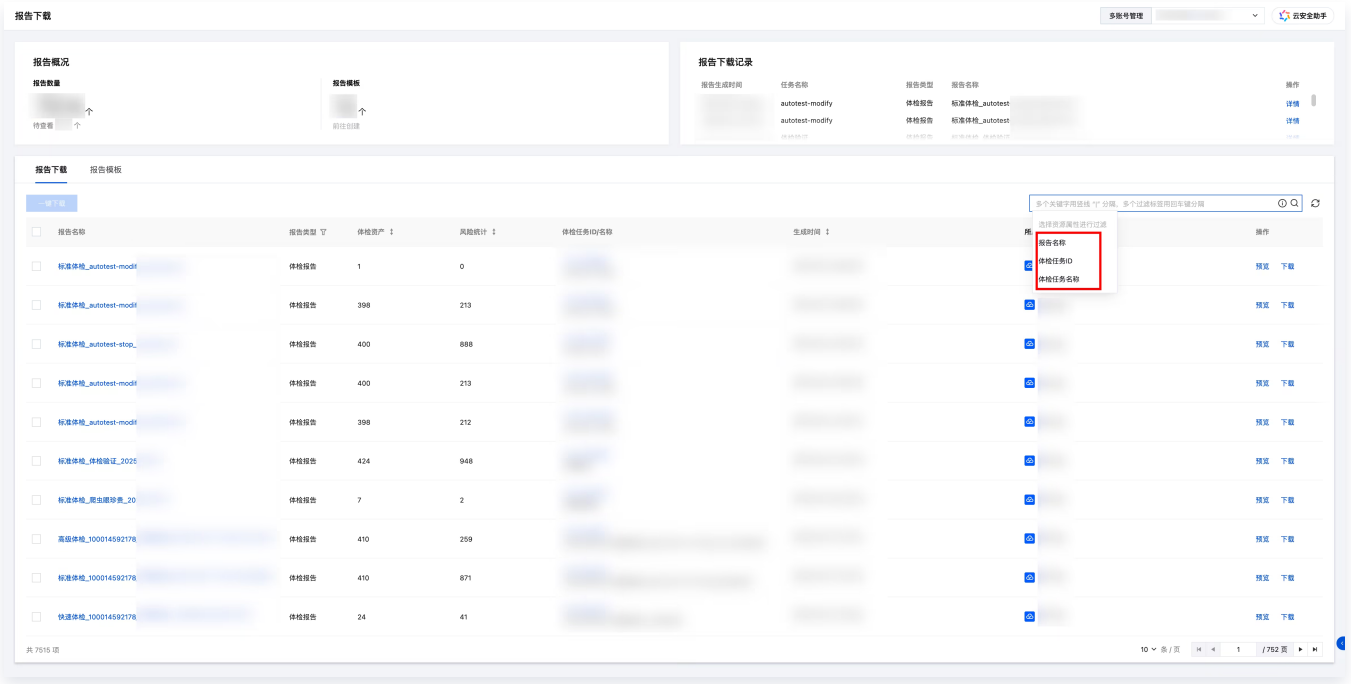
- 按语句检索：支持 Lucene 语法，默认表名为 logTable。

报告下载

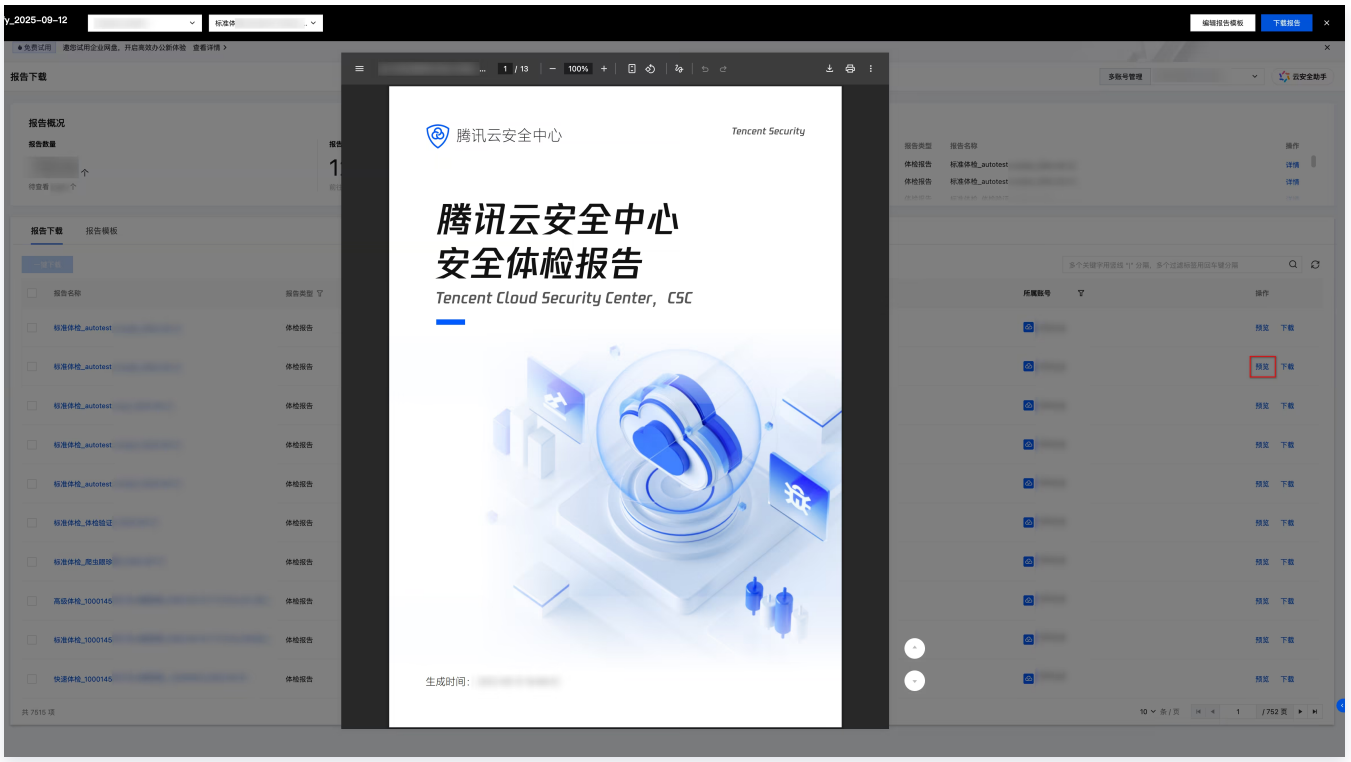
最近更新时间：2025-09-17 21:26:21

报告下载功能允许用户以报告的形式获取安全体检结果，并支持编辑报告模板，按需定制报告。

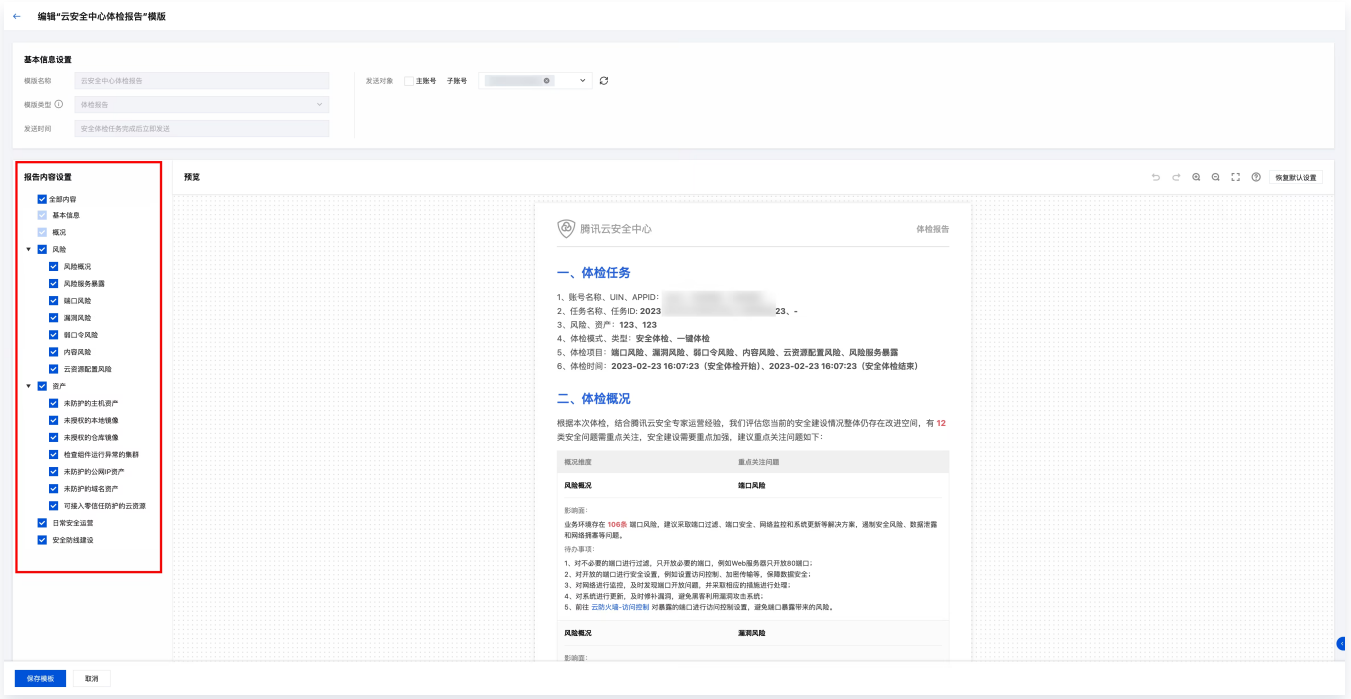
1. 登录 云安全中心控制台，在左侧导览中，单击**报告下载**。
2. 在报告下载页面，您可以根据体检任务筛选报告。支持通过**体检任务 ID** 或 **体检任务名称**进行模糊搜索，快速定位目标报告。



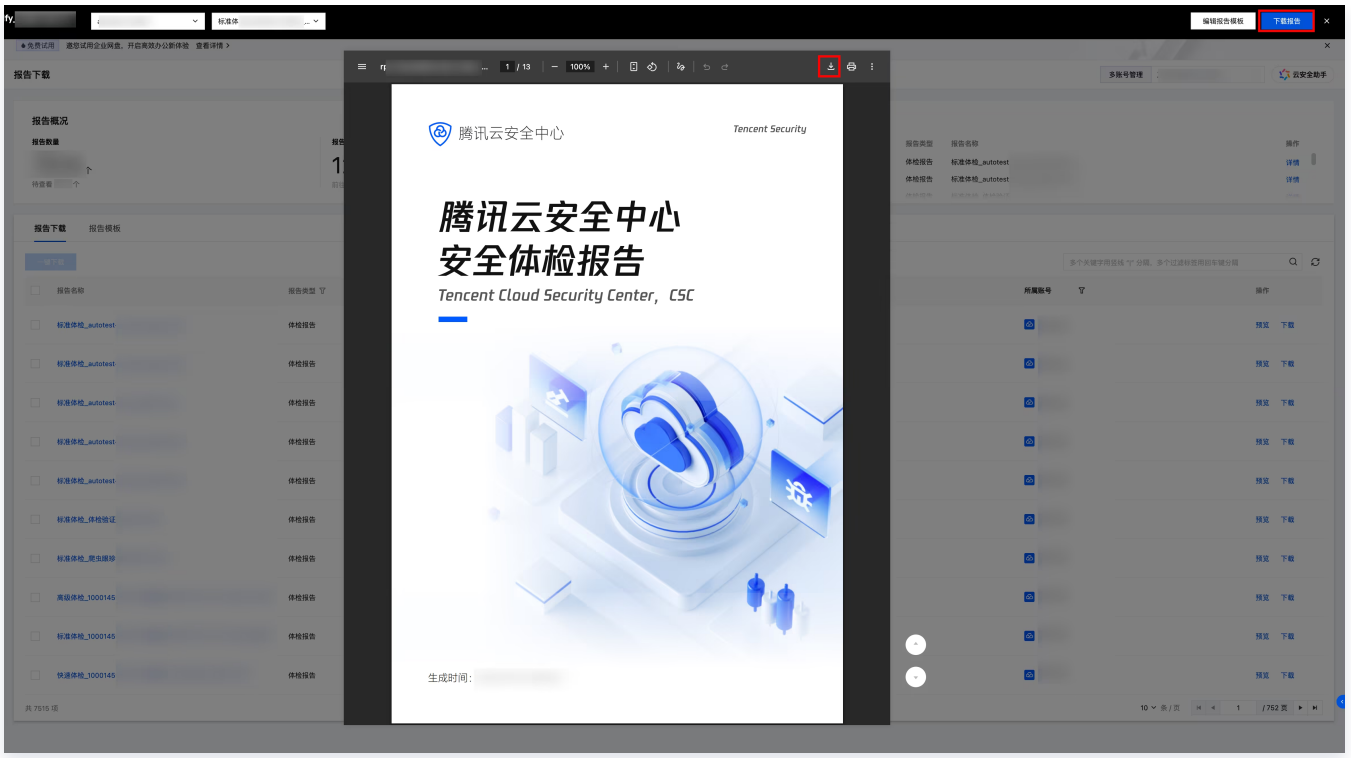
3. 单击目标报告操作列的**预览**，查看报告内容并确认结果。



4. 若需要变更报告内容，单击**编辑报告模板**，进入编辑模式，设置报告内容，完成后单击**保存模板**后生效，生效后该模板将生效于后续的所有体检报告。



5. 确认报告内容无误后，单击**下载报告**将报告导出到本地。


报告下载
报告概况
报告下载
报告模板
腾讯云安全中心
Tencent Security
腾讯云安全中心
安全体检报告
Tencent Cloud Security Center, CSC
生成时间:

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**。

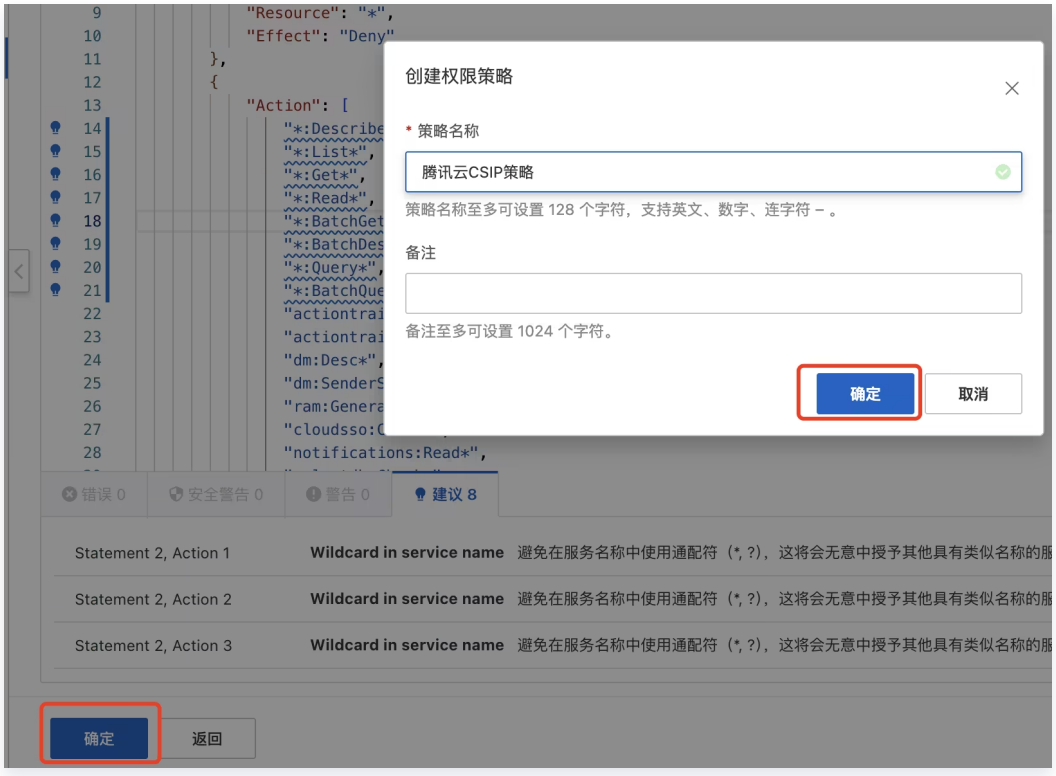
2. 在策略脚本编辑框中，填写下方内容，可访问 文档 了解所需权限的具体原因及参考的系统策略。

```
{
  "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。

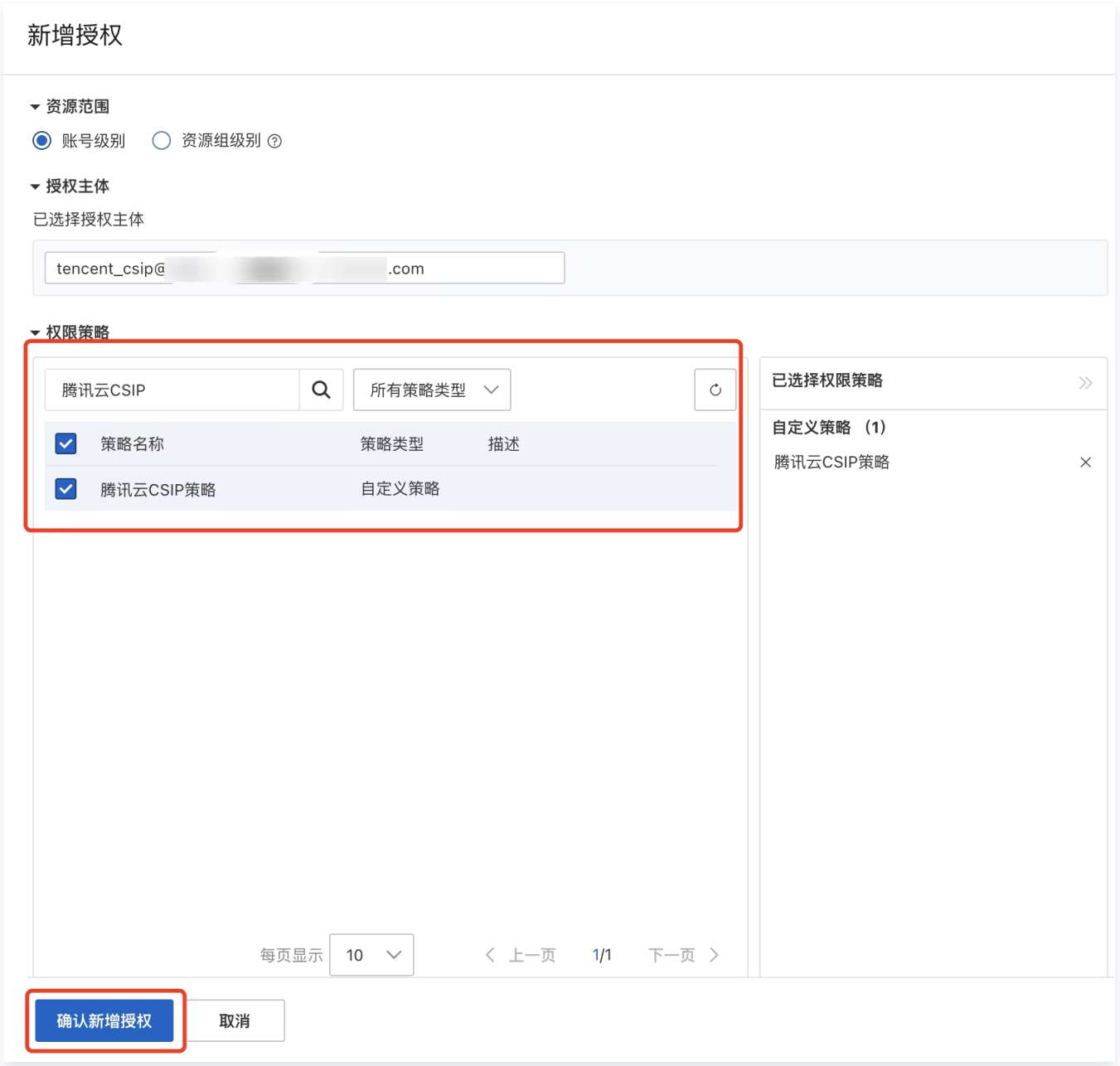


4. 登录阿里云控制台后前往 RAM 访问控制-创建用户 ，选择**使用永久 AccessKey 访问**，推荐使用 tencent_csip 作为名称，便于理解账号用途。

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

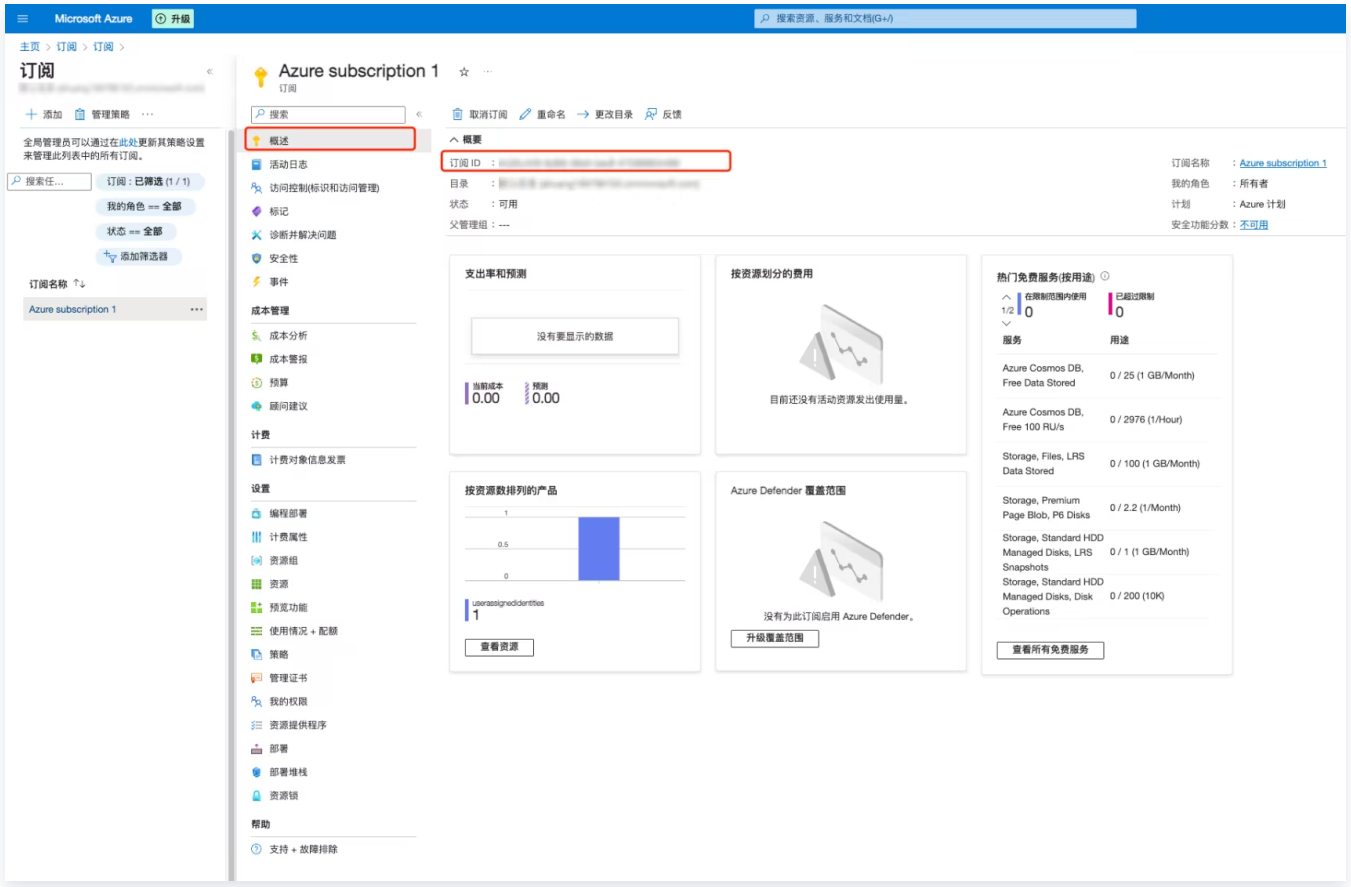
1. 登录 Azure 后前往应用注册页面，单击**新注册**（如果已有应用注册，跳到第二步）。

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**。

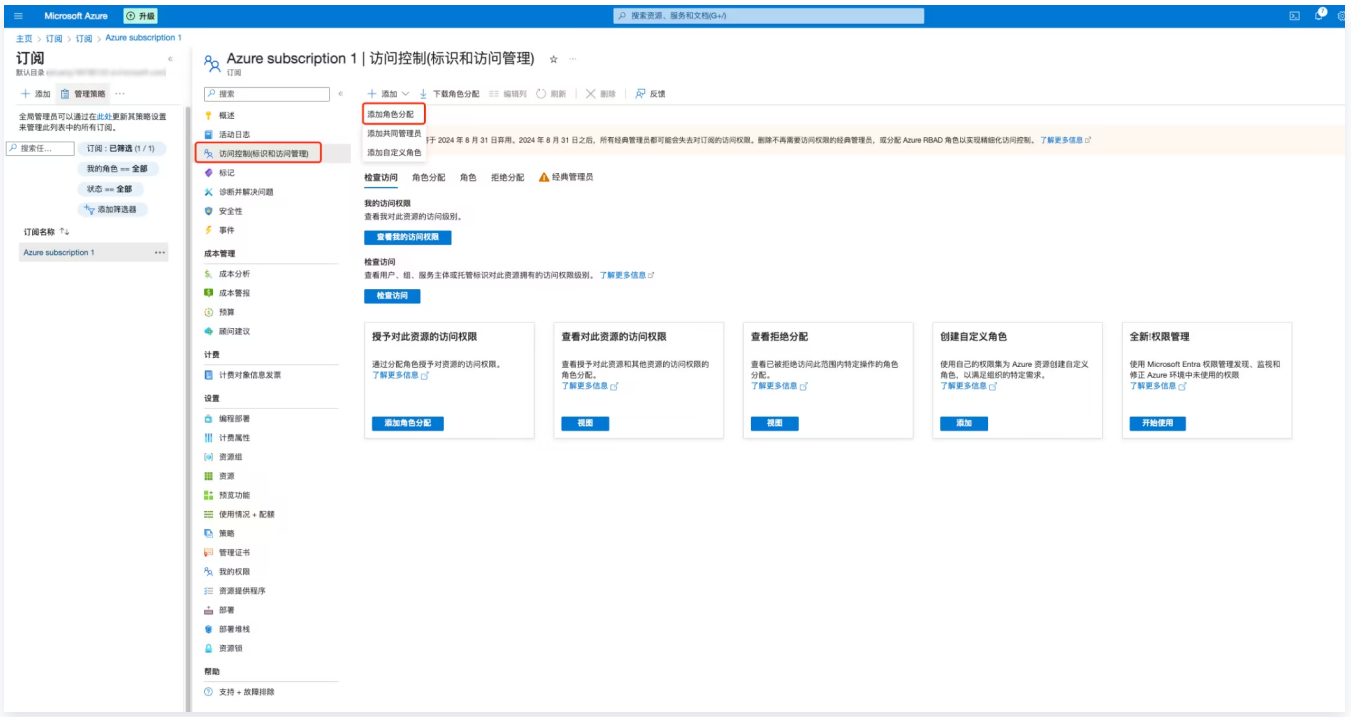
步骤2：获取订阅 ID

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**。

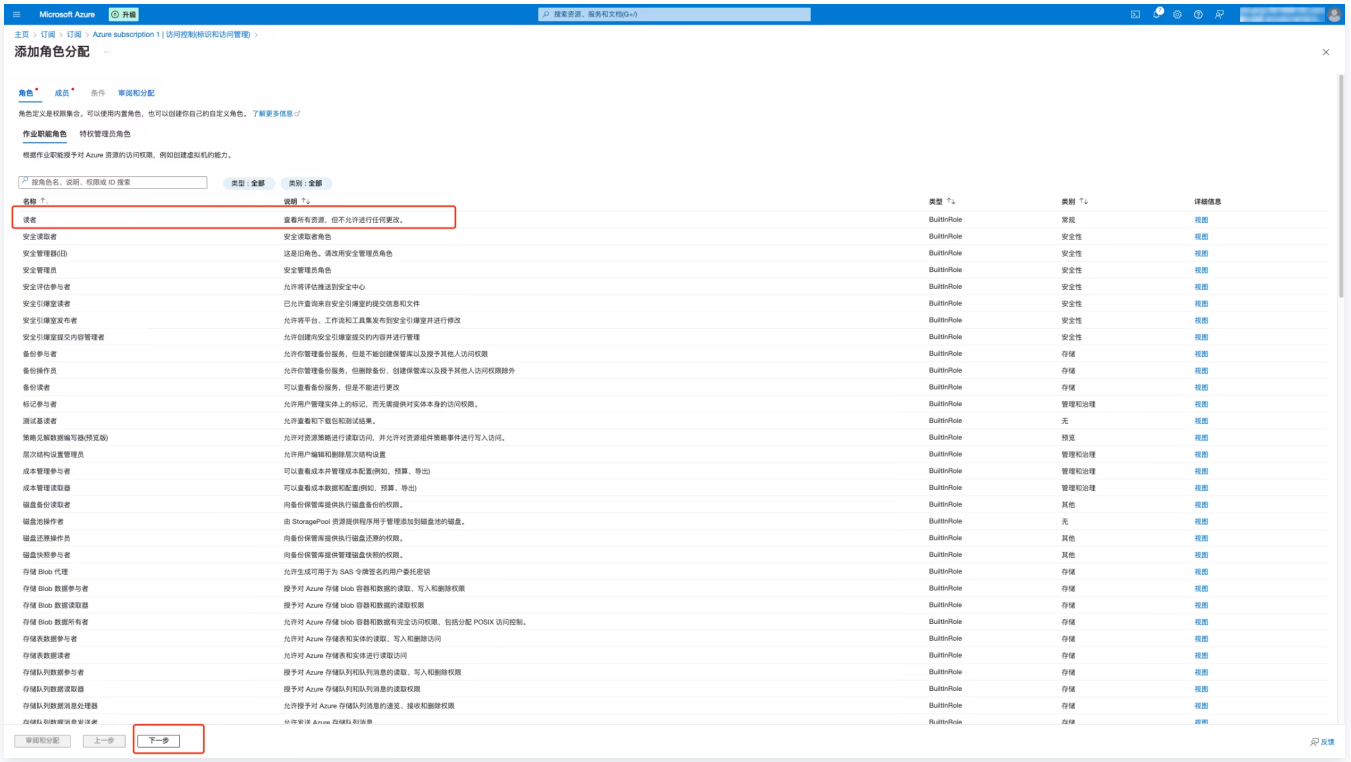
2. 在订阅详情页面，单击**概述**，获取**订阅 ID**。



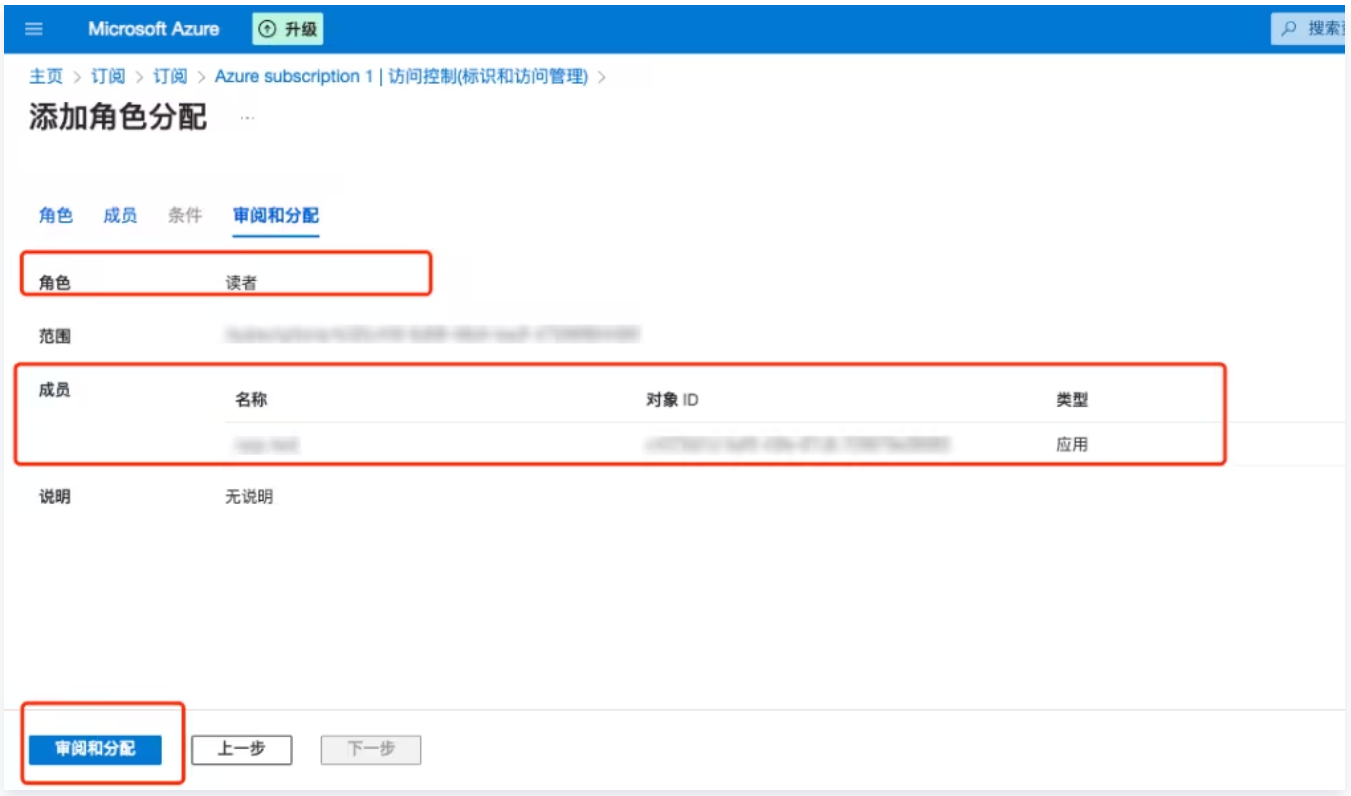
3. 选择**访问控制**，单击**添加**，选择**添加角色分配**。



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**。

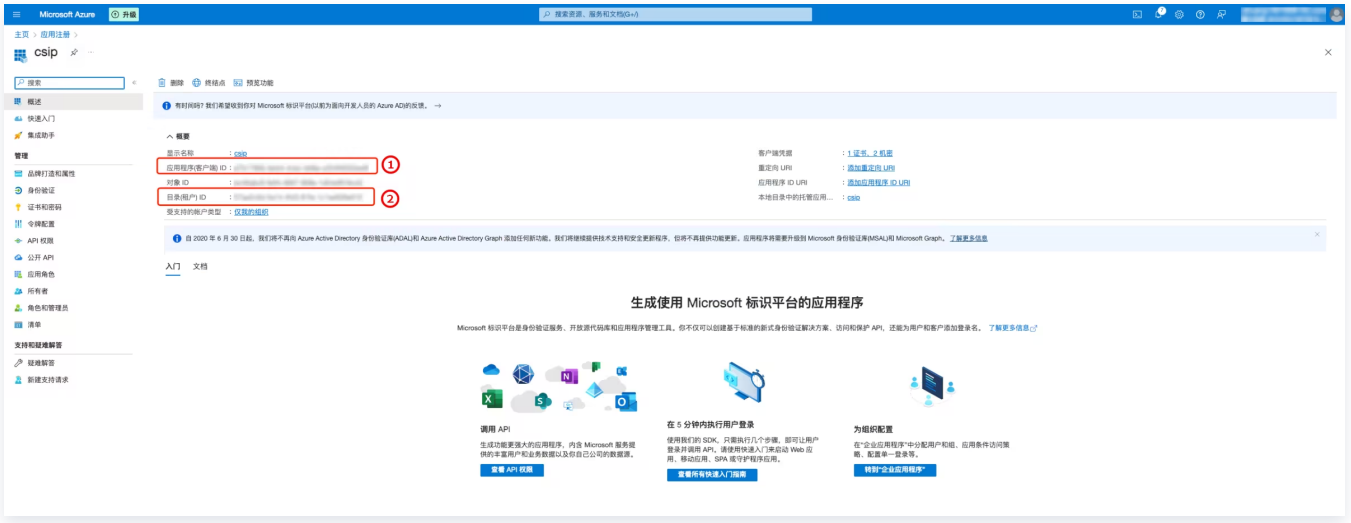


5. 添加需要分配的用户，单击**选择成员**，在搜索框输入要添加的“应用注册”名称，选择该**应用注册**，单击**下一步**。
6. 确定角色与成员，单击**审阅和分配**。



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**。

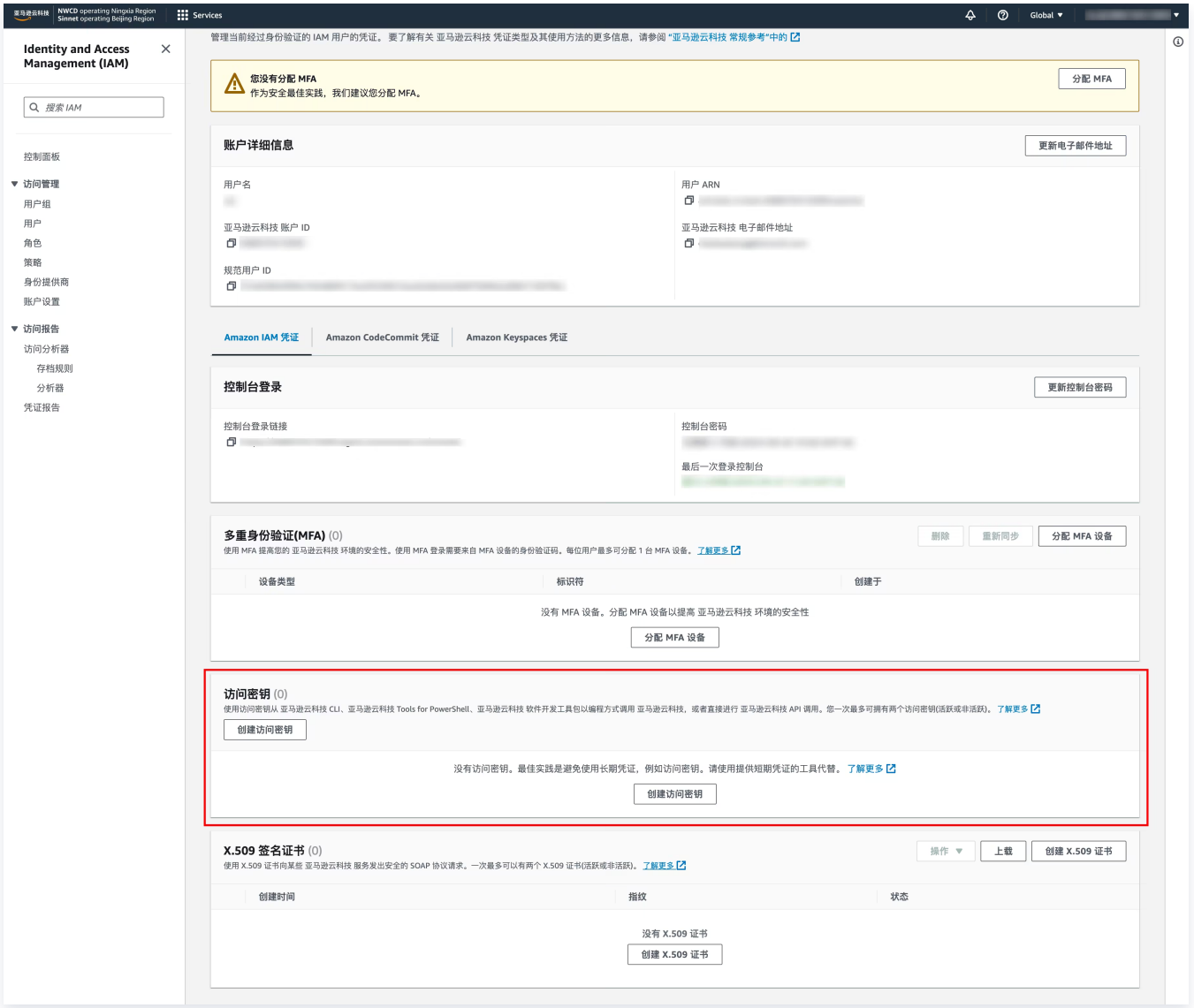
3. 在证书和密钥页面，获取**客户端密钥**。

AWS 账号

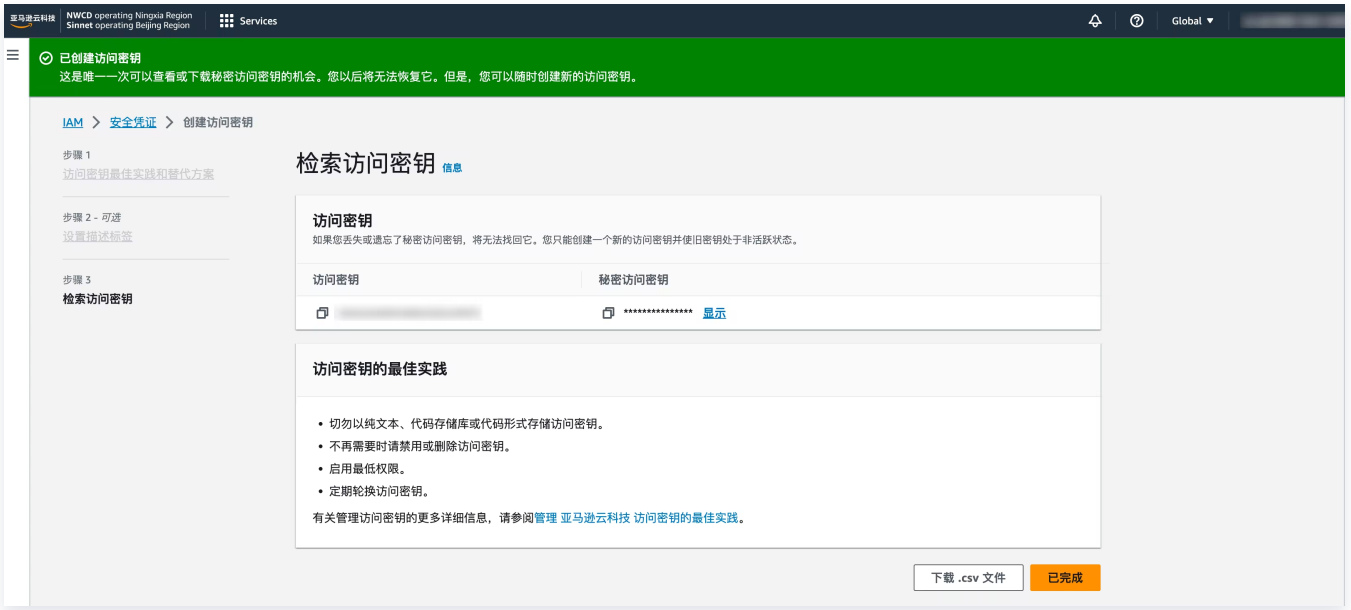
快速配置

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。

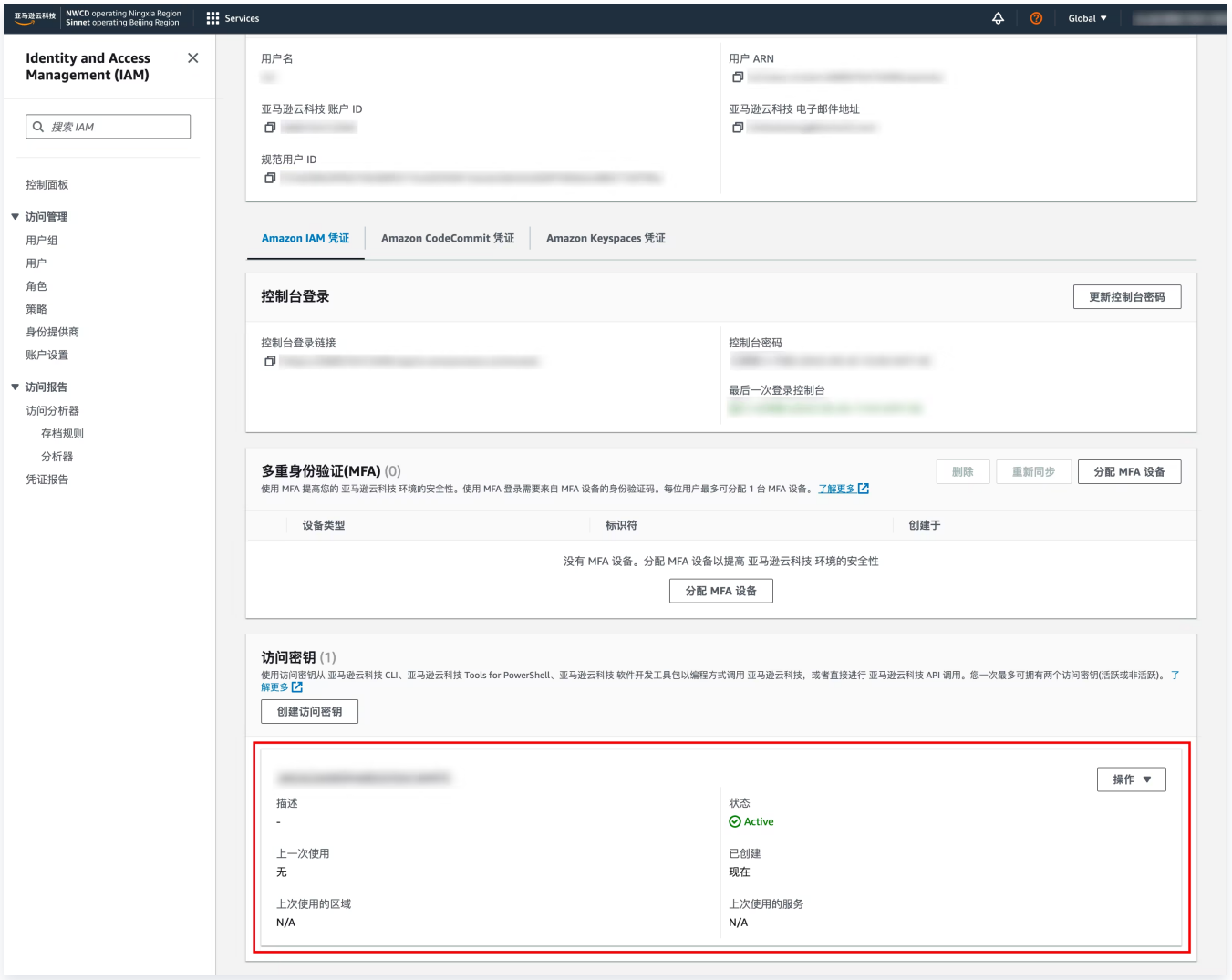
1. 请登录 AWS 后前往 安全凭证 页面，单击**创建访问密钥**生成可用于监控或管理亚马逊云科技资源的“访问密钥”、“秘密访问密钥”。



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”。

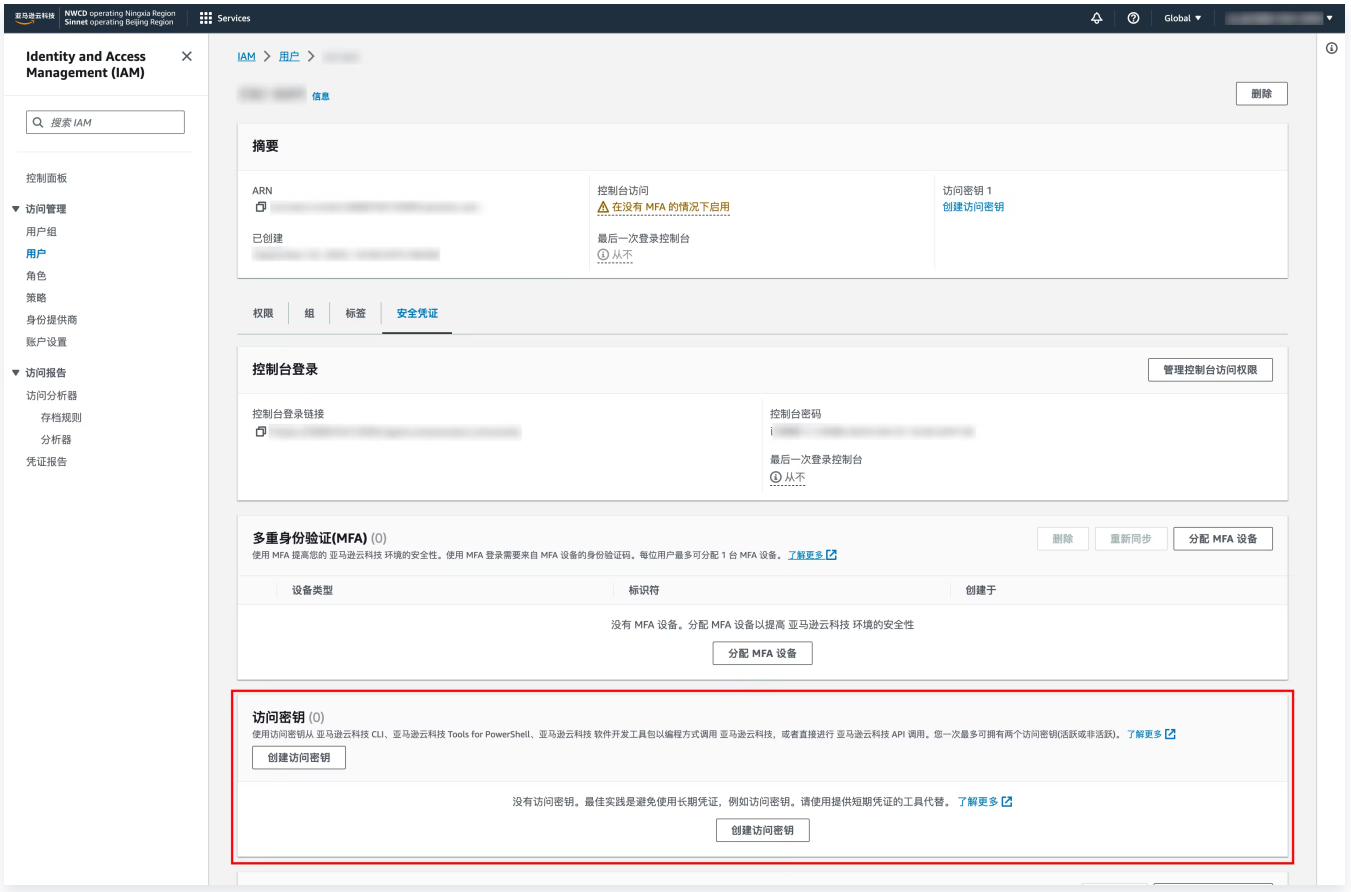


手动配置

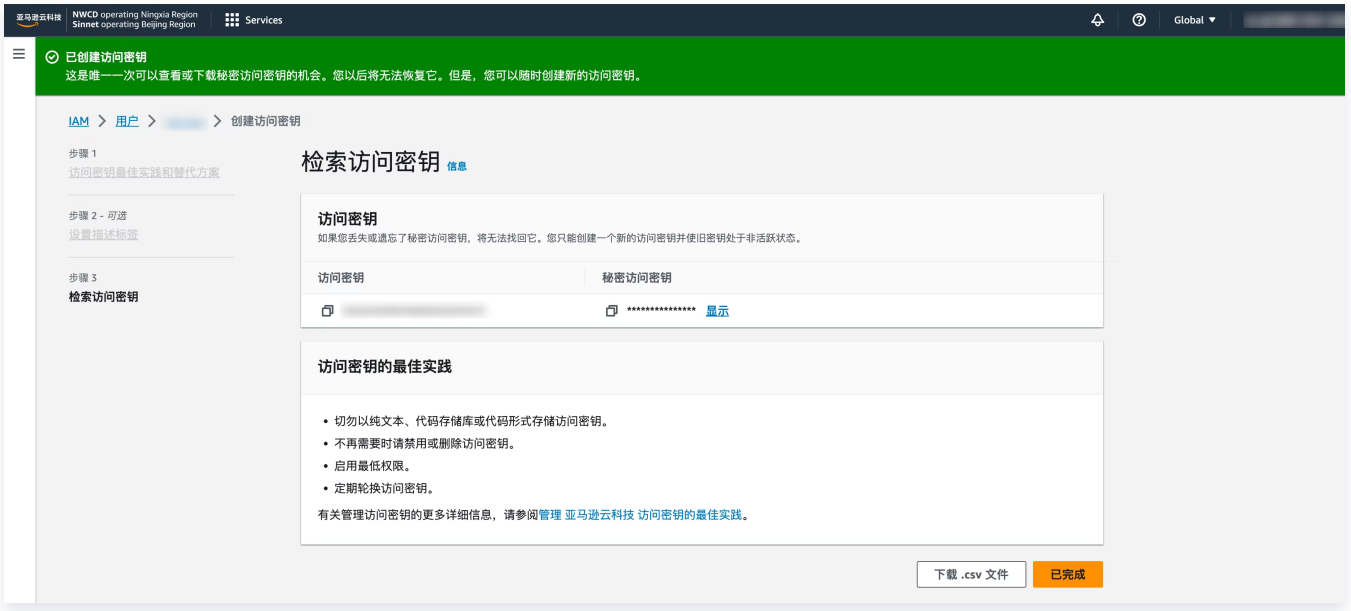
完成时间约为5分钟，但权限配置较为复杂，需要为创建好的子账号配置访问密钥（AK），以便更灵活地控制权限范围。

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”。



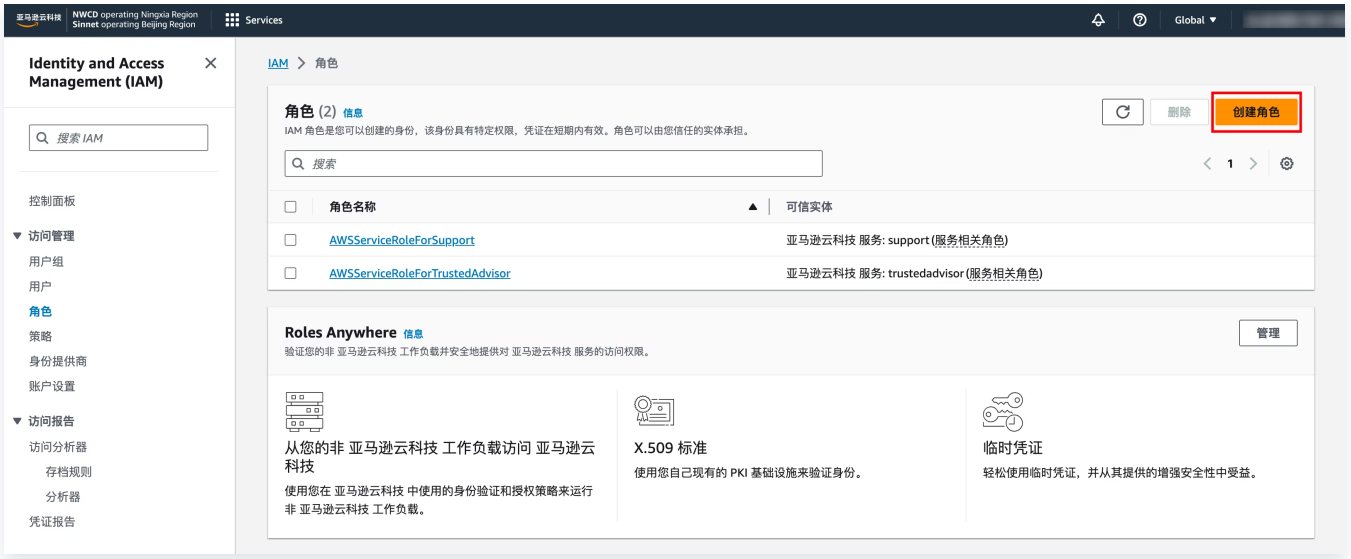
3. 查看或下载“访问密钥”、“秘密访问密钥”，确保“访问密钥”的状态为 Active 后，将“访问密钥”、“秘密访问密钥”填写至“子账号SecretID”、“子账号 SecretKey”。



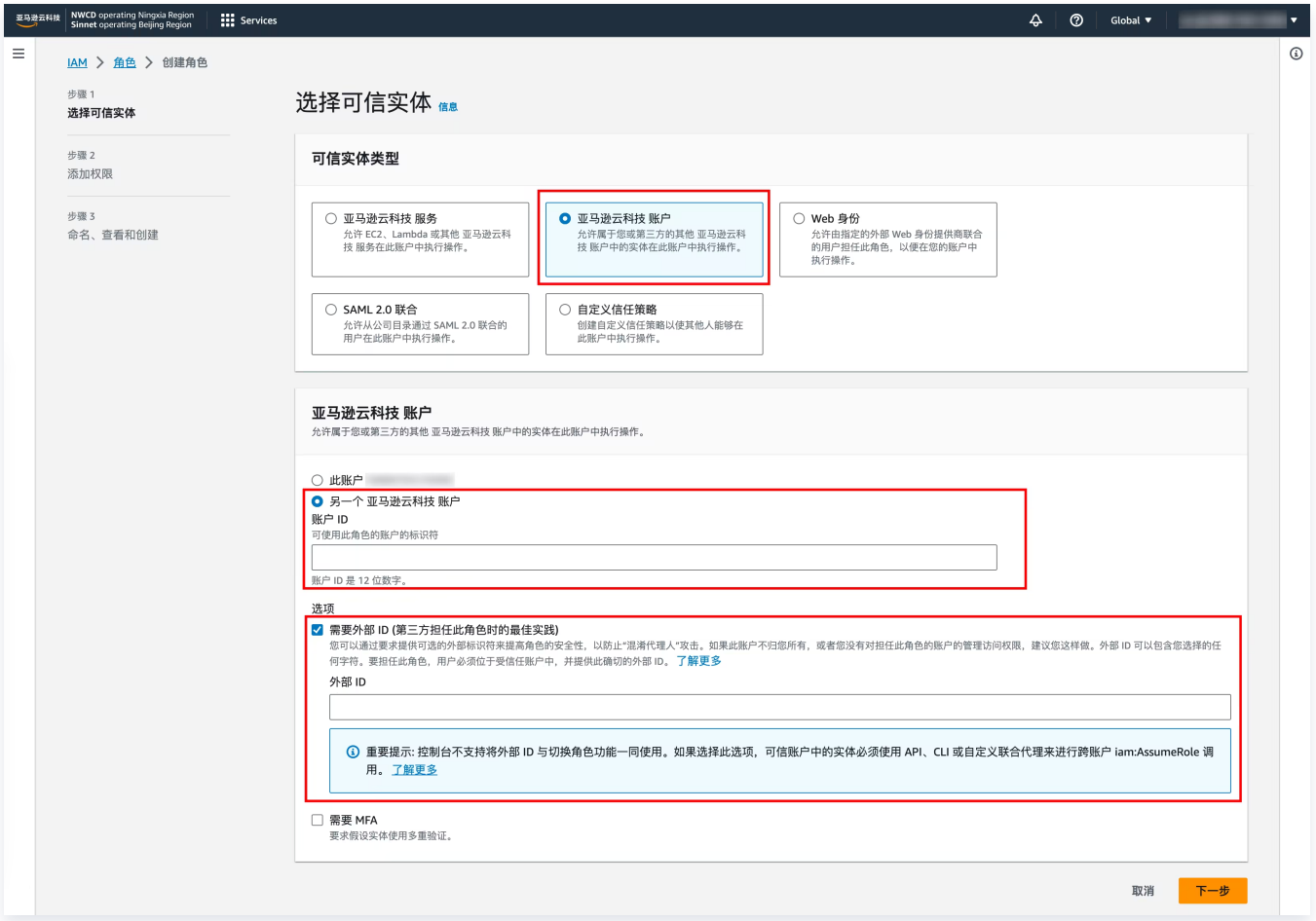
高级配置

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。

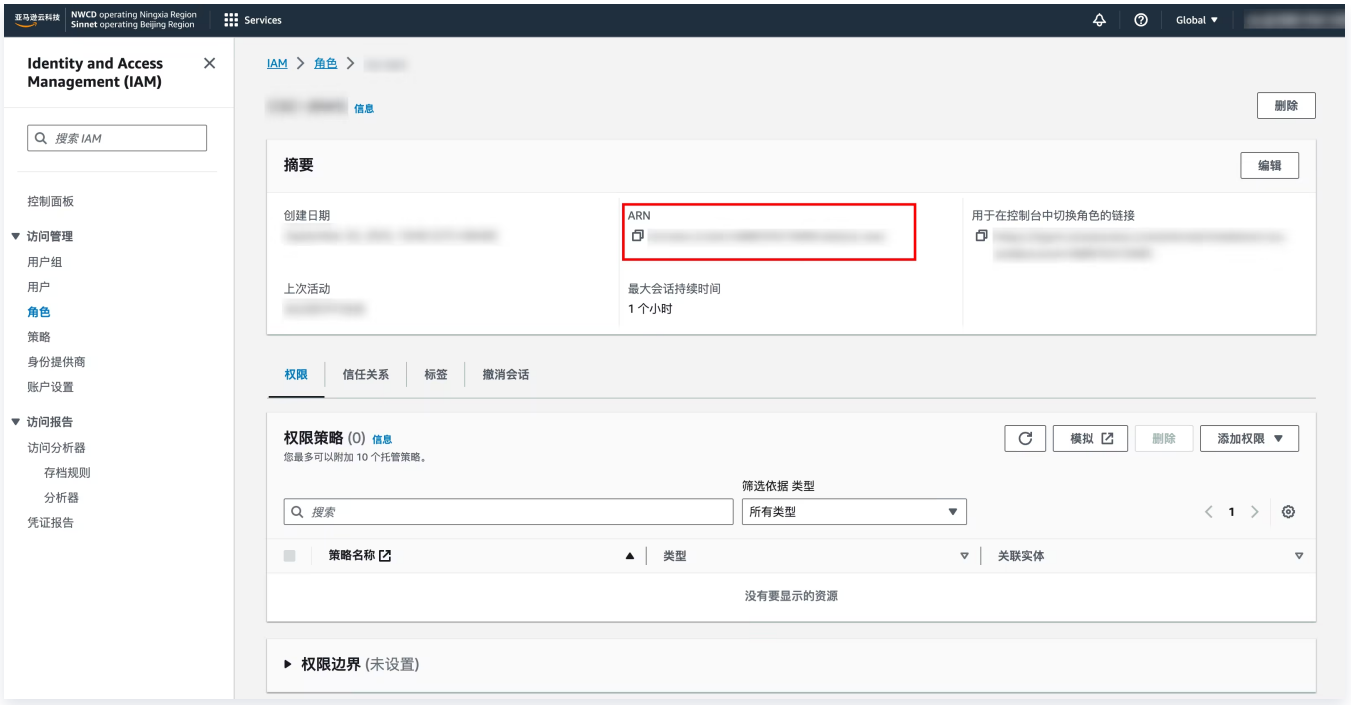
1. 请登录 AWS 后前往 IAM > 角色 页面，单击**创建角色**，该身份具有特定权限，凭证在短期内有效。角色可以由您信任的实体承担。



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：2026-04-29 17:55:00

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，适用于高效且安全的免密码切换。

集中管理账号

无需部署，集团管理员/委派管理员支持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。

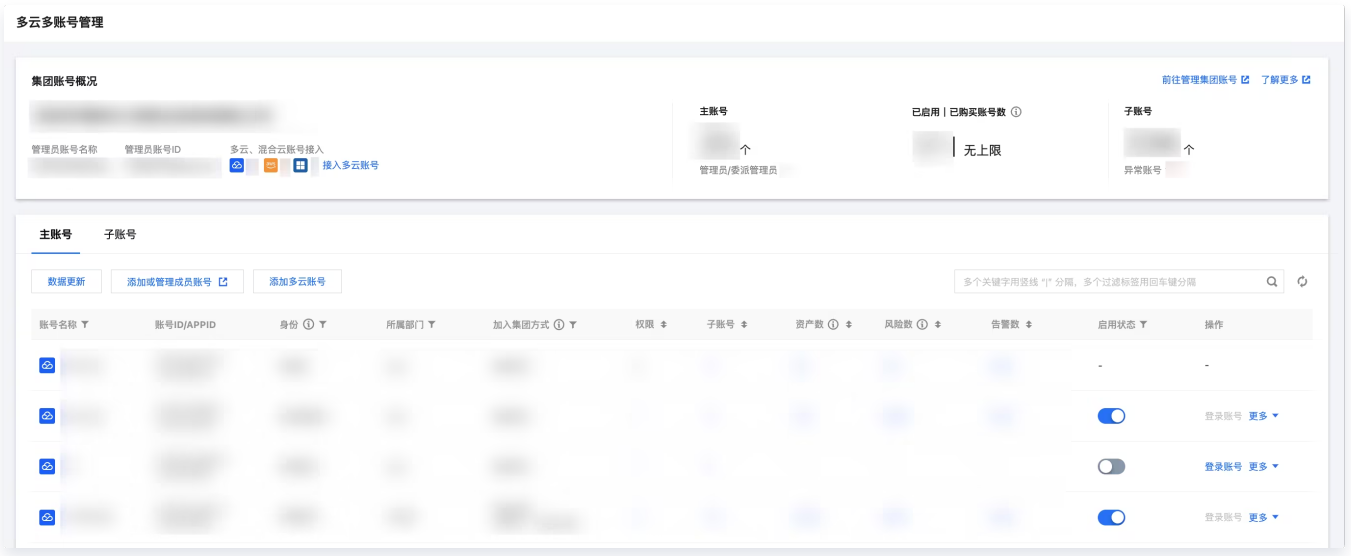
账号切换

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。

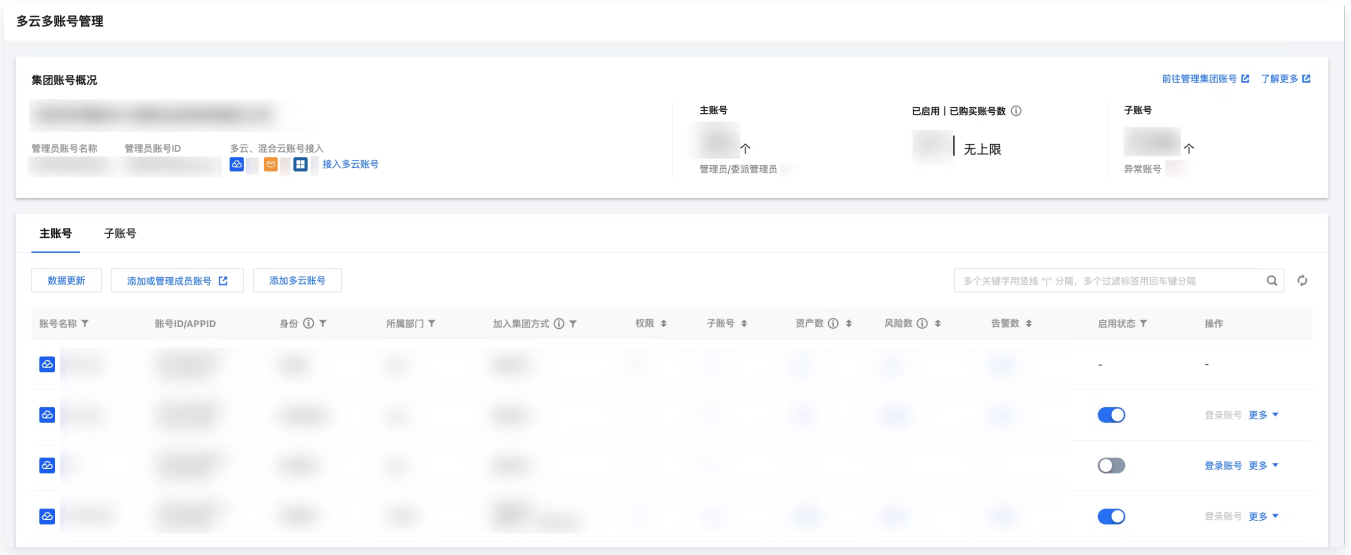
系统设置-多账号管理

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，适用于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



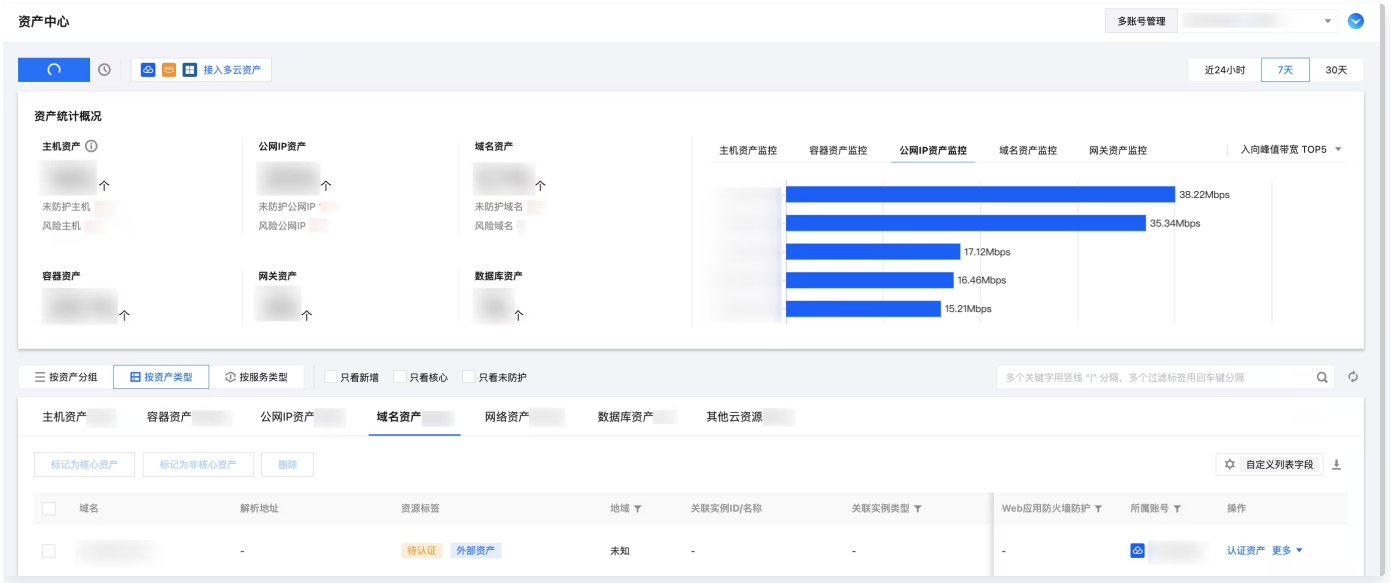
- 管理员子账号登录



- 成员主账号、子账号登录

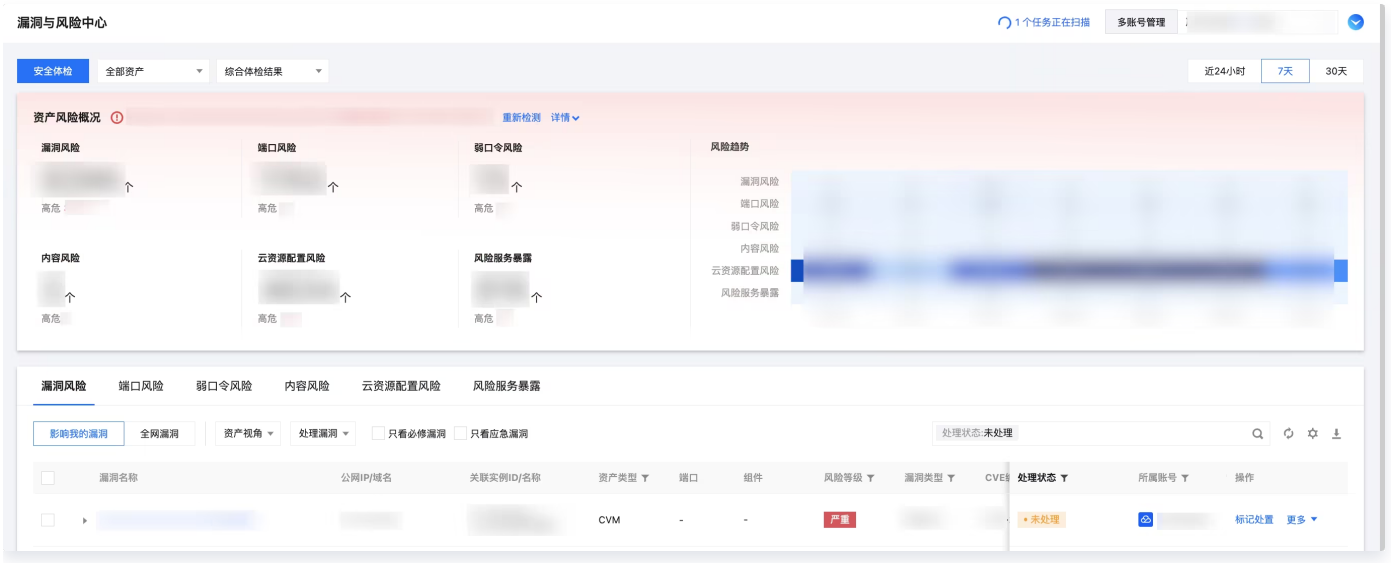
资产中心

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。

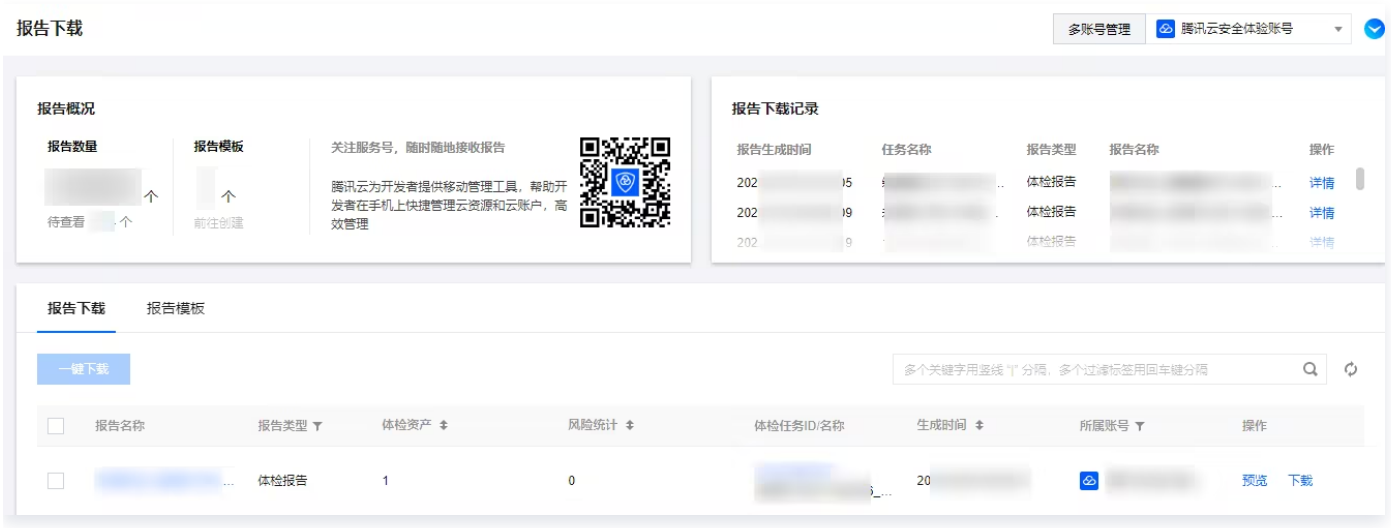


安全体检

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

非管理员账号能否使用多账号管理功能?

需先完成 管理委派管理员账号 设置，才能使用多账号管理功能。

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：2025-12-11 14:40:12

权限说明

云安全中心纳管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"
                    ]
                }
            }
        }
    ]
}
```

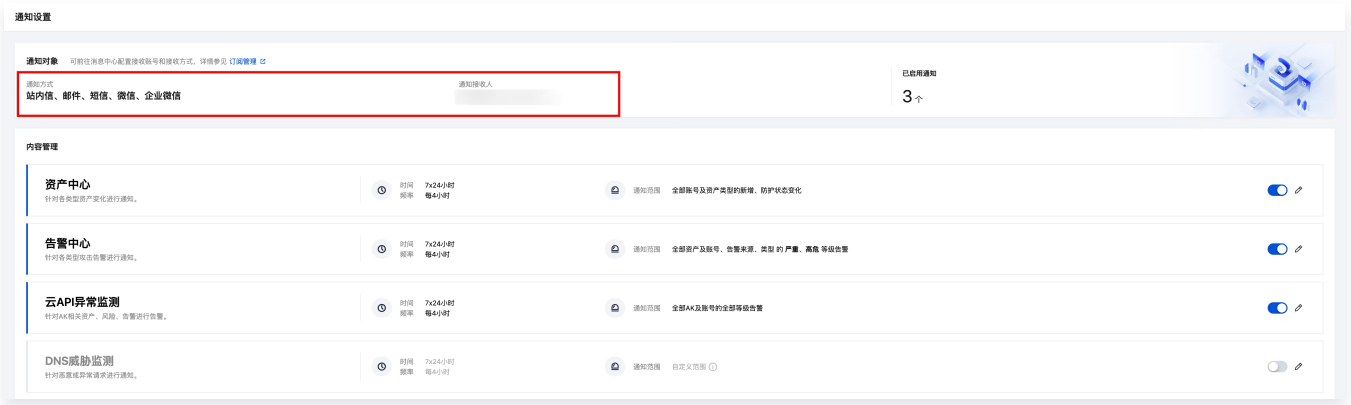
通知设置

最近更新时间：2025-09-17 21:26:21

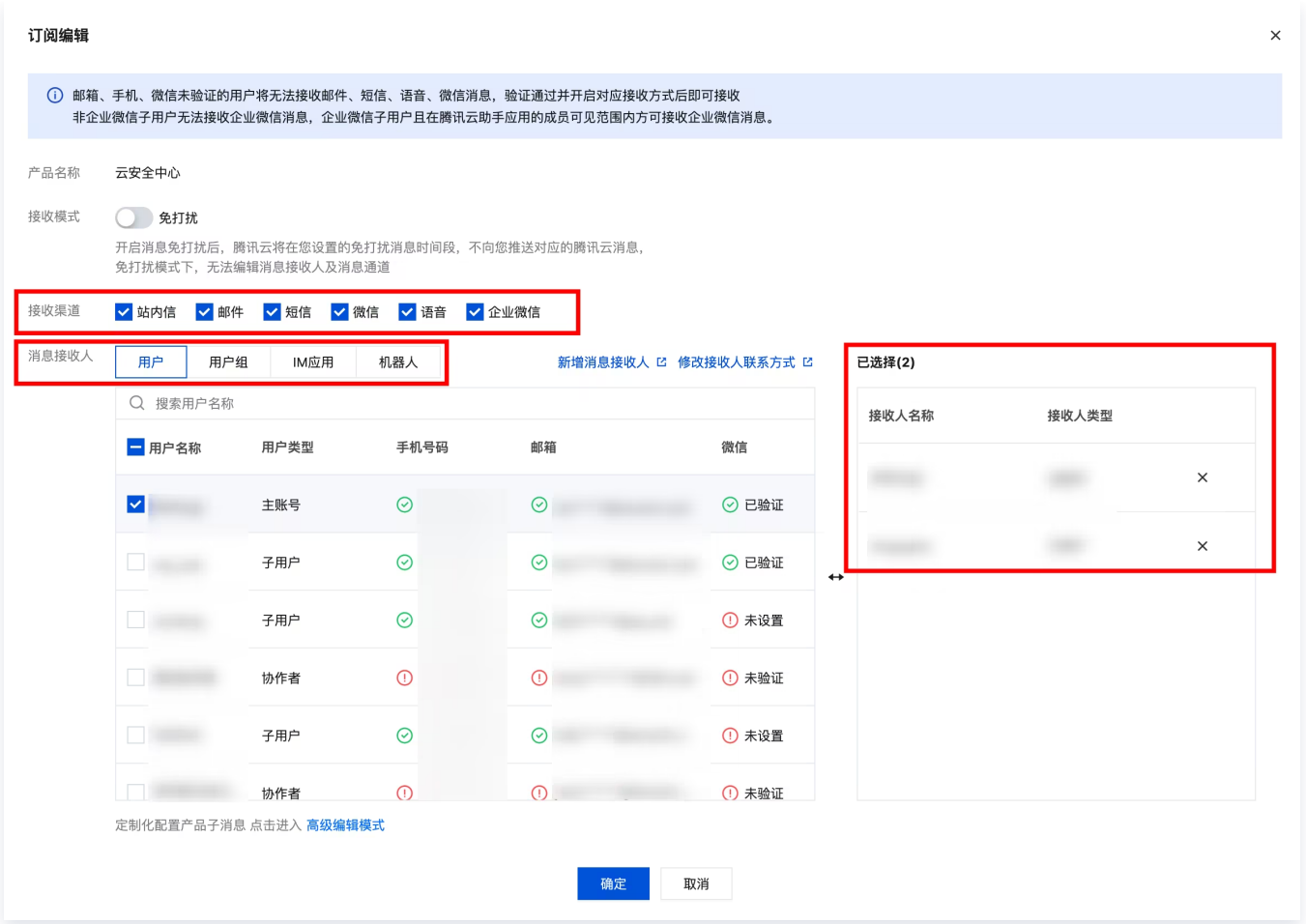
通知设置是用于配置和管理安全事件告警通知的功能模块。它允许用户自定义接收通知的时间、范围，以及管理通知方式与通知接收人。

通知对象管理

1. 登录 云安全中心控制台，在左侧导览中，单击**通知设置**。
2. 在通知设置页面，确认通知方式与通知接收人是否符合预期，若需要修改，请前往消息中心进行配置。

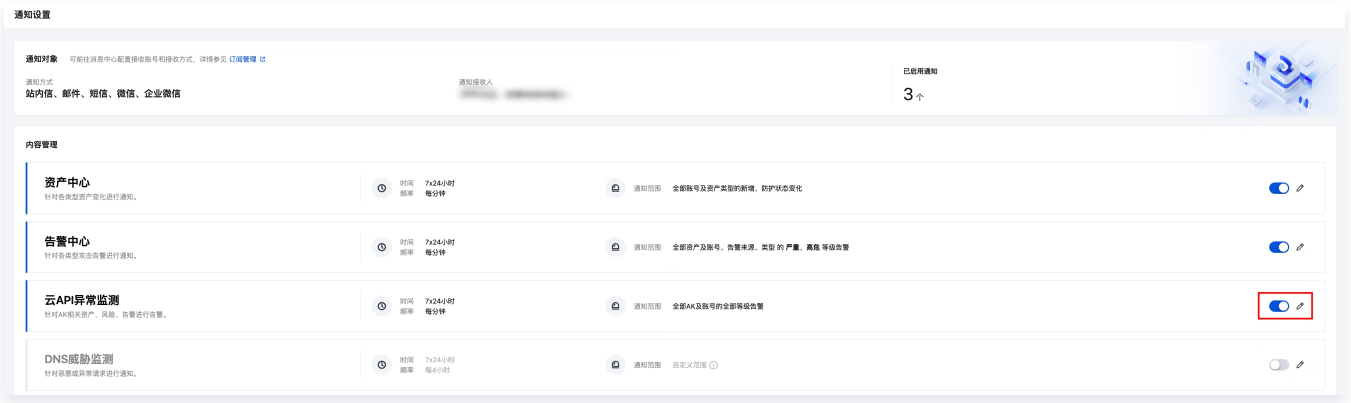


3. 在**消息中心** > 消息订阅 页面，选择产品云安全中心进行订阅编辑。
   - 确保接收渠道为预期内渠道，云安全中心支持的通知方式包括**站内信、邮件、短信、微信、企业微信**。
   - 选择对应的接收人，并确认已设置选择的接收渠道对应的联系方式，云安全中心支持通知**用户、机器人**。



通知内容管理

1. 登录 **云安全中心控制台**，在左侧导览中，单击**通知设置**。
2. 在通知设置页面，对于需要进行通知的板块，可单击卡片右侧的**开关**一键开启。



3. 开启后按照默认的时间、频率、通知范围进行通知。

4. 如果需要对通知的时间、频率、通知范围进一步自定义，单击卡片右侧的**编辑**。

5. 在编辑页面，根据实际需求调整通知模式、时间、范围，单击**确定**。


通知设置-告警中心
通知模式
标准通知
高级通知 (自定义配置)
通知时间
7x24小时
自定义时间
星期一, 星期...
08:00:00 ~ 20:00:00
通知范围
告警来源/频率
云安全中心
每分钟
云防火墙
每分钟
主机安全
每分钟
容器安全
每分钟
Web应用防火墙
每小时
告警类型
信息收集
扫描探测
攻击尝试
疑似成功入侵
资产异常行为
主动外联
横向移动
用户异常行为
告警等级
严重
高危
中危
低危
提示
所属账号
告警资产范围
核心资产
全部资产
从现有资产选择
确定
取消

访问权限管理

最近更新时间：2025-12-11 14:40:12

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 。

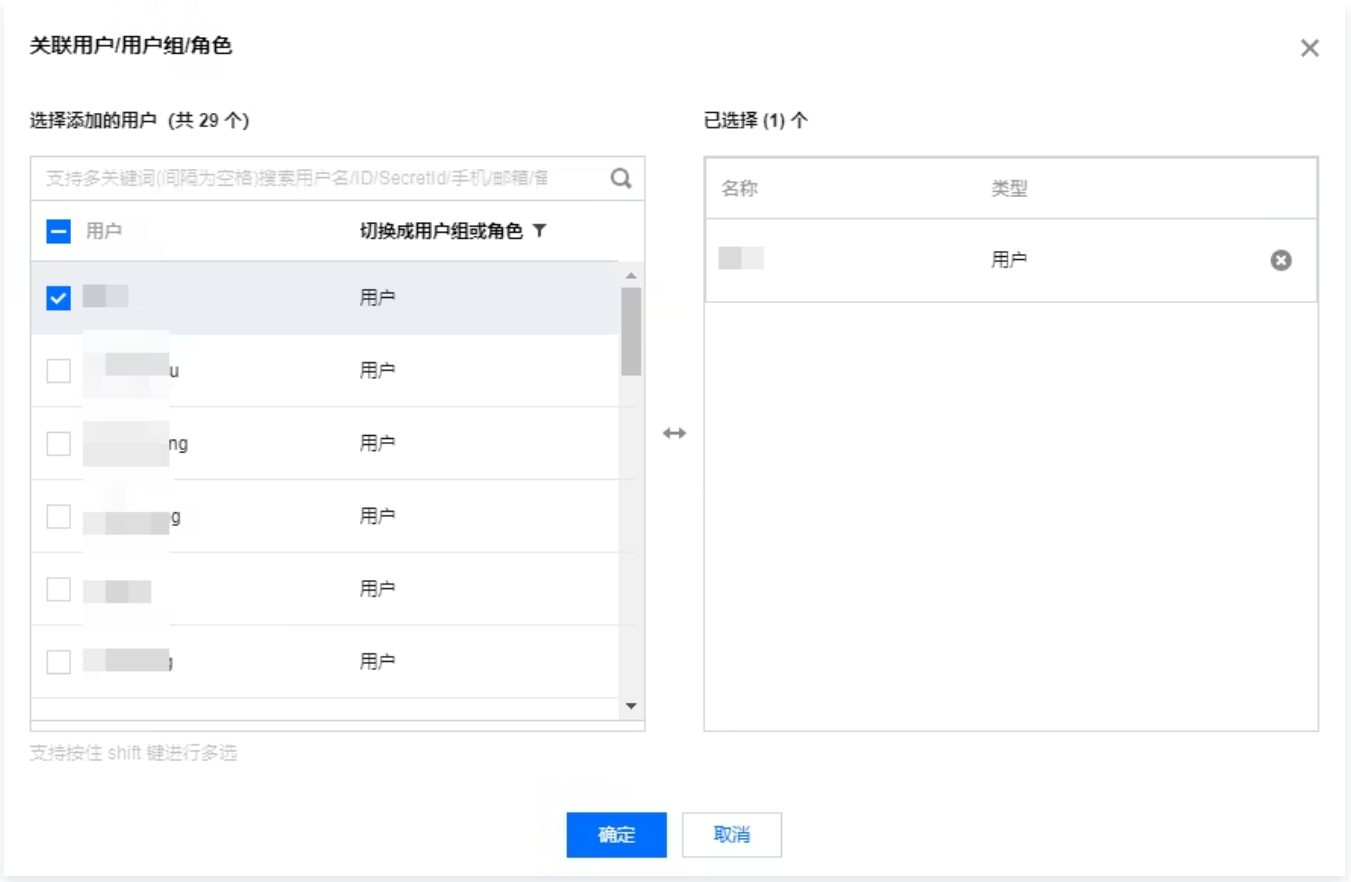
SOC 相关资源的策略

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）
已选择 (1) 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
名称
类型
用户
支持按住 shift 键进行多选
确定
取消

实践教程
等级保护测评解读

最近更新时间：2025-08-29 17:36:01

云安全中心产品符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），云安全中心高级版满足第三级及以下安全要求：

等保标准章节	等保标准序号	等保标准内容	云安全中心对应功能	功能解读
安全区域边界-安全审计	8.1.3.5 a)	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	日志审计	云安全中心可集中存储 xx 时间的日志数据，包含主机安全告警、Web 应用防火墙告警、DDoS 防护告警、云用户操作行为等安全相关日志数据
安全区域边界-安全审计	8.1.3.5 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
安全区域边界-安全审计	8.1.3.5 c)	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	日志审计	云安全中心日志通过多副本实时存储多分，保障用户日志在其存储周期内不丢失、可恢复
安全计算环境-安全审计	8.1.4.3 a)	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
安全计算环境-	8.1.4.3 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息

安全审计				
安全计算环境-安全审计	8.1.4.3 c)	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	日志审计	云安全中心日志通过多副本实时存储，保障用户日志在其存储周期内不丢失、可恢复
安全区域边界-集中管控	8.1.5.4 f)	应能对网络中发生的各类安全事件进行识别、报警和分析	威胁告警	云安全中心可通过威胁分析将全网不同安全产品识别的告警进行分析，并结合威胁情报及事件调查能力，将告警串联起来，形成事件攻击链，帮助安全管理员更好的判断与处置问题