云安全中心

操作指南

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

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

文档目录

操作指南
功能导航总览

最近更新时间：2026-04-30 14:08:12

概览

核心理念：用一张图看清当前安全状态，驱动优先行动。

功能	核心价值
安全评分	综合量化当前云上安全水位，0~100 分直观反映整体风险高低
高危待办清单	自动汇聚最紧迫的风险项，减少人工巡检工作量
安全趋势	周期性风险变化曲线，量化安全运营改善成效

AI 工作台

核心理念：让每位安全人员都拥有一位随时在线的 AI 安全专家。

功能	核心价值
告警智能研判	自动分析告警上下文，给出真实威胁/误报判断，减少人工研判工作量
自然语言操作引导	用对话方式引导用户完成复杂操作，降低产品使用门槛

资产中心

核心理念：安全的起点是知道自己有什么，统一资产基座是一切防护的前提。

功能	核心价值
全景资产总览	跨主机、容器、云产品、AI 资产的统一视图，消除资产盲区
主机资产	管理全量云服务器，实时掌握 Agent 在线状态与防护覆盖率
容器资产	集群与镜像双维度纳管，理清容器化环境的完整资产底数
云资产	自动发现账户下全量云产品实例，为配置检查提供检测基础

风险治理

核心理念：风险治理优先于事后响应，将安全问题消灭在被利用之前。

漏洞治理

持续扫描主机系统与软件漏洞，主机安全（旗舰版）支持**一键修复+自动验证**，实现漏洞从发现到闭环的完整管理。

云安全态势管理

检查云产品配置是否符合安全规范，三个维度全覆盖：

功能	核心价值
云产品配置检查	自动扫描存储桶、安全组、数据库等配置风险，对标行业最佳实践
系统基线治理	主机操作系统安全加固基线检查，为等保合规提供技术支撑
云边界分析	绘制云上网络暴露面，识别不必要的公网开放和横向访问路径

AI Agent

针对 AI Agent 工作流的权限滥用、提示词注入等新型风险进行专项检测与治理。

云 API 风险治理

全量梳理账户下 API 调用行为，识别权限过大、异常调用等 API 安全风险。

数据安全态势（DSPM）

自动发现敏感数据分布，识别数据存储与访问中的安全风险，支撑数据安全合规治理。

检测响应

核心理念：实时感知在途攻击，快速响应将损失降到最低。

功能	核心价值
告警中心	聚合主机入侵、容器逃逸、APIServer 异常等全类型安全告警，统一研判与处置

安全运营

核心理念：安全不是一次性建设，而是持续运营，用数据驱动安全改进。

功能	核心价值
日志分析	集中存储与检索主机、容器操作日志，为事件溯源提供完整证据链

防护配置

核心理念：主动设防，在攻击到达之前建立纵深防护体系。

主机防护

功能	核心价值
勒索监测	实时识别勒索病毒行为特征，配置快照周期策略，保护关键业务数据
核心文件监控	对关键系统文件和配置文件实施防篡改监控，检测异常变更

系统设置

核心理念：统一管理接入、权限与通知，保障平台安全高效运转。

功能	核心价值
通知中心	配置告警通知渠道（邮件/企微/短信），确保安全事件第一时间触达
接入管理	多云多账户接入，统一纳管多个云账户与跨云资产，集团用户一个平台统管全局
授权管理	支持对产品使用授权进行管理

概览

最近更新时间：2026-04-30 14:08:12

本文档将为您介绍安全概览各模块功能及操作步骤。

概述

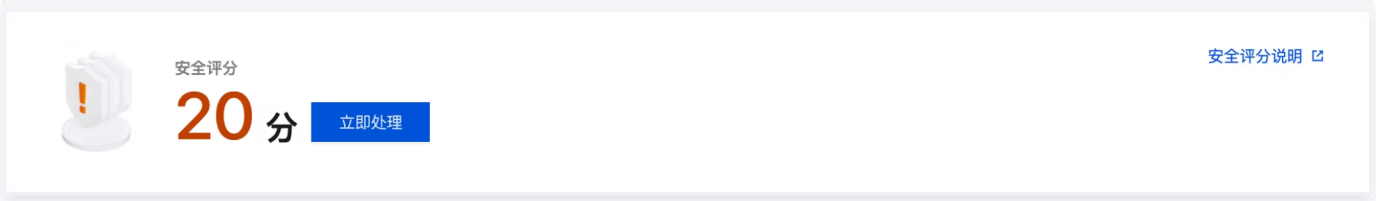
云安全中心的 安全概览 实时展示您的安全评分、待处理风险、安全防护状态、风险趋势以及安全实时动态；推送安全播报，方便您了解最新威胁情报；提供帮助文档和云安全中心升级服务建议，帮助您抵御黑客入侵风险及攻击威胁，保障企业云资产安全。

操作指南

登录 云安全中心控制台，在左侧导航中，单击**安全概览**，进入安全概览页面。该页面提供安全概览信息和相关处理操作，各模块功能说明如下：

安全状态

1. 在安全概览页面，展示您的云安全中心评分和安全风险情况，并提供快捷处理入口。



云安全中心安全评分划分为3个等级：

等级	体检评分	字体颜色	状态说明
优	90分 – 100分	绿色	资产安全状态较好，需继续保持，定期巡检。
中危	60分 – 89分	橙色	资产存在较多安全风险，建议您及时处理安全事件。
高危	20分 – 59分	红色	资产存在严重安全风险，请您尽快处理安全事件。

> **说明：**
> 云安全中心状态体检评分最低分数为 20分。

按安全事件分类计算扣分项，安全事件等级分类及扣分规则：

等级	安全事件（按事件数计算）	扣分/个	叠加最大扣分

严重	木马文件、暴破成功、恶意请求	-40分	-50分
高危	严重漏洞、高危漏洞、严重基线、高危基线、异常登录（高危）、本地提权、反弹 Shell	-10分	-20分
中危	中危漏洞、中危基线	-3分	-10分
低危	低危漏洞、低危基线	-2分	-5分
其他	基础版防护、未安装主机安全客户端	-1分	-5分

2. 在安全概览页面，单击安全评分的**立即处理**，将打开风险处理详情弹框，在风险处理详情页面，可以查看漏洞风险、入侵检测、基线风险和网络风险具体详情。单击对应风险卡片的**立即处理**，页面将跳转至相对应的风险处理界面。
   - 漏洞管理：包括 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，合并统计待处理风险数和受影响主机数。
   - 入侵检测：包括入侵检测模块的7个功能，即文件查杀、异常登录、密码破解、恶意请求、反弹 Shell、本地提权、高危命令，合并统计待处理风险数和受影响主机数。
   - 基线管理：只统计基线待处理风险数和受影响主机数。
   - 网络防御：统计攻击事件待处理风险数和受影响主机数。

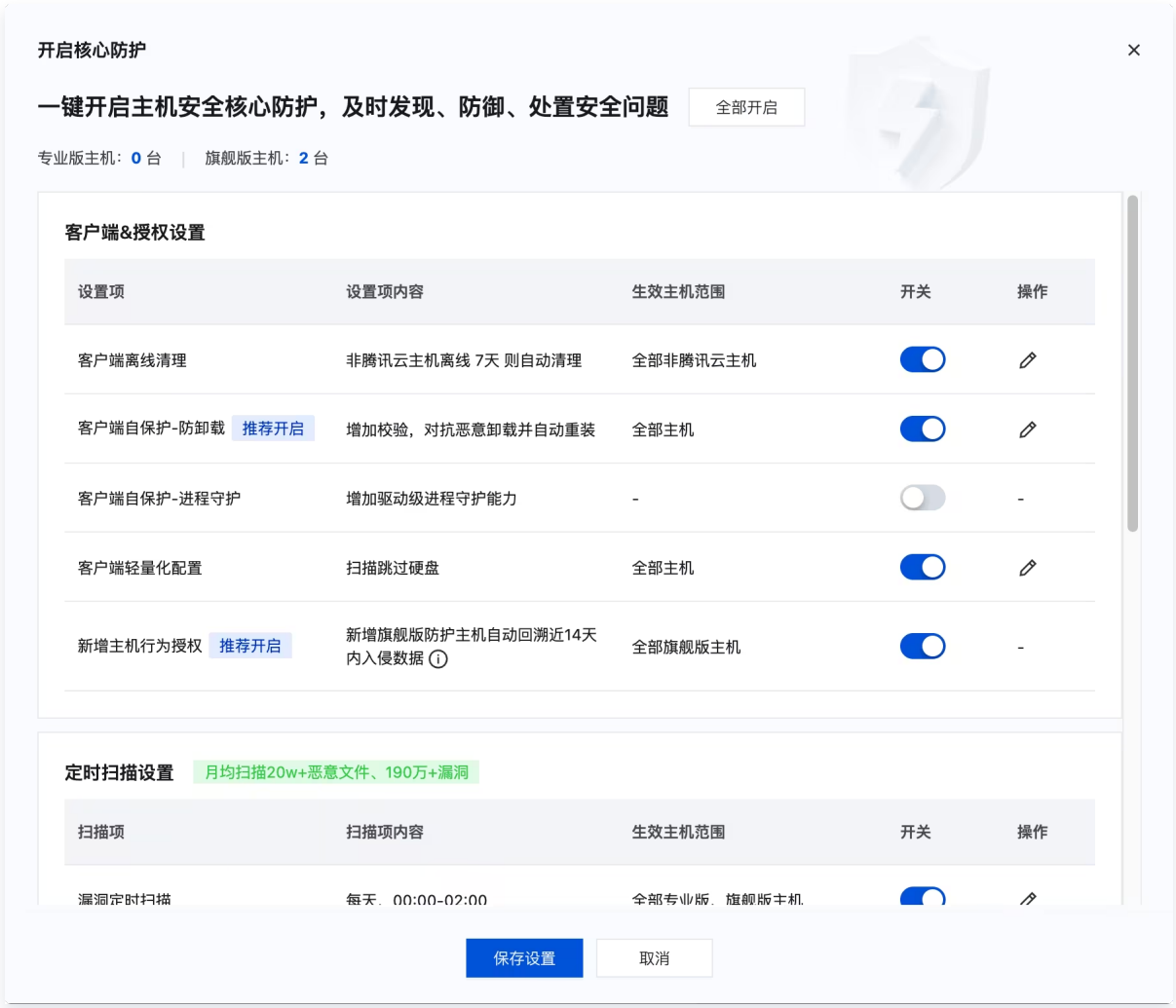
安全播报

在安全播报功能中，展示相关产品功能更新、行业荣誉、紧急通知和版本发布信息。单击**更多**，显示安全播报的每条播报信息。单击**单个播报**内容显示播报详情。

安全开关

1. 安全开关提供云安全中心核心安全功能的统一管理和快速配置。通过安全开关，您可以集中查看和管理云安全中心核心安全功能的开启状态，包含客户端&授权设置、定时扫描设置、自动防御设置。

2. 单击**编辑**，将打开开启核心防护设置弹窗，可以查看主机防护版本分布和授权使用情况、查看各设置项内容和生效主机范围、按需开启/关闭/编辑各项核心防护功能。



防护详情

在防护详情功能中，可查看目前主机总数、在线主机总数量、关机或离线的主机数量、未安装客户端的主机数，目前已防护主机数、旗舰版数量、专业版数量、基础版数量、日志分析使用情况和网页防篡改授权数量，同时提供资产更新时间、病毒库更新时间、漏洞库更新时间以及安全引擎防护等信息。

> **说明：**
> 由于基础版主机防护程度相对较弱，“已防护主机数”仅包含旗舰版与专业版主机。

字段说明：

- 单击右上方**同步资产**，可更新资产信息。
- 在未安装客户端主机中，单击**安装**，界面展示安装引导。
- 在未防护主机数目右侧，单击**升级防护**，将跳转到云安全中心购买页，您可以在购买页购买更多授权，为您的主机提供更为强大的风险威胁抵御能力。
- 安全引擎防护将展示8个引擎图标，分别代表云查杀引擎、BinaryAI 引擎、TAV 引擎、异常行为、威胁情报、攻击防御、泰石引擎、分级告警引擎。若未开启防护功能，对应功能图标处于灰色状态。若有任意一台主机，开通防护功能，则对应功能图标处于点亮状态。

风险趋势

风险趋势功能通过折线图，为您展示近7天、近14天或近30天的安全风险和威胁发生趋势，并且支持按时间段筛选查看。将鼠标在趋势图中悬停，将显示该日期文件查杀、异常登录、密码破解、恶意请求、高危命令、本地提权、反弹Shell、漏洞风险、网络攻击等安全事件数。单击右上角**导出**图标，支持将所选中日期的安全事件数下载至本地。

> **说明：**
> 数据来源为当日新增待处理事件数，每小时更新一次，历史事件数将保留，不再变更。

实时动态

实时动态功能按照时间倒序实时展示发现的主机风险及威胁事件。单击蓝色字段的**主机 IP**，页面跳转至“主机详情页”的相应子页面；单击事件动态右侧的**查看详情**，将跳转至相应事件处理页面。

资产中心
主机资产

最近更新时间：2026-04-30 14:08:12

功能简介

主机资产模块提供主机的统一管控与资产盘点能力。通过主机列表，您可以集中接入和管理主机，可视化掌握主机安全状态并高效响应风险；通过资产概览，您可以从资产维度查看主机资产的概况统计，包括资产趋势、资源监控及 TOP 资产排行等，快速掌握资产全貌；通过资产指纹，您可以查看和管理 16 项关键资产指纹的采集数据，及时了解主机上的软件、进程、端口等资产详情及变更情况。

操作步骤

1. 登录 云安全中心控制台 ，在左侧导览中，单击**资产中心** > **主机资产**。
2. 在**主机资产**页面，可以通过不同菜单切换到不同资产管理模块，具体操作指南如下：

功能名称	功能描述	操作指南
主机列表	主机列表是主机安全服务的核心管控界面，支持集中接入和管理腾讯云主机、非腾讯云主机及多云账号资产。您可以在此查看每台主机的防护状态与安全风险概况，并执行客户端安装、版本升级、标签管理、资产同步、事件调查等操作，帮助安全管理员统一管控主机并快速响应安全风险。	主机列表
资产概览	资产概览从资产维度对主机及各项关键资产指纹进行统计盘点与可视化呈现。页面涵盖资产总量与今日新增概况、主机趋势与标签分布、服务器资源监控（CPU/内存/硬盘）以及各类资产指纹的 TOP 排行，帮助您一目了然地掌握主机资产全貌与资源使用情况。	资产概览
资产指纹	资产指纹通过自动化采集（每 8 小时一次，支持手动触发），对服务器上的 16 项关键资产（包括账号、端口、进程、软件应用、数据库、Web 服务、Jar 包、计划任务、内核模块等）进行全面盘点。支持按指纹分类浏览详情、模糊搜索及数据导出，适用于资产盘点、异常排查、漏洞组件识别及合规审计等场景。	资产指纹

风险治理
漏洞治理

最近更新时间：2026-04-30 14:08:12

漏洞治理旨在帮助客户扫描系统中存在的安全漏洞并提供漏洞信息及修复建议等信息，部分漏洞可开启精准防御、可自动修复。本文档将为您介绍如何进行漏洞治理。

限制说明

- 解锁漏洞治理功能，须至少存在1台专业版/旗舰版主机。
- 漏洞治理范围说明如下：（‘✓’表示支持，‘–’表示暂不支持）。

漏洞治理功能	漏洞类型	Linux 系统	Windows 系统
漏洞扫描 专业版、旗舰版主机适用	Linux 软件漏洞	✓	–
	Windows 系统补丁	–	✓
	Web-CMS 漏洞	✓	✓
	应用漏洞	✓	✓
漏洞防御 旗舰版主机适用	Linux 软件漏洞	–	–
	Windows 系统补丁	–	–
	Web-CMS 漏洞	✓仅支持部分漏洞	–
	应用漏洞	✓仅支持部分漏洞	–
漏洞自动修复 专业版、旗舰版主机适用	Linux 软件漏洞	✓ 仅支持部分漏洞	–
	Windows 系统补丁	–	✓
	Web-CMS 漏洞	✓ 仅支持部分漏洞	✓ 仅支持部分漏洞
	应用漏洞	–	–

- 漏洞扫描和自动修复支持的操作系统，详情如下：

操作系统	系统版本	系统漏洞	应用漏洞/Web-CMS 漏洞
CentOS	CentOS 5	✓	✓

	CentOS 6	✓	✓
	CentOS 7	✓	✓
	CentOS 8	✓	✓
Debian **说明：** 仅支持漏洞扫描，不支持漏洞自动修复。	Debian 8	–	✓
	Debian 9	–	✓
	Debian 10	–	✓
	Debian 11	–	✓
	Debian 12	–	✓
Windows **说明：** 仅支持漏洞扫描，不支持漏洞自动修复。	Windows Server 2008	✓	✓
	Windows Server 2012	✓	✓
	Windows Server 2016	✓	✓
	Windows Server 2019	✓	✓
	Windows Server 2022	✓	✓
Ubuntu	Ubuntu 16.04	✓	✓
	Ubuntu 18.04	✓	✓
	Ubuntu 20.04	✓	✓
	Ubuntu 21.04	✓	✓
	Ubuntu 22.04	✓	✓
	Ubuntu 24.04	✓	✓
Tlinux/TencentOS	Tlinux	–	✓
RockyLinux	RockyLinux	–	✓
OpenCloudOS	OpenCloudOS	–	✓

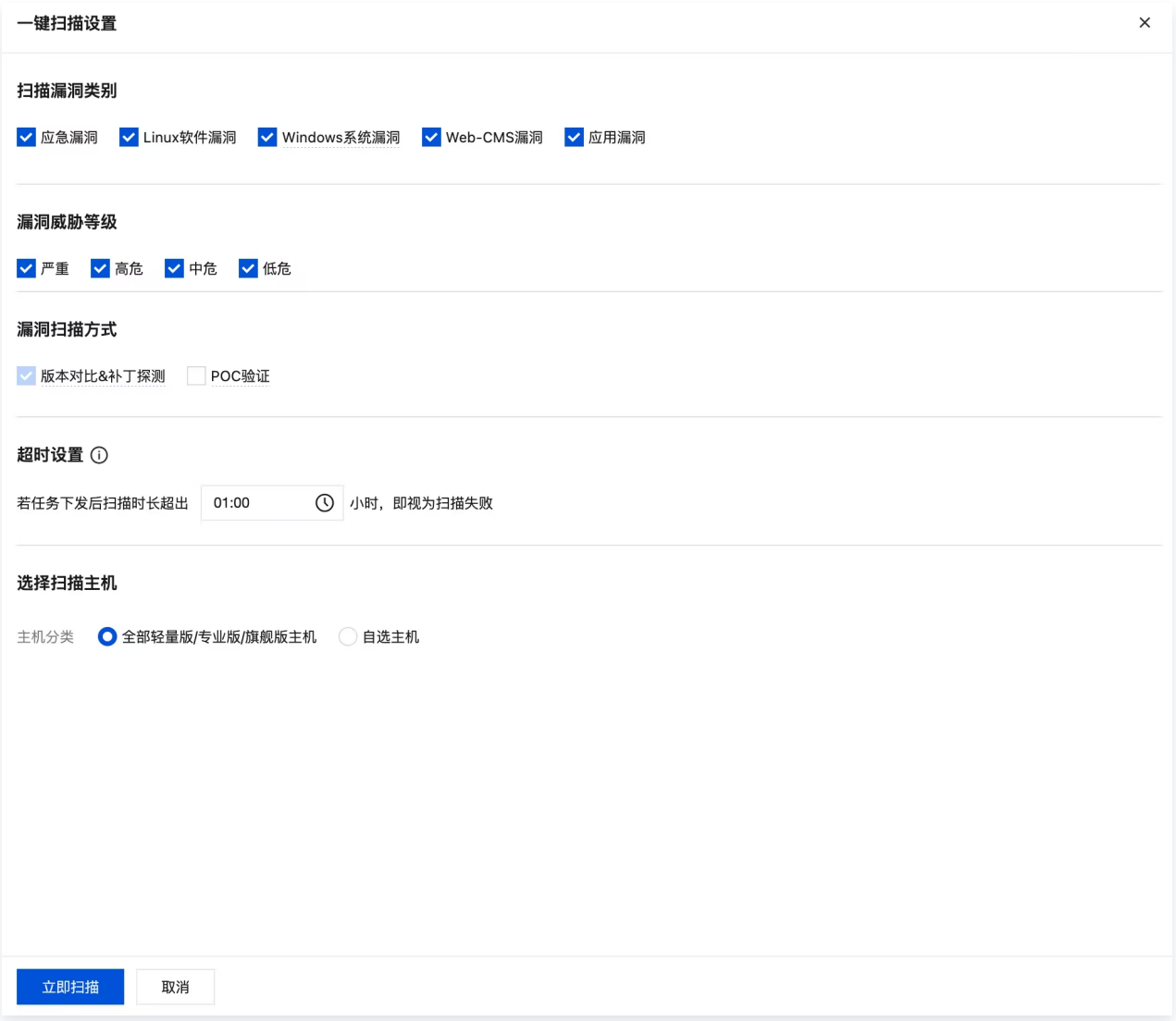
- 为避免修复操作影响用户业务，漏洞修复不会在检出漏洞后立即自动执行，须由用户评估风险后，主动单击**修复并完成数据备份**，才会启动自动化修复流程。具体操作详情请参见 漏洞自动修复文档 。
- 操作系统生命周期限制。针对已进入停更状态的操作系统（即官方已停止更新的操作系统的版本），云安全中心将不再提供停更时间之后新出现漏洞的扫描和修复支持。停更时间前出现的漏洞仍会得到支持，已支持漏洞的范围也不受影响，停更系统列表如下：

操作系统版本	官方停止更新时间
Windows Server 2003	2015年07月14日
Windows Server 2008	2020年01月14日
Windows Server 2008 R2	2020年01月14日
Windows Server 2008 SP2	2020年01月14日
Windows Server 2012	2023年10月10日
Windows Server 2012 R2	2023年10月10日
Ubuntu 12.04 LTS	2017年04月28日
Ubuntu 14.04 LTS	2019年04月
Ubuntu 16.04 LTS	2021年04月
Ubuntu 18.04 LTS	2023年04月
CentOS 5	2017年03月31日
CentOS 6	2020年11月30日
CentOS 7	2024年6月30日
CentOS 8	2021年12月31日

漏洞扫描

1. 登录 云安全中心控制台 ，在左侧导览中，单击**漏洞管理**。
2. 在漏洞扫描模块中，支持一键扫描、定时扫描设置。

- **单击一键扫描，将打开一键扫描设置弹窗，您可对本次扫描的漏洞类别、漏洞威胁等级、超时设置、扫描主机范围进行设置。**



- **单击扫描设置，将打开漏洞设置弹窗并锚点至定时扫描，您可对定时扫描开关、扫描漏洞类别、漏洞威胁等级、漏洞扫描方式、定时扫描周期、扫描主机范围进行设置。**

- 单击**详情**可查看上一次扫描的详情，并支持下载 PDF 扫描报告、Excel 扫描结果。

应用防护

1. 在应用防护模块中，支持查看已开启防护的资产、防御成功次数及防御趋势情况。

> **说明：**
> 应用防护针对 Linux 系统主机（JDK 版本 ≥ 1.6.0），提供 0day 应用漏洞防御、内存马防御能力，支持精准漏洞与通用漏洞攻击检测防御，监测面更广、规则更精准。无需修改应用程序代码或重新部署，推荐重保场景及热门应用漏洞防御场景使用。

2. 单击**前往防护配置**将打开**应用防护 > 防护开关配置**，您可设置应用防护的开关、查看可防御漏洞、选择防御主机范围、查看防御插件详情。

> **注意：**
> 开启应用防护时，将会有短暂的资源占用升高（平均1~2分钟），建议您避开业务高峰时期，分批开启。

漏洞处置

1. 在漏洞治理页下方，您可查看当前检出漏洞的统计情况及详细漏洞列表。
2. 在漏洞概览模块中，展示了漏洞检出情况、网络攻击事件次数及今日新增情况，并展示了云安全中心漏洞库总数。

字段名称	字段说明
高优修复漏洞	该分类下展示热度攻击漏洞，以及严重/高危漏洞，需要优先修复处理，默认统计待修复漏洞数量。单击自定义规则可对高优修复漏洞进行自定义规则判定。
全部漏洞	检出 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞的数量总和。
影响主机	检出漏洞的主机数量。
网络攻击事件（近1月）	统计近1个月内网络攻击事件的数量。
已支持漏洞	可查看云安全中心支持检测的漏洞库，每日最多可检索25次，单次搜索最多可展示100条结果。

3. 在漏洞列表模块中，展示当前检出的具体漏洞，已分为应急漏洞、全部漏洞2类，二者功能无太大差异，下面以全部漏洞举例，为您介绍漏洞处置。

> **说明：**
> - 应急漏洞：专为新发现、影响广、危害高的紧急漏洞而设，相当于一份重点漏洞走查清单，用户可对其发起手动扫描或设置定期扫描，以确保及时响应高危风险。
> - 全部漏洞：汇总展示所有检测到的服务器漏洞，涵盖从低危到严重的全部威胁等级，包含已检测到的应急漏洞。

字段名称	字段说明
漏洞名称/	漏洞名称指当前检出的漏洞，标签指该漏洞的标签（如：远程利用、服务重启、存在 EXP

标签	等）。
检测方式	版本对比、POC 验证。
漏洞类型	Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞。
威胁等级	严重、高危、中危、低危。
全网攻击热度	高、中、低、无热度。
CVSS	指通用漏洞评分系统的评分，分数范围从0到10，0代表最不严重，10代表最严重。
CVE 编号	公共漏洞暴露库中，识别该漏洞的唯一编号。
最后扫描时间	最近一次扫描到该漏洞的时间。
影响主机	存在该漏洞的主机数量。
处理状态	待修复、修复中、扫描中、已修复、已忽略、修复失败。
自动修复状态	暂不支持修复、可自动修复（无需重启）、可自动修复（需重启）。
操作	• 一键修复：部分 Linux 软件漏洞、Web-CMS 漏洞支持自动修复，可单击**一键修复**打开漏洞详情弹窗，选择需要修复的主机进行修复，详情请参见 漏洞自动修复 。 • 更多：重新扫描（重新对该漏洞进行扫描）；忽略漏洞（对该漏洞进行忽略，后续不再对该主机扫描该漏洞）。

云安全态势管理
云资源配置检查

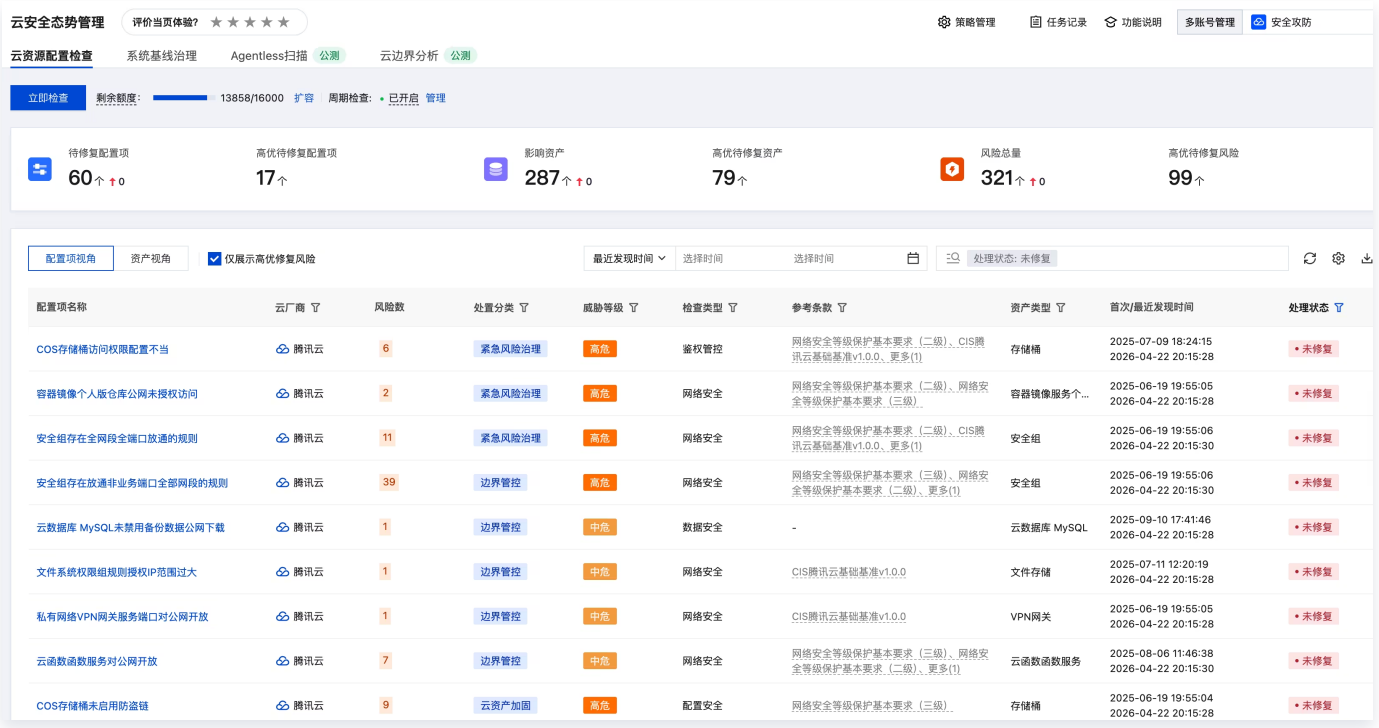
最近更新时间：2026-04-30 14:08:12

功能介绍

云资源配置检查功能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。

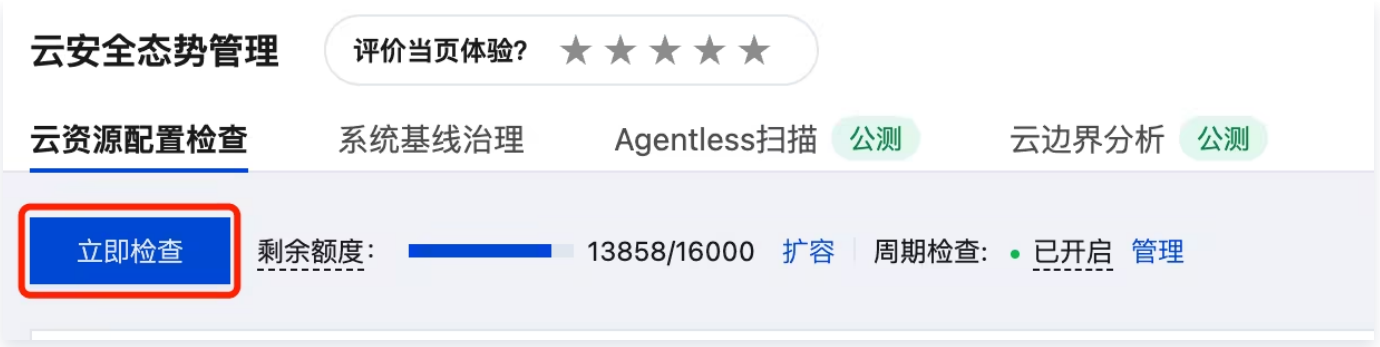
访问入口

1. 登录 云安全中心控制台，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理 > 云资源配置检查**中，支持查看云资源配置风险。



发起风险检查

1. 登录 云安全中心控制台，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理 > 云资源配置检查**中，单击**立即检查**。



3. 在弹出的对话框中，可以选择不同的检测模式。检测模式支持全量规则、免费规则、按周期计划已选规则、自选规则4种不同场景。可以查看对应配额的预期消耗情况。

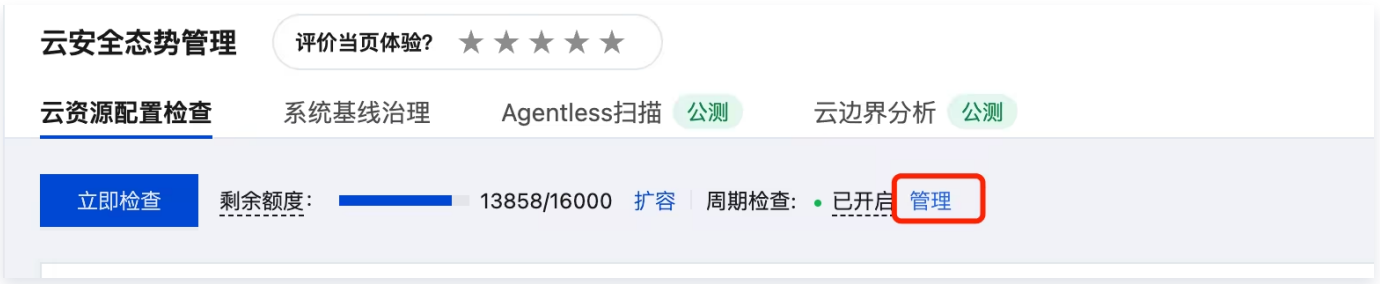
> **注意：**
> 在执行云资源配置检查时，会进行一次资产的同步，因此，实际消耗的额度预期有微小差异。

4. 鼠标移至**立即检查**上方，您可以看到最近一次检测任务的运行时间。

周期检查管理

云资源配置检查支持周期自动检查，需要您手动开启配置。

1. 登录 云安全中心控制台 ，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理** > **云资源配置检查**中，单击**管理**。



3. 在弹出的抽屉中，单击**开关**，完成周期检查启用。

4. 您还可以单击**周期运行**中的**编辑**，来调整执行时间。

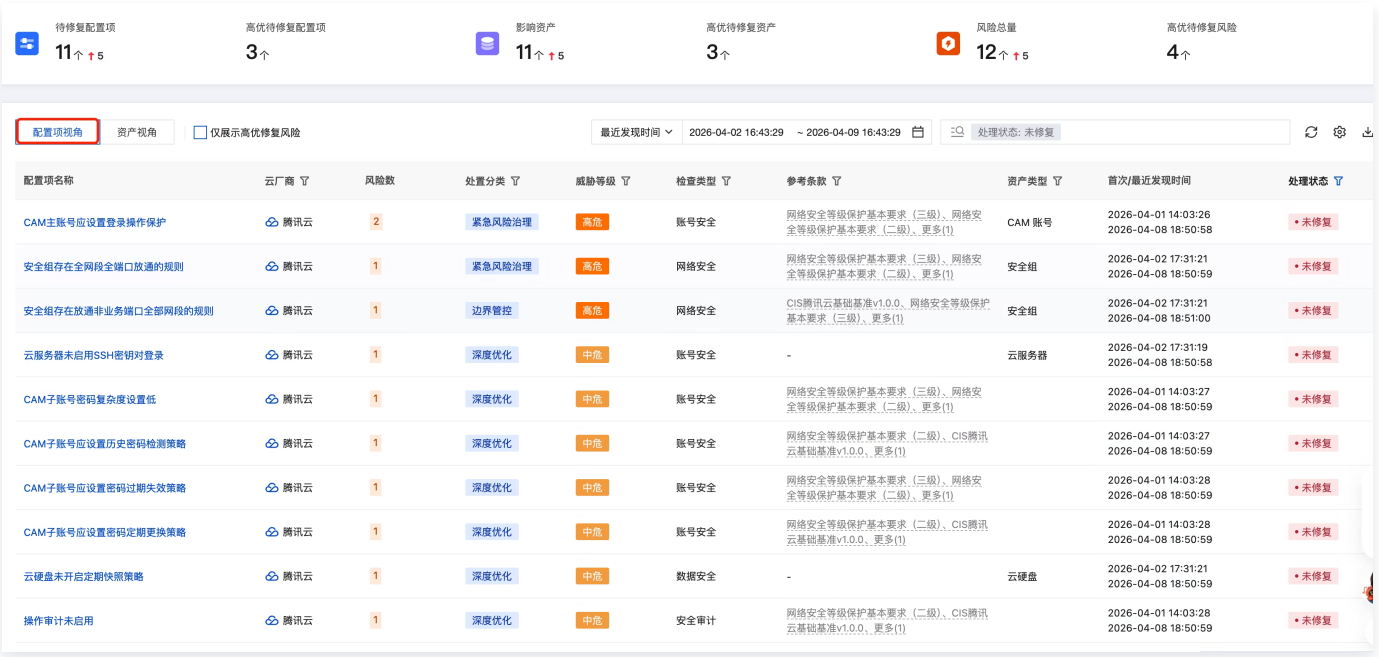
5. “新增规则自动启用”功能说明，当该功能处于启用状态时，云安全中心新增的检查规则将自动加入您的执行列表；当该功能处于关闭状态时，云安全中心新增的检查规则将不会加入您的执行列表。该功能默认启用，且建议您将该功能保持开启状态，能及时发现新风险。

6. 通过控制**开关**，可以调整您希望执行的规则列表。支持检索、批量操作。

配置项视角

在配置项视角中，您可以查看按规则名统计的风险情况。

1. 登录 云安全中心控制台，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理 > 云资源配置检查**中，选择**配置项风险**。



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. 您可以根据首次发现时间、最近发现时间、处理状态、风险等级和云厂商、威胁等级筛选数据。系统会将风险与 CIS 基准、网络安全等级保护基本要求等参考条款进行关联，并提供检索功能。
6. 选择目标数据，单击**配置项名称**，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。

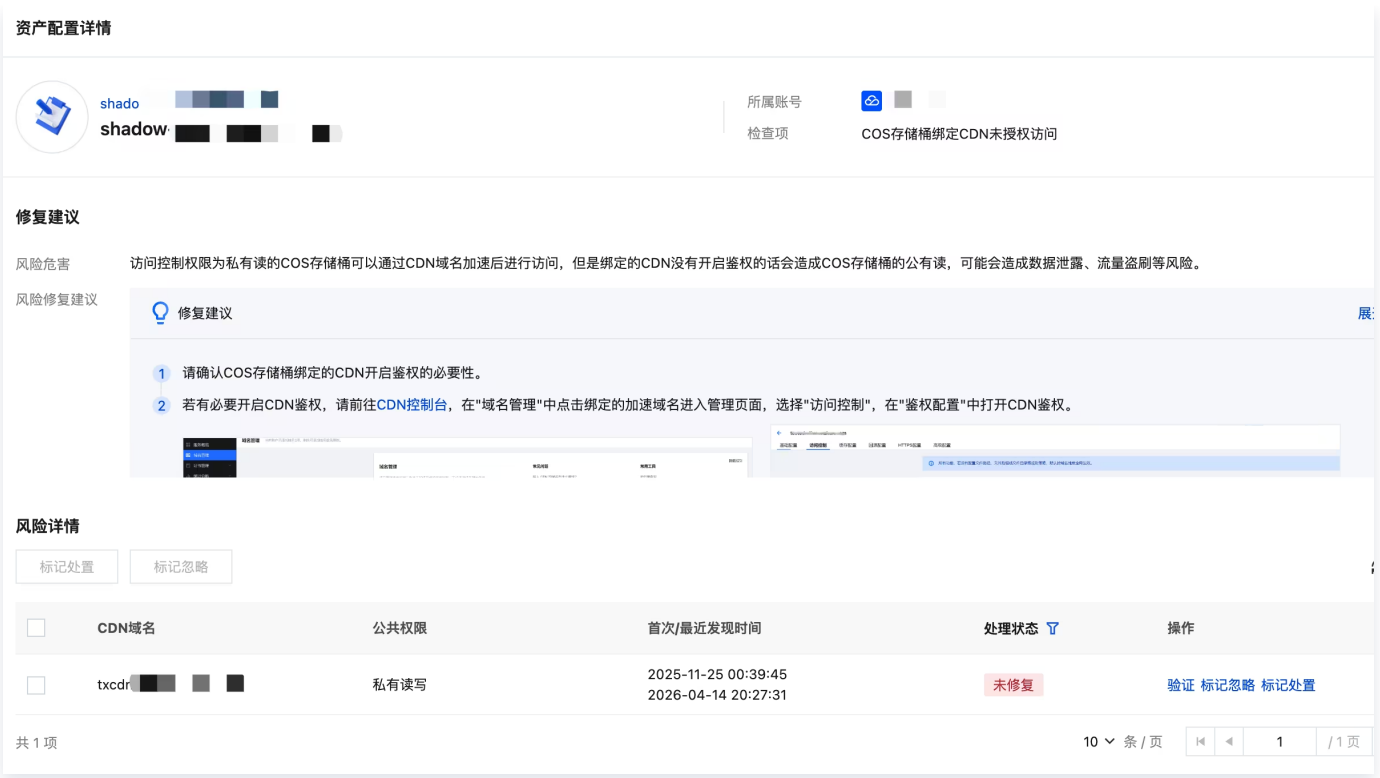
资产视角

1. 登录 云安全中心控制台 ，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理** > **云资源配置检查**中，选择**资产视角**。

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. 您可以根据首次发现时间、最近发现时间、处理状态、威胁等级和云服务提供商筛选数据。系统会将风险与 CIS 基准、网络安全等级保护基本要求等参考条款进行关联，并提供检索功能。
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。

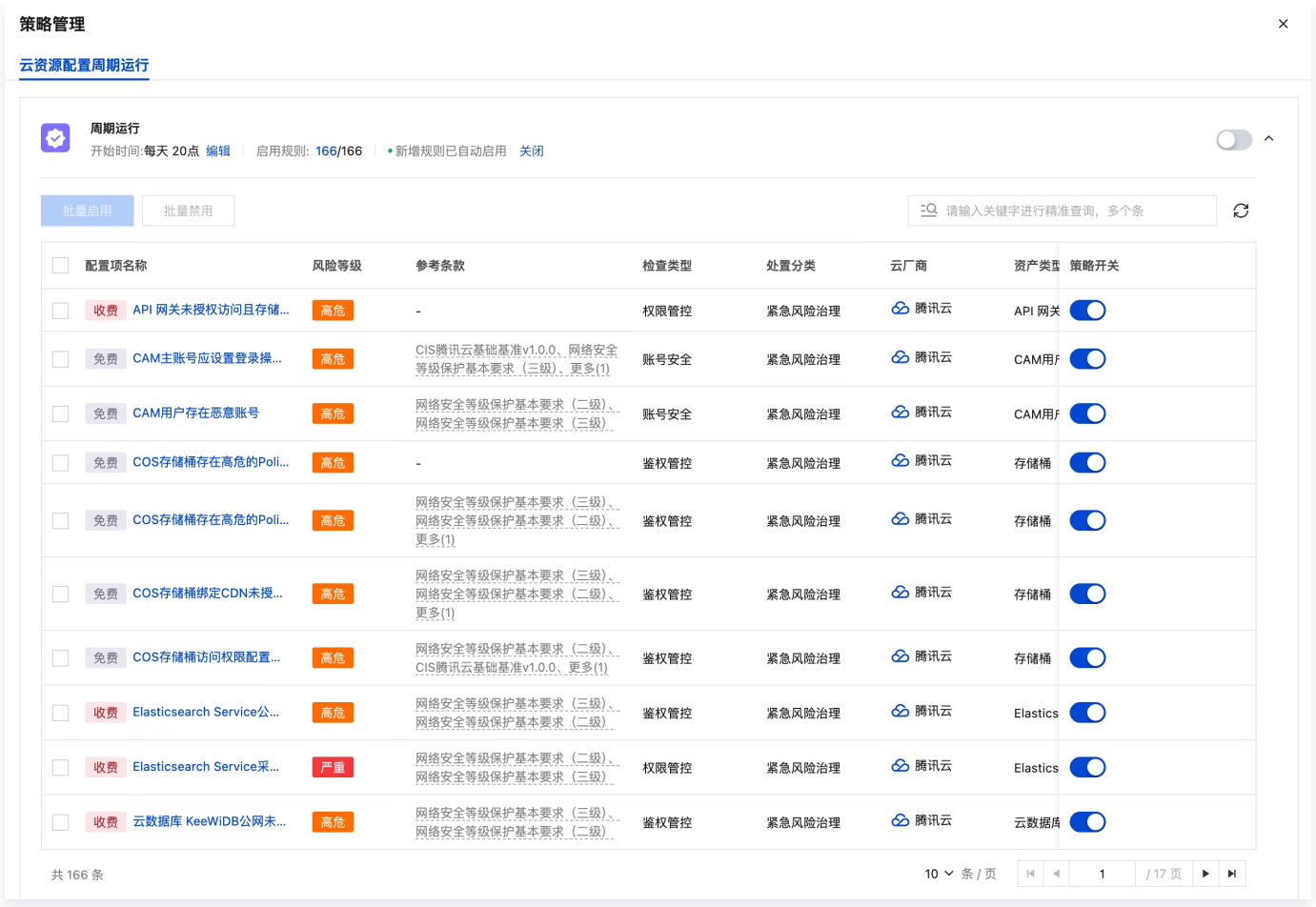
7. 在详情页面，您可以查看风险危害、风险修复建议、风险详情。



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。

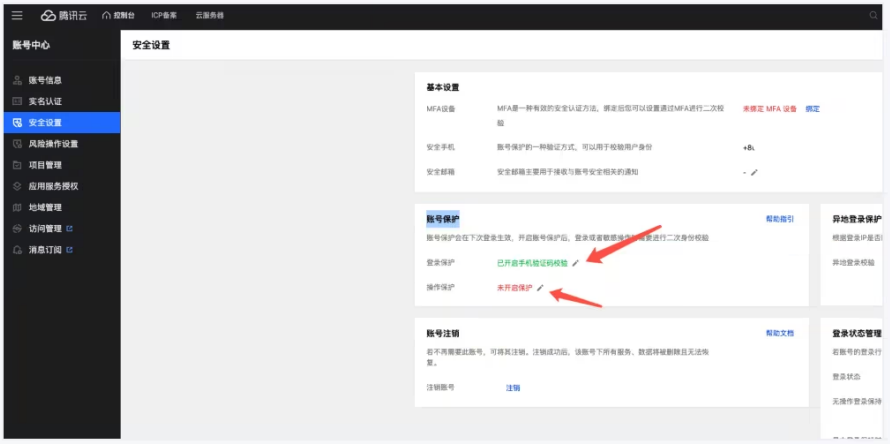
策略配置

1. 登录 云安全中心控制台 ，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理** > **云资源配置检查**中，单击左上角的**策略配置**
3. 在策略管理中，您可以查看风险配置项列表，也可以选择规则进行禁用。



4. 单击**目标配置项名称**，通过弹框方式展示该配置项风险的危害和修复建议，帮助您了解该配置项。

配置项详情

风险危害	CAM主账号未设置登录和操作保护，一旦攻击者登录到控制台，将可以任意操作账号下资产，对账号下的资产造成危害。
风险修复建议	修复建议 1 登录账号中心控制台，在安全设置 页面，账号保护区域，点击登录保护、操作保护设置按钮。  2 选择启用MFA设备校验、或开启手机验证码校验、或开启微信扫码验证，单击确定，完成设置。 

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

云边界分析
功能简介

最近更新时间：2026-04-30 14:08:12

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。云边界分析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。

前提条件

面向已购买 主机安全（旗舰版）的客户开启公测，公测结束时间以官网公告为准。

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。根据网络状态可分为：

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。

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

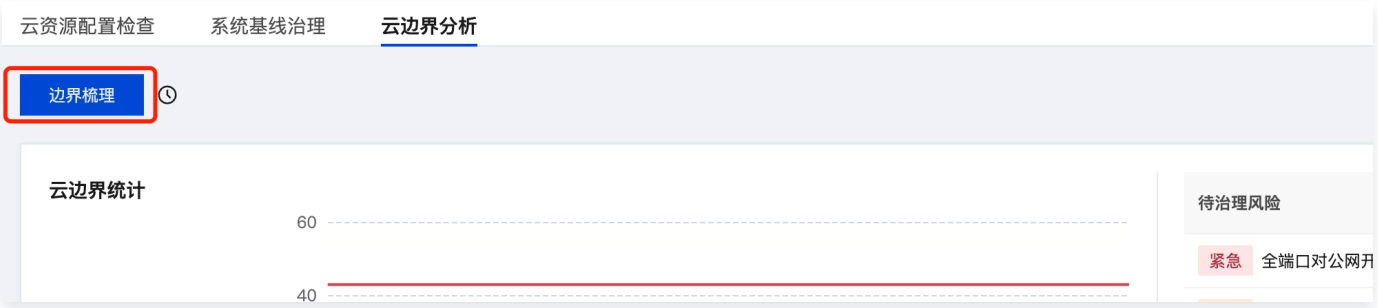
1.1.1.1	80	无法访问

> **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、以及云服务器的安全组规则。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**云安全态势管理**。
2. 在**云安全态势管理** > **云边界分析**中，支持查看相关数据内容。

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。



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了云厂商官网文档。

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

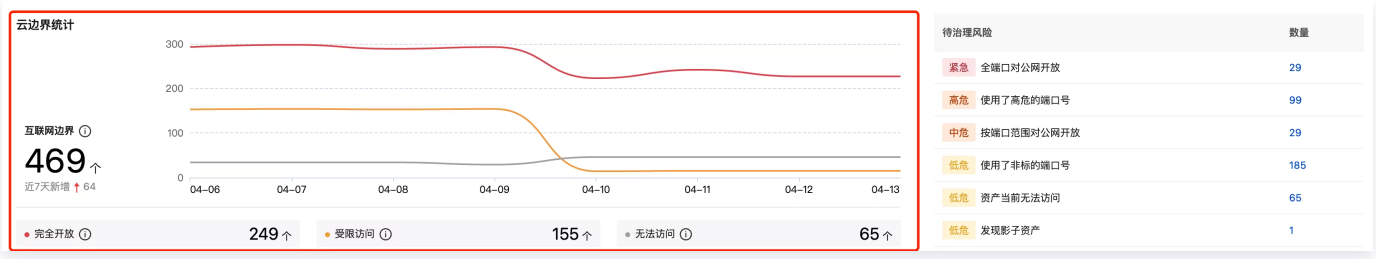
查看统计面板

最近更新时间：2026-04-30 14:08:12

云边界统计

1. 登录 云安全中心控制台 ，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理** > **云边界分析**中，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。

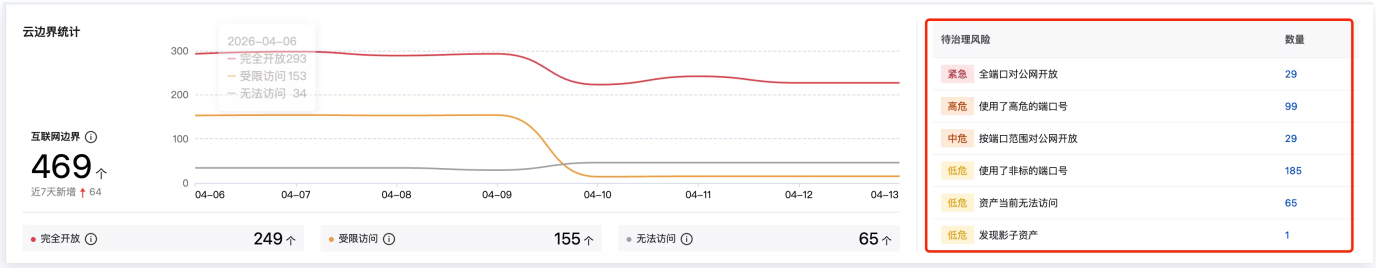


3. **功能交互**：单击4个**统计数据**，将在下方**边界列表**内，展示具体的结果。下图是单击**云边界统计**面板中“**受限访问**”对应数字的展示结果。

4. **云边界数量趋势图**：展示了近7天边界数量的整体趋势。

待治理风险

1. 登录 云安全中心控制台，在左侧导览中，单击**云安全态势管理**。
2. 在**云安全态势管理 > 云边界分析**中，统计面板右侧即**待治理风险**。



3. 选择对应的风险，单击**数量**即可查看该风险对应的内容。

查看边界列表

最近更新时间：2026-04-30 14:08:12

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**云安全态势管理**。
2. 在**云安全态势管理** > **云边界分析**中，支持查看云上边界列表的详细列表。

   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结果，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，仅允许白名单里的地址访问该端口。 • **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。
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。
首次/最近发现时间	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。

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。

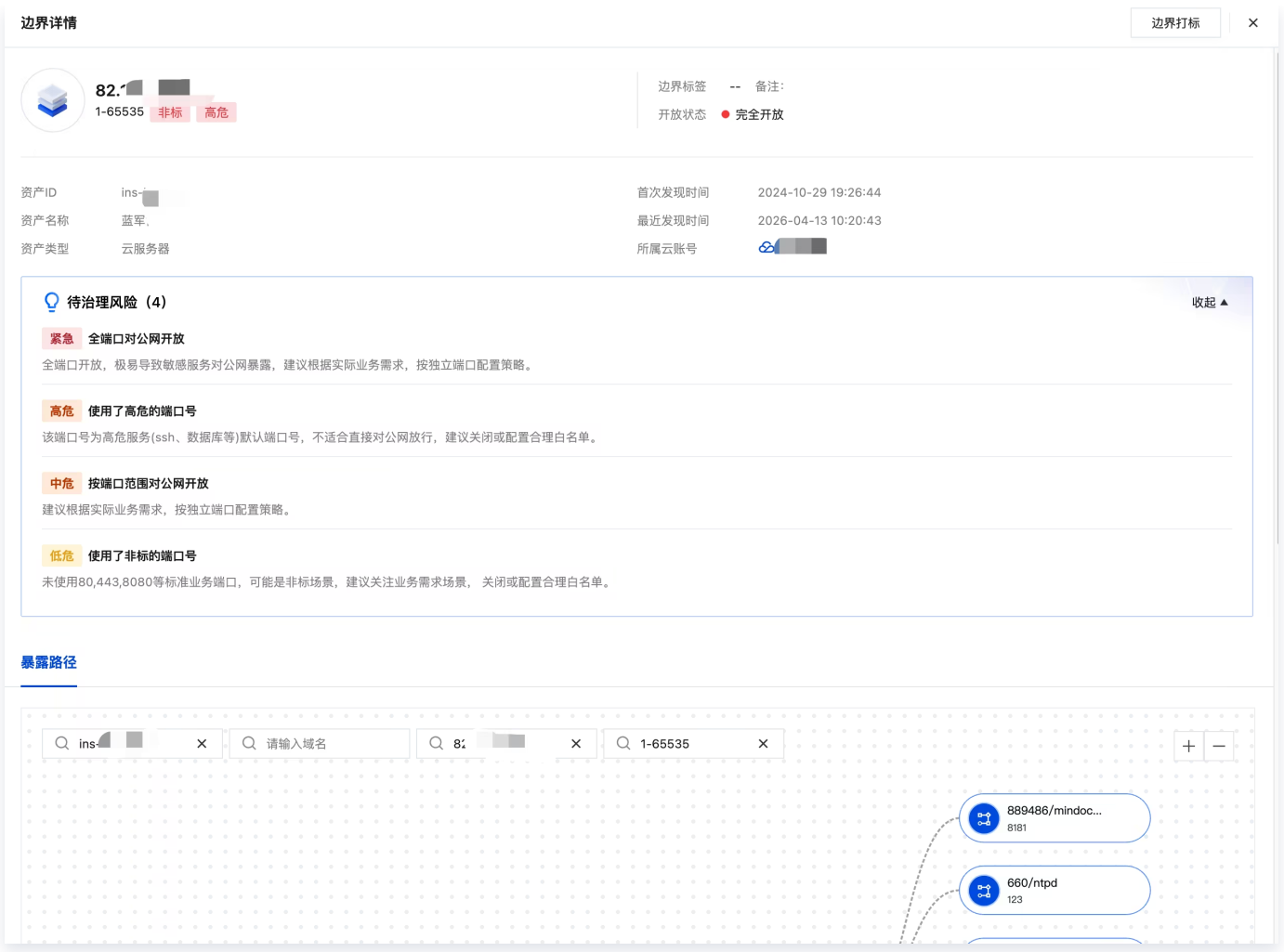
4. 选择目标数据，在**边界标签**处，单击**编辑**，即可对该数据进行打标签，系统将边界数据分为合理业务、需要收敛、临时开放三种类型，方便您持续治理云边界。

5. 单击右侧的**导出**，可以导出数据，格式是 Excel。

边界详情

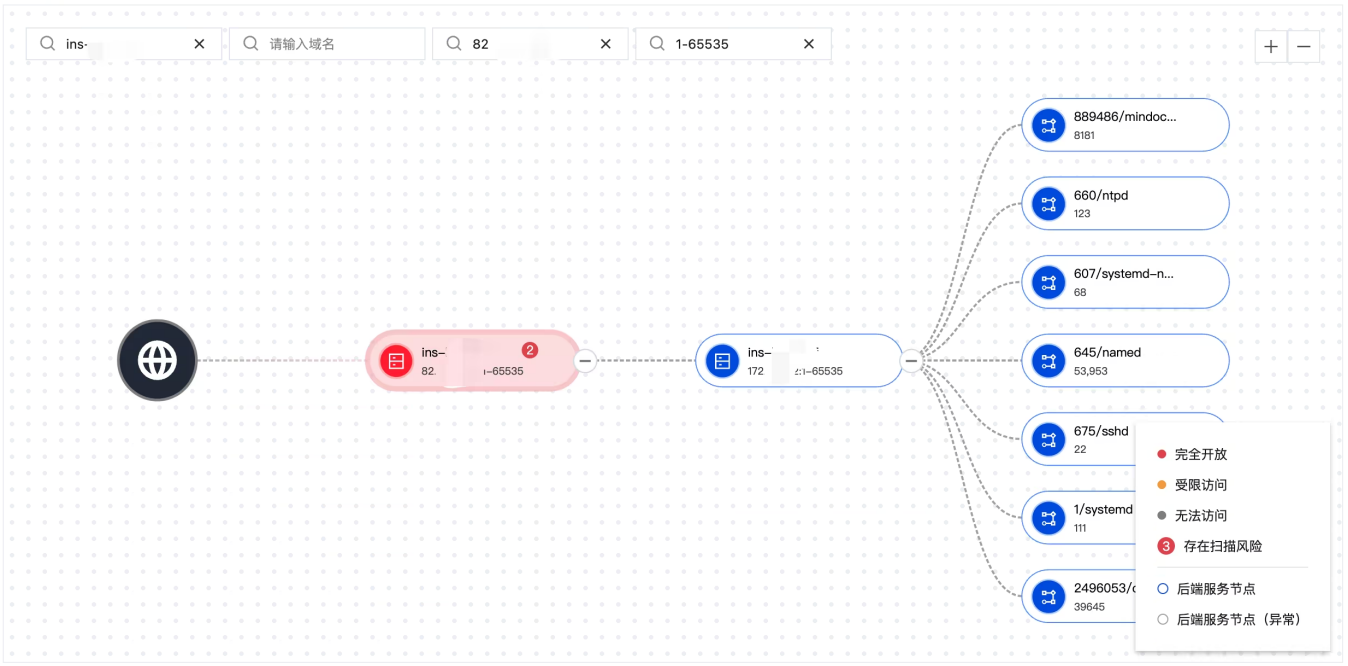
1. 登录 云安全中心控制台 ，在左侧导览中，单击**云边界分析**。
2. 在**云安全态势管理** > **云边界分析** > **边界列表**中，选择目标数据，单击**详情**。

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. **下方暴露路径**，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，请参阅相关 文档 。

暴露路径



互联网节点（1） 后端服务节点（1） 主机列表（1） 主机进程（34） 主机风险（872）

检索暴露路径

最近更新时间：2026-04-30 14:08:12

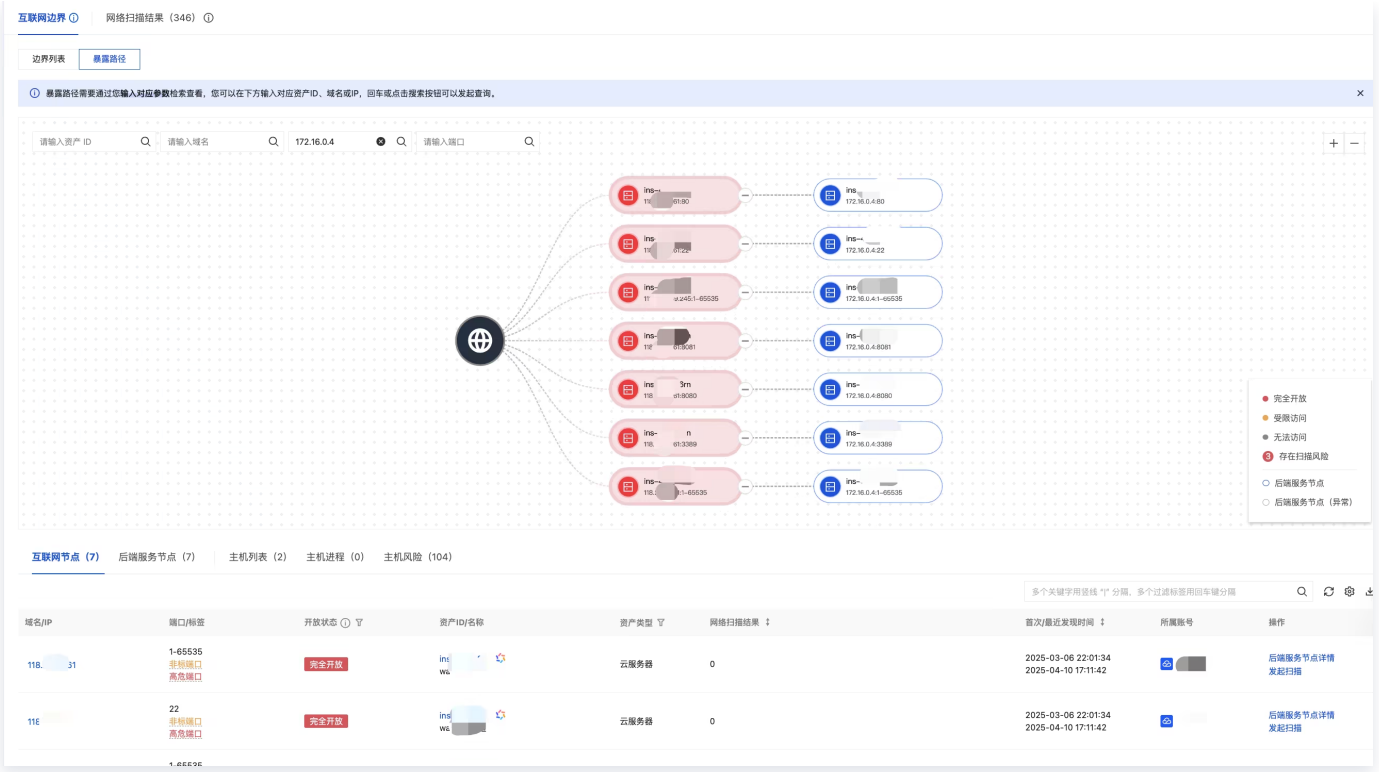
功能介绍

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类产品，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（例如：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**云安全态势管理**。
2. 在**云安全态势管理** > **云边界分析** > **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。

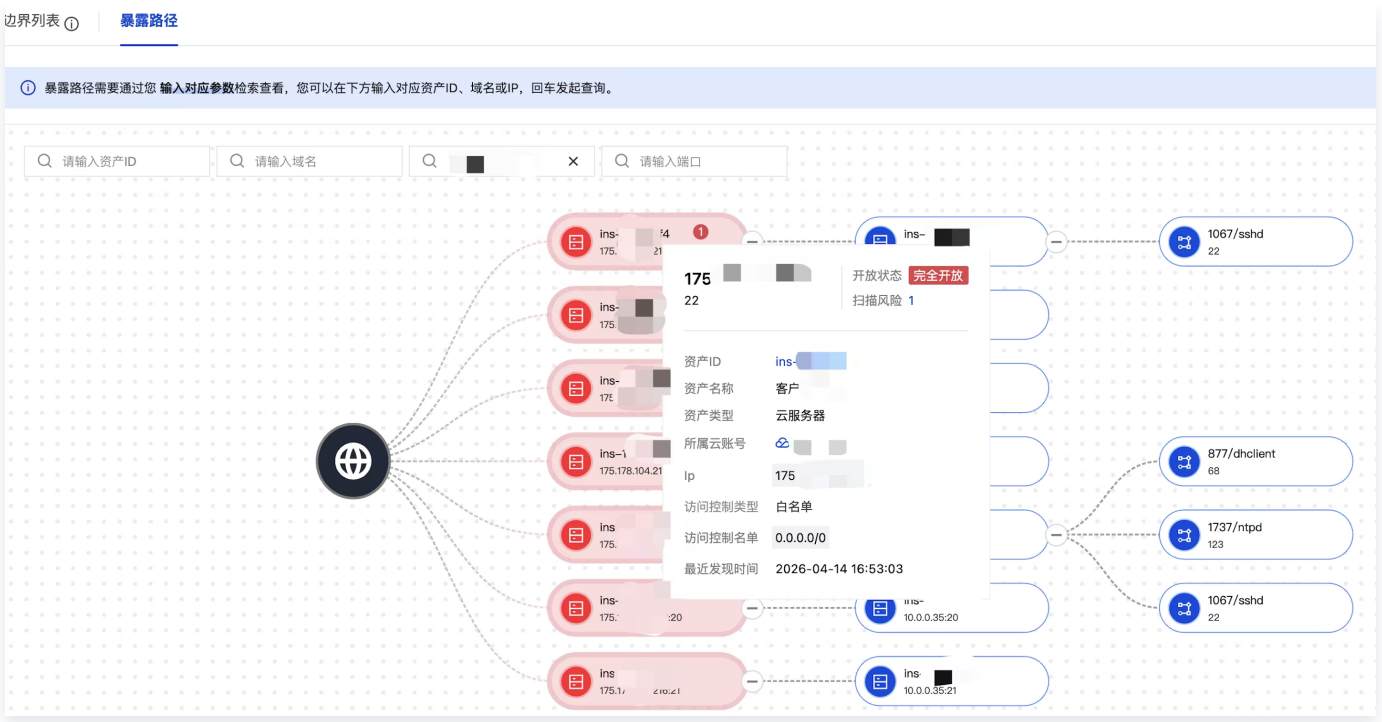


暴露路径树状图

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

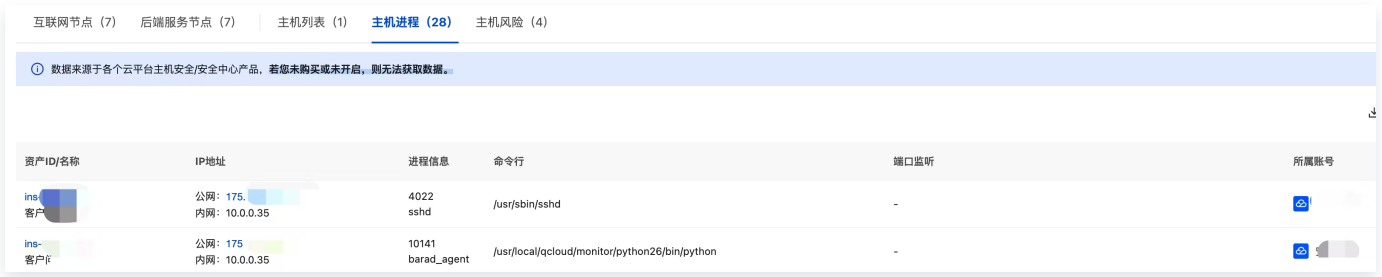
在暴露路径中，云安全中心将根据暴露路径的节点信息提供更详细的数据展示。

- 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：展示通过主机列表及安全防护状态、漏洞与高危基线风险数据。

- 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。

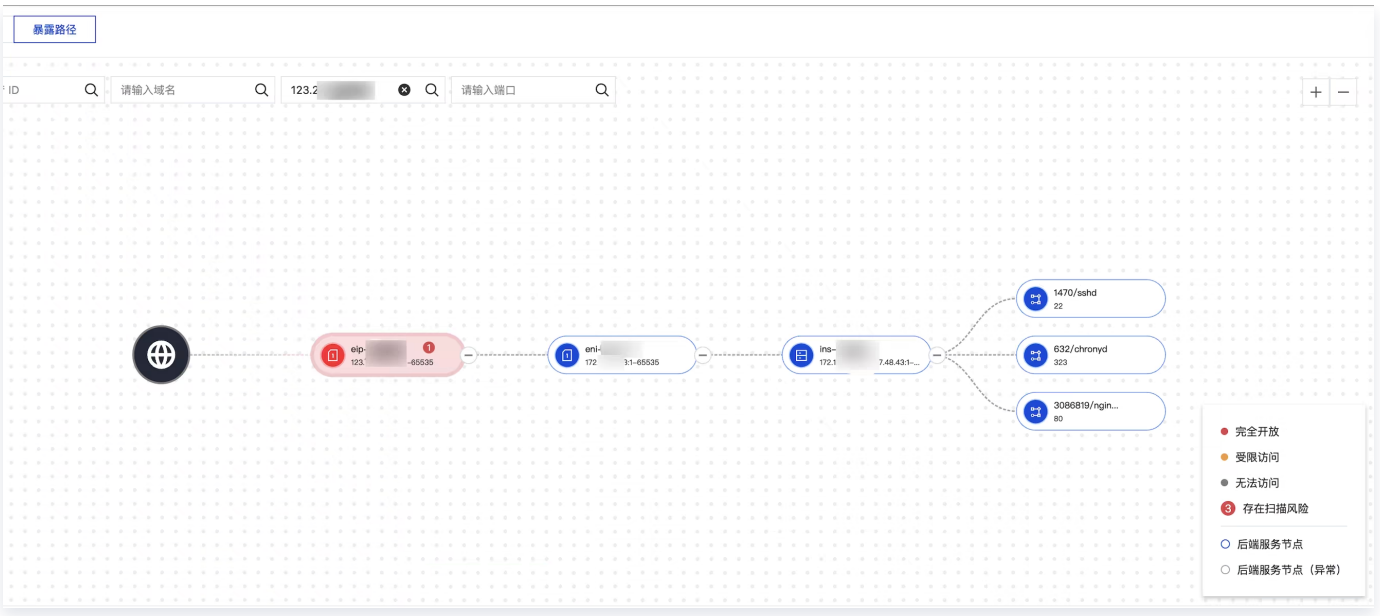


- 主机风险列表：分为主机漏洞、高危基线风险。高危基线风险包含弱口令检查、未授权访问等。

暴露路径示例解读

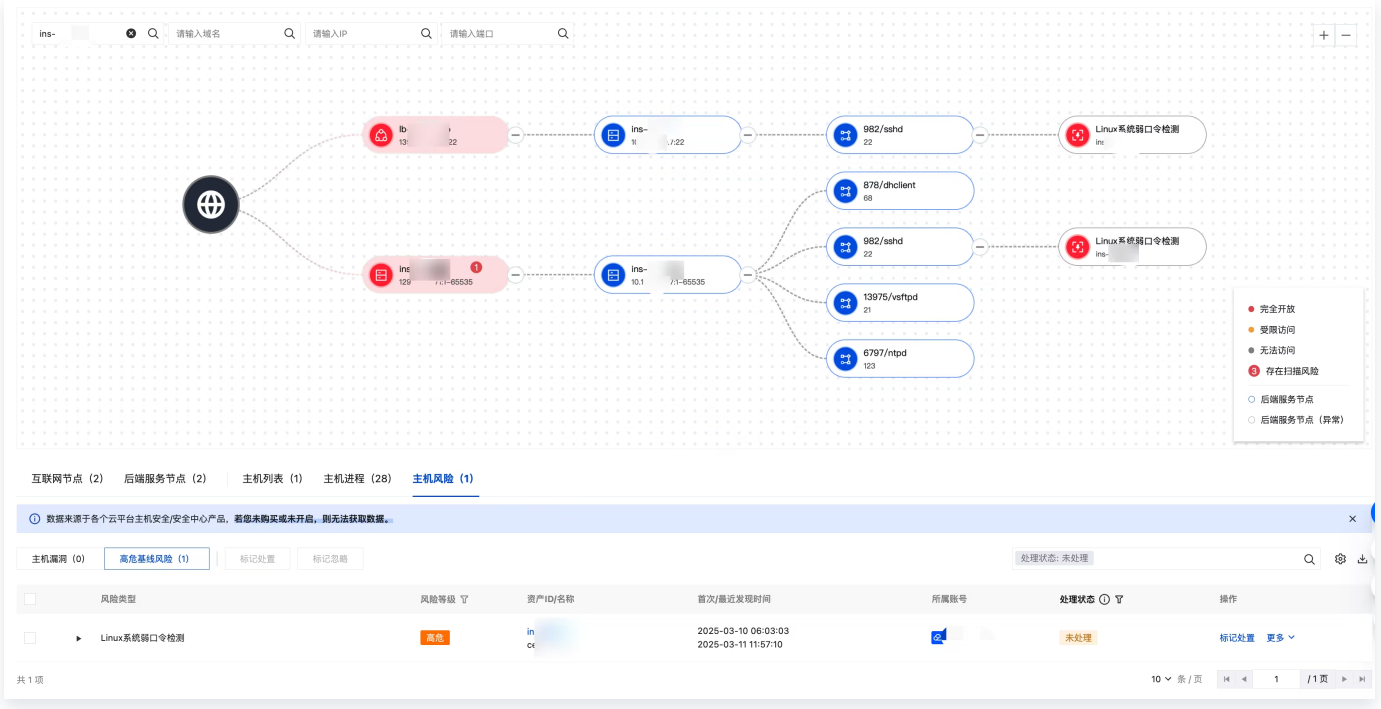
下图的路径关系如下：

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。

数据安全态势管理
对象存储风险监测
功能简介

最近更新时间：2026-04-30 14:08:12

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，这个 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	异常访问	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
	恶意文件	实时监测增量文件中的恶意文件，若存储桶存在恶意文件，将产生恶意文件告警。	通过恶意文件识别，第一时间发现恶意文件上传威胁，降低数据泄露、病毒感染风险。	
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。		
	数据识别策略	针对对象存储的敏感数据识别策略配置	通过敏感数据识别，可以帮您摸清存储中的数据分布，避免因敏感数据违规存储、泄露带来的合规风险。	

统计面板

最近更新时间：2026-04-30 14:08:12

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
建议立即处理资产	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。
建议加固资产	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，包含异常访问、恶意文件等类型的告警事件数量。
   - **风险：**统计全部待处理的风险，包含风险资产数量及风险对应的安全等级等信息。
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：2026-04-30 14:08:12

资产列表模块是对象存储异常监测的核心资产管理区域，分为对象存储资产、调用源 IP、关联 AK 三个核心子模块，集中展示纳管资产的详细信息、风险状态等。本文将为您详细描述相关操作：

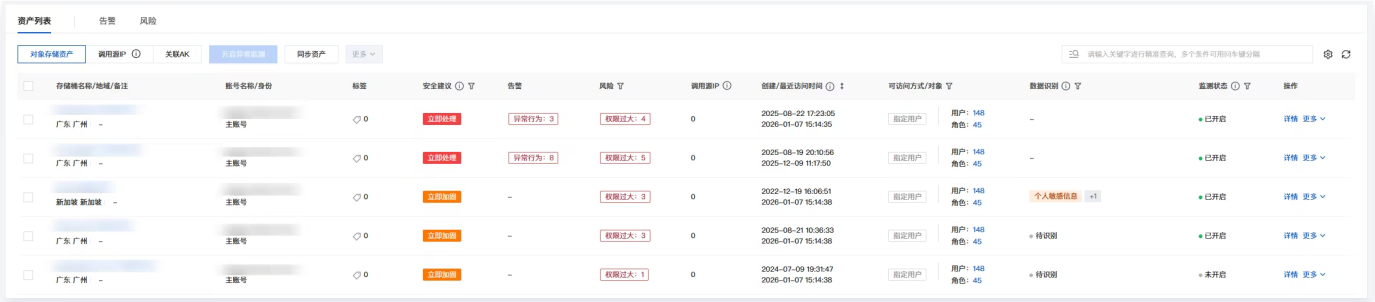
资产视角	说明
对象存储资产	以对象存储资产（存储桶）为核心资源维度，整合来源 IP、关联 AK 对该资产的访问数据，提供资产访问拓扑可视化、IP / 账号精准打标及安全策略快速调整能力，实现对访问目标端的集中精细化管控。
调用源 IP	以访问发起端的调用源 IP 为核心管控维度，整合该 IP 对对象存储资产的访问数据，提供访问拓扑可视化、IP / 账号精准打标及 IP 隐藏 / 访问控制策略快速调整能力，实现对访问发起端的集中精细化管控。
关联 AK	以访问身份凭证的关联 AK 为核心管控维度，整合 AK 对对象存储资产的访问数据，提供 AK 权限分析、调用行为审计及 AK 禁用 / 权限调整策略快速配置能力，实现对访问身份的集中精细化管控。

对象存储资产

对象存储资产展示已同步纳管的所有对象存储桶（存储桶 / 地域 / 备注）的全维度信息，是资产安全态势监控的核心页面：

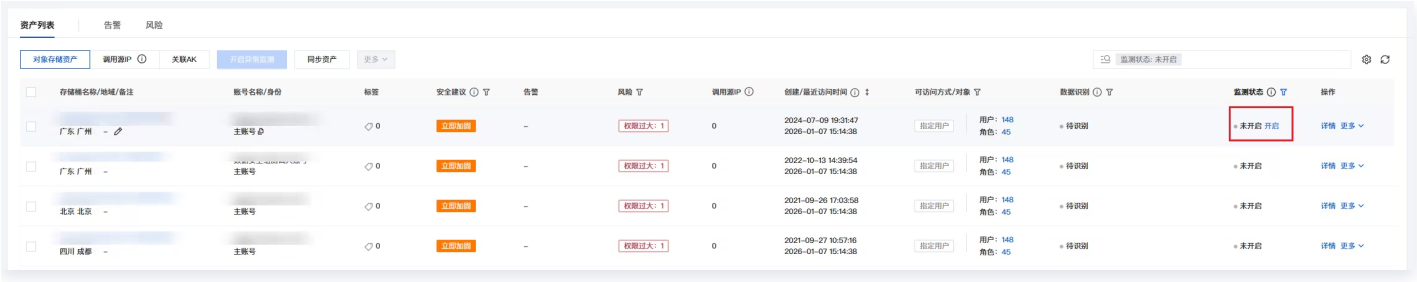
对象存储资产列表

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。



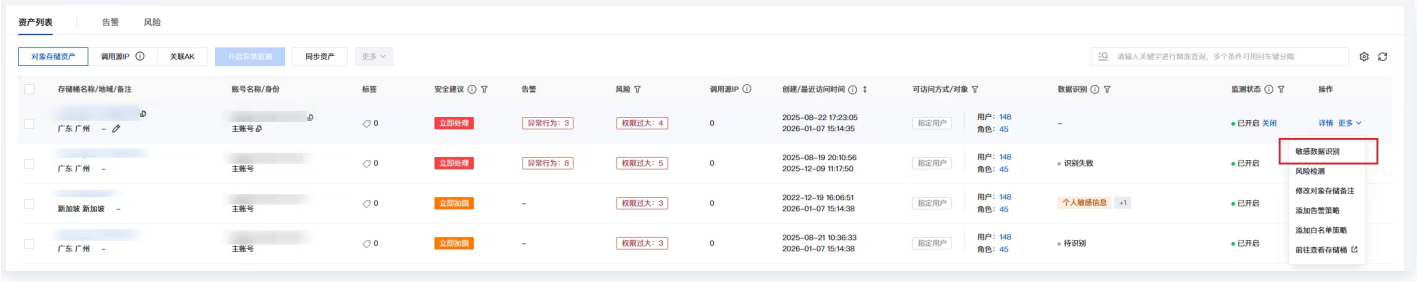
开启异常监测

实时监测异常行为，若存储桶调用行为触发已开启的告警策略，将产生异常行为告警。
在对象存储资产页中，选择所需开启异常检测的资产，单击检测状态列的**开启**。即可开启异常检测



开启敏感数据识别

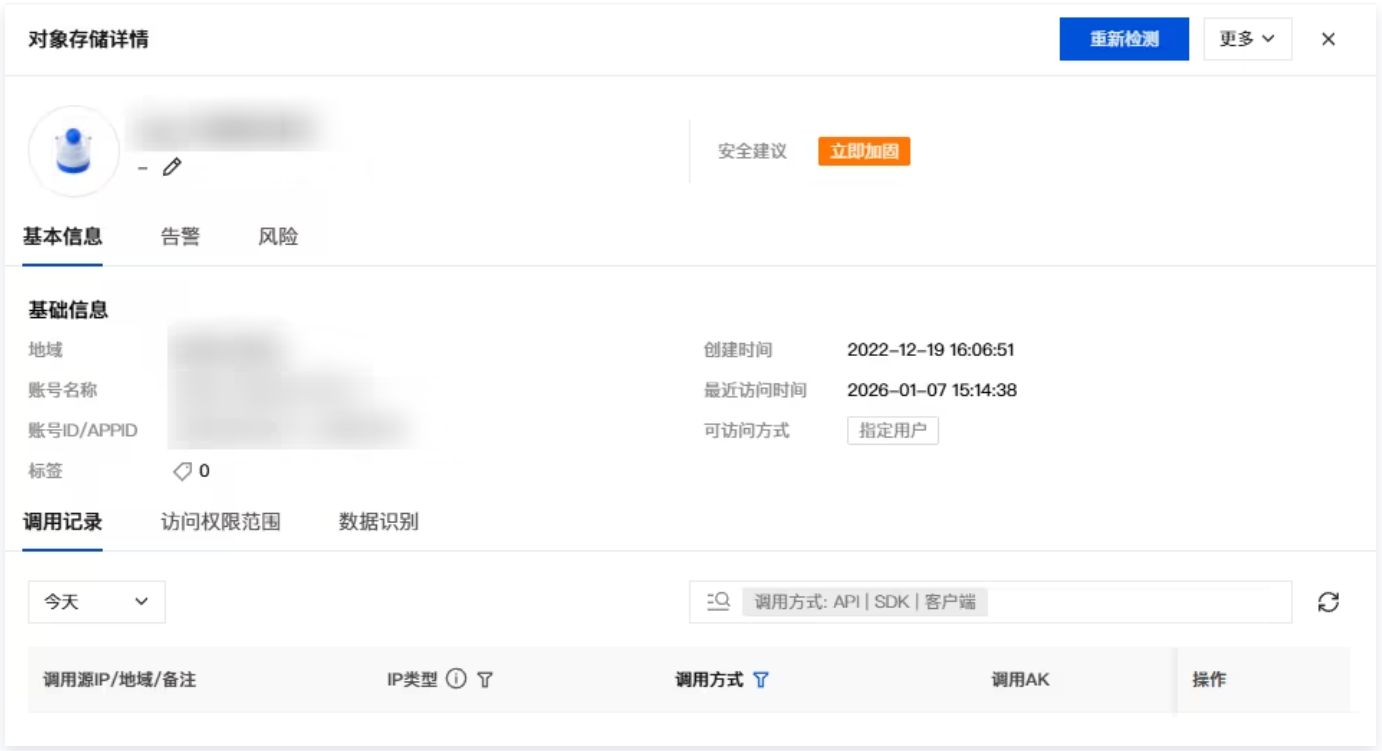
在对象存储资产页中，选择已开启异常检测的资产，单击操作列的**更多 > 敏感数据识别**，即可创建开启敏感数据识别。



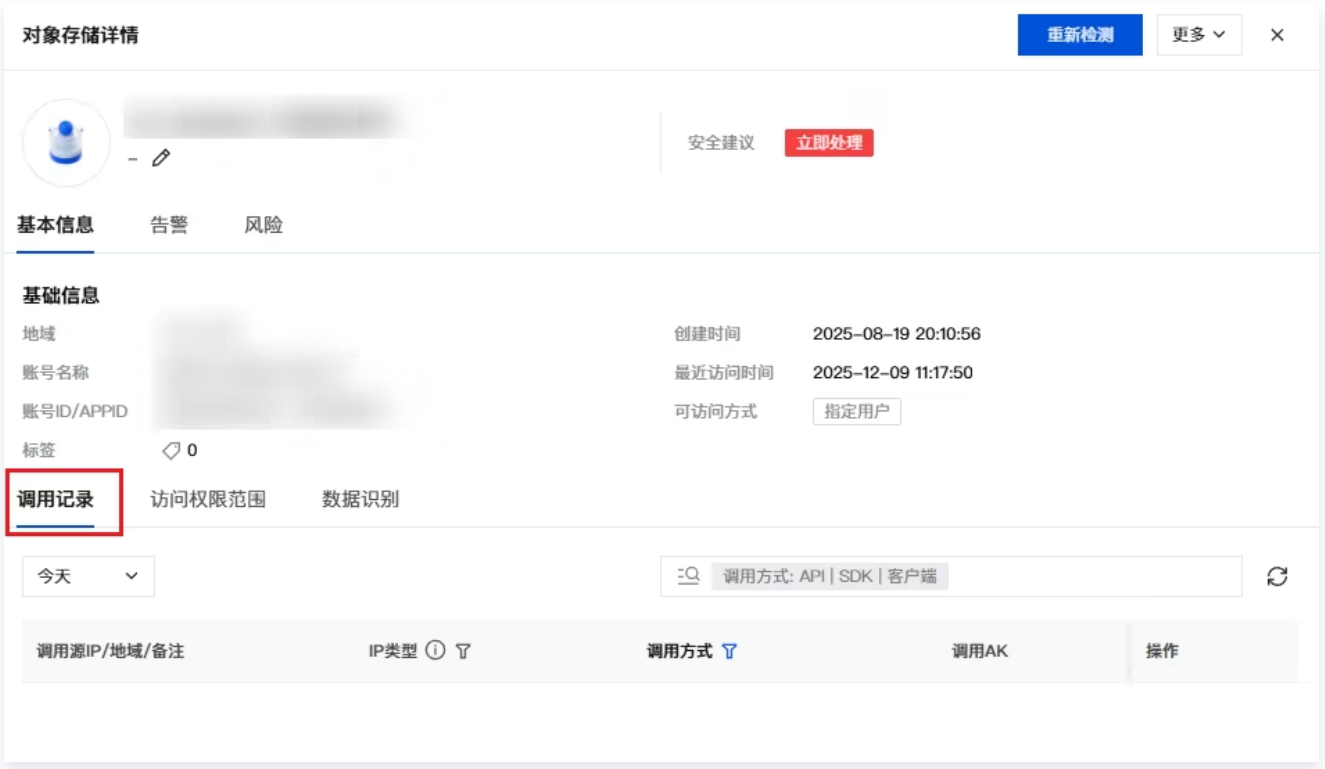
对象存储详情

1. 在对象存储资产页中，选择所需资产，单击**详情**。

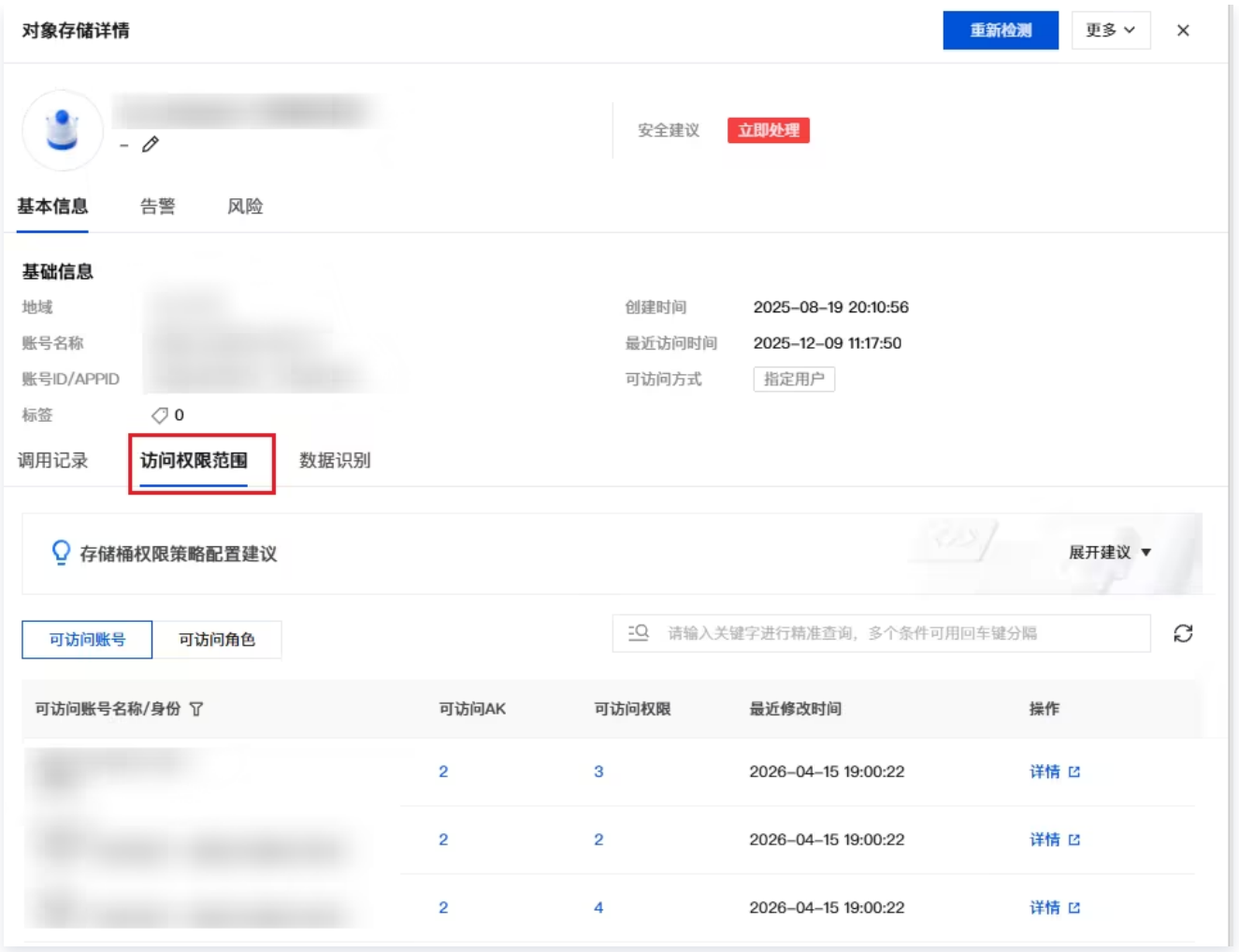
2. 在对象存储详情页面，您可以查看当前对象存储资产的基本信息、调用记录、访问权限范围以及关联的告警风险详情。通过该页面，您可以针对性地进行数据安全治理。
3. 在对象存储详情页面，单击**基本信息**，可查看存储桶基本信息，包括地域、账号名称、账号 ID/APPID、标签、创建时间、最近访问时间、可访问方式。



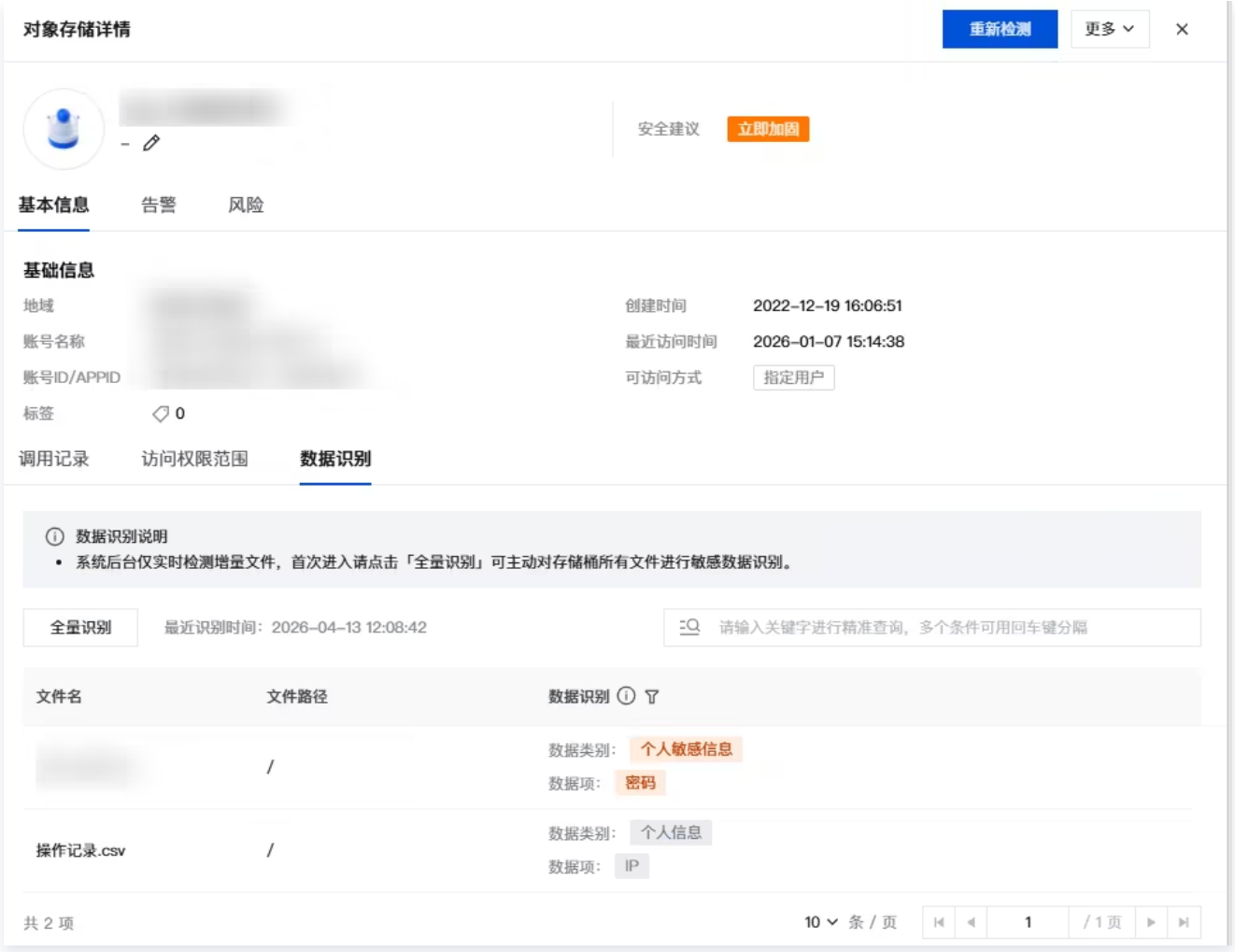
- 在对象存储详情页面，单击**基本信息 > 调用记录**，可查看当前对象存储资产的调用记录，包括：调用源 IP/地域/备注、IP 类型、调用方式、调用 AK、操作动作、操作状态/次数、首次/最近调用时间。



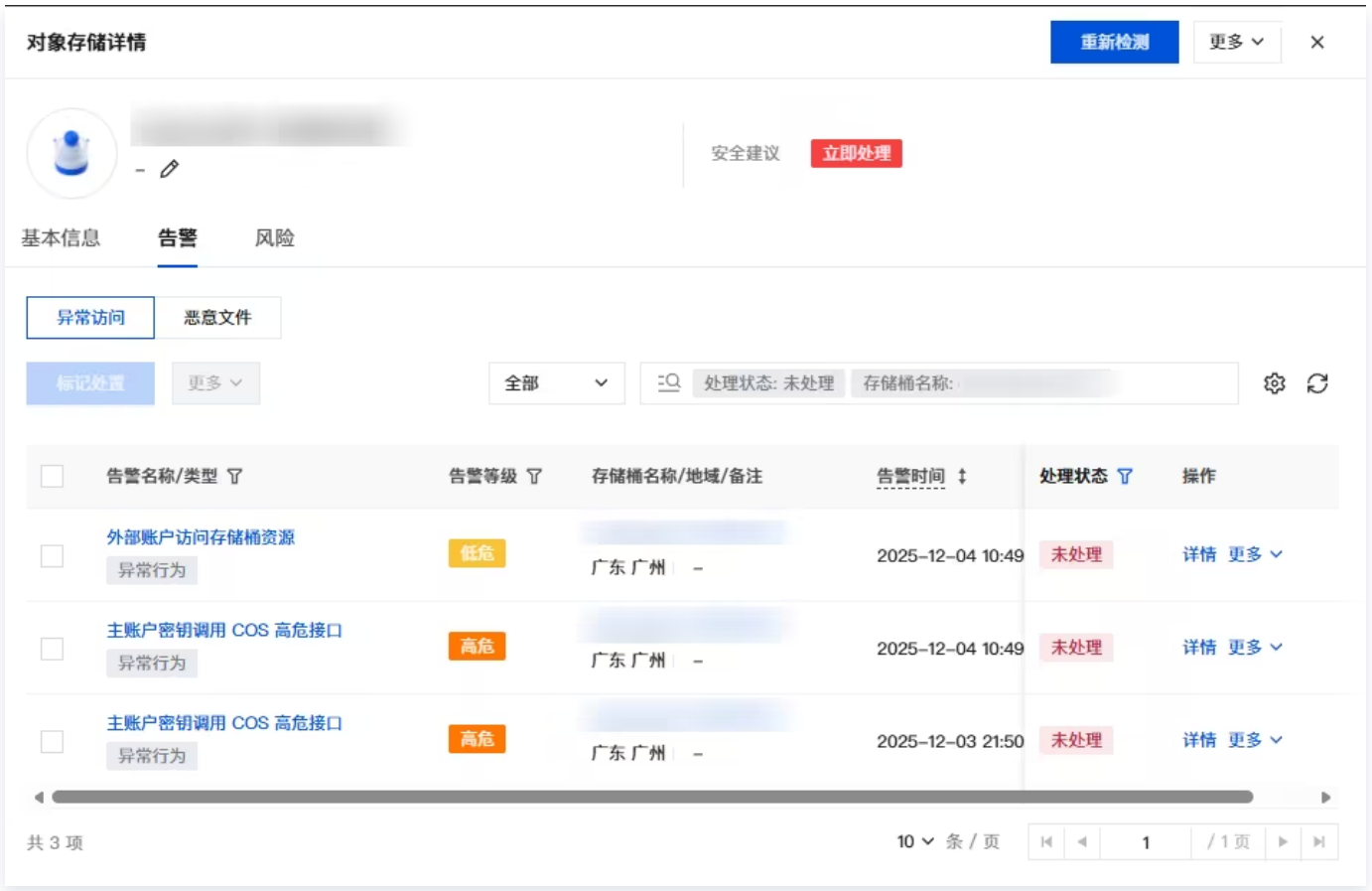
- 在对象存储详情页面，单击**基本信息 > 访问权限范围**，可通过访问账号和访问角色视角查看当前对象存储资产的访问权限范围。



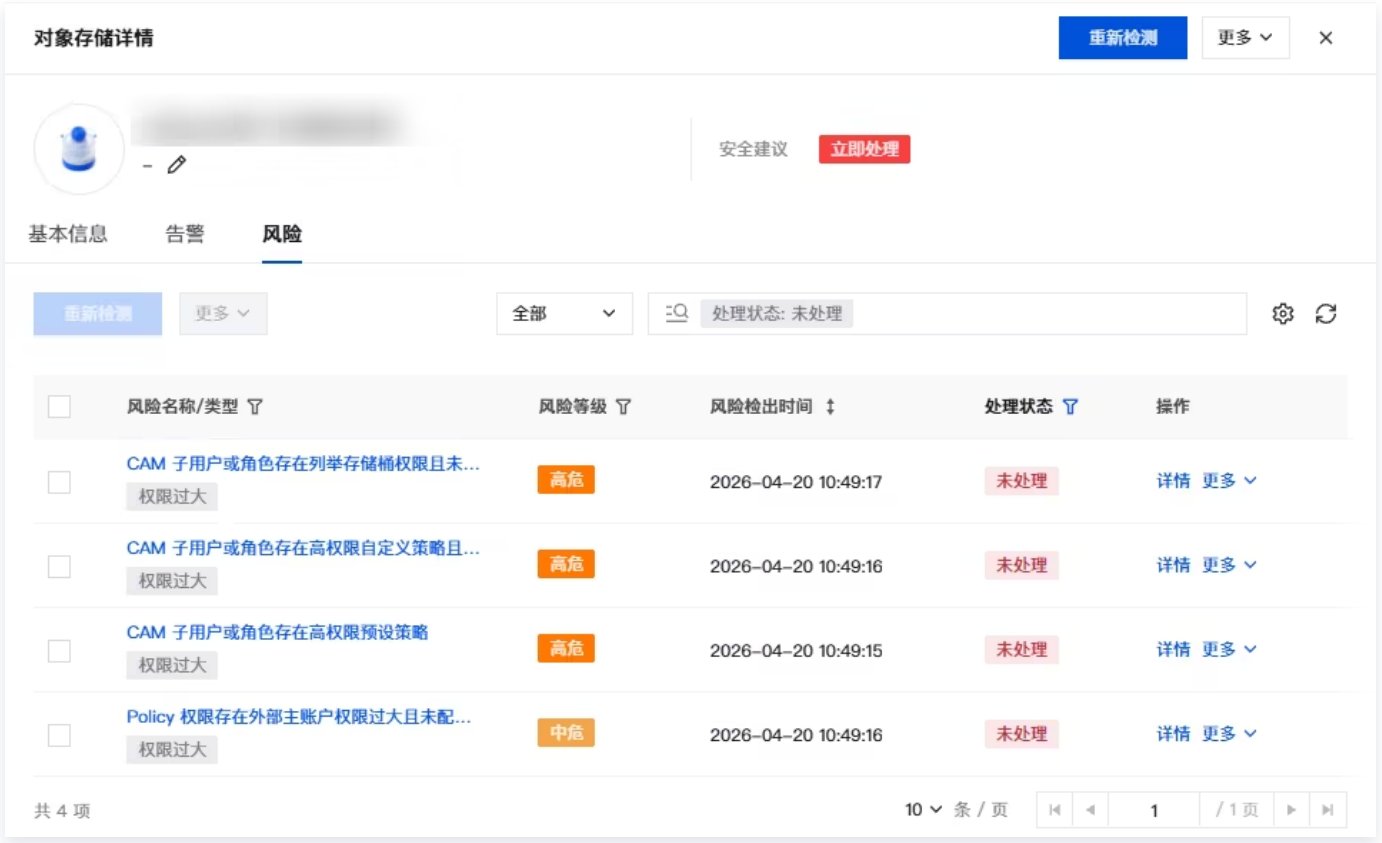
- 在对象存储详情页面，单击**基本信息** > **数据识别**，可查看对象存储的敏感数据识别结果。



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**。



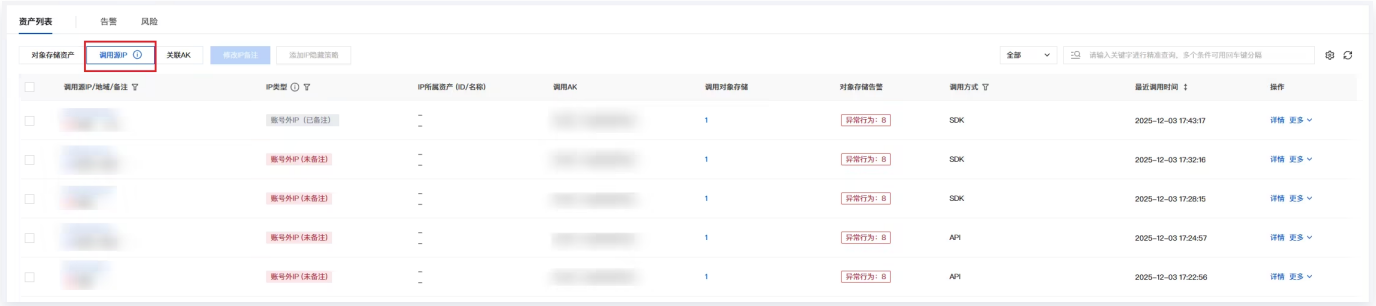
5. 在对象存储详情页面，单击**风险**，可查看存储桶风险信息，默认展示未处理风险，单击**详情**可打开**风险详情**。



调用源 IP

调用源 IP 列表

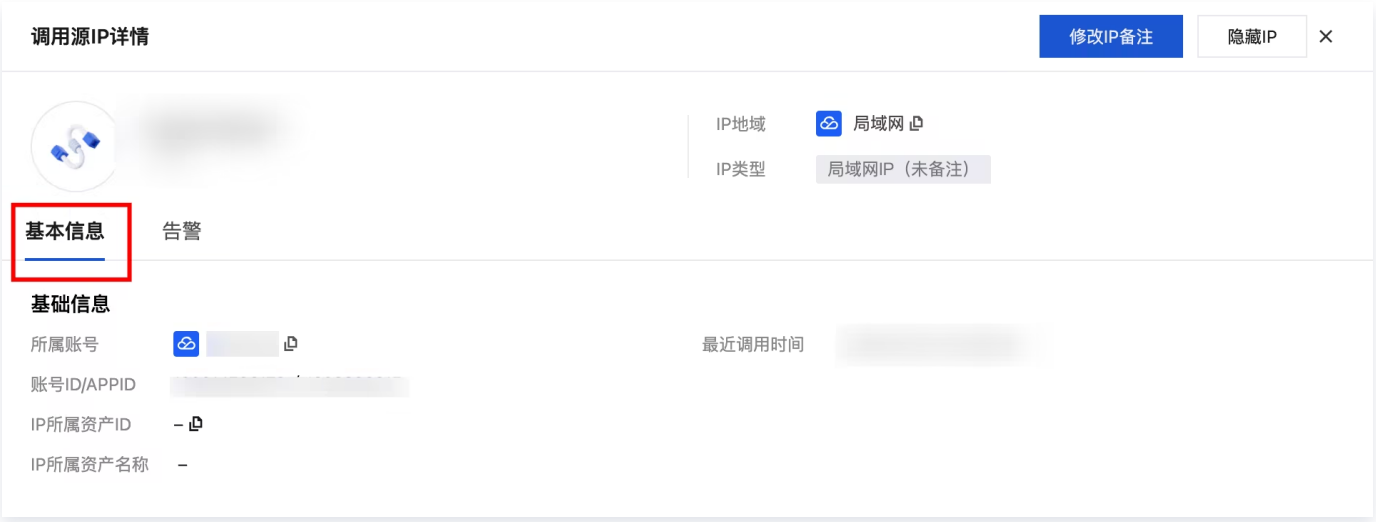
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势感知 > 对象存储异常监测**。
2. 在对象存储异常监测页面，**单击资产列表 > 调用源 IP**。
3. 在调用源 IP 页面中，基于调用源 IP 视角，可查看调用源 IP 信息、调用 AK、调用对象存储、关联告警、调用方式以及调用时间。



> **说明：**
> 仅展示被永久密钥访问过的 IP。

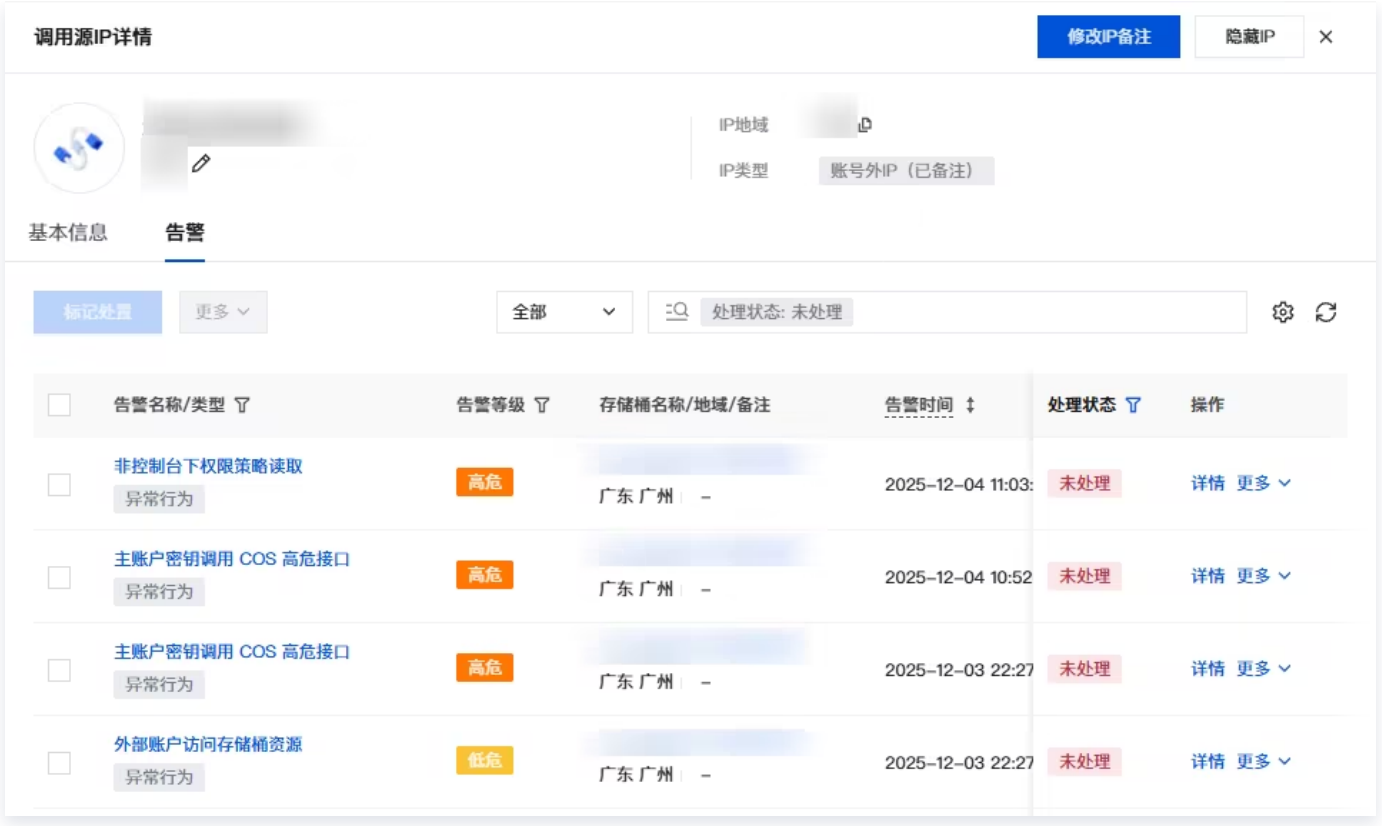
调用源 IP 详情

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 。

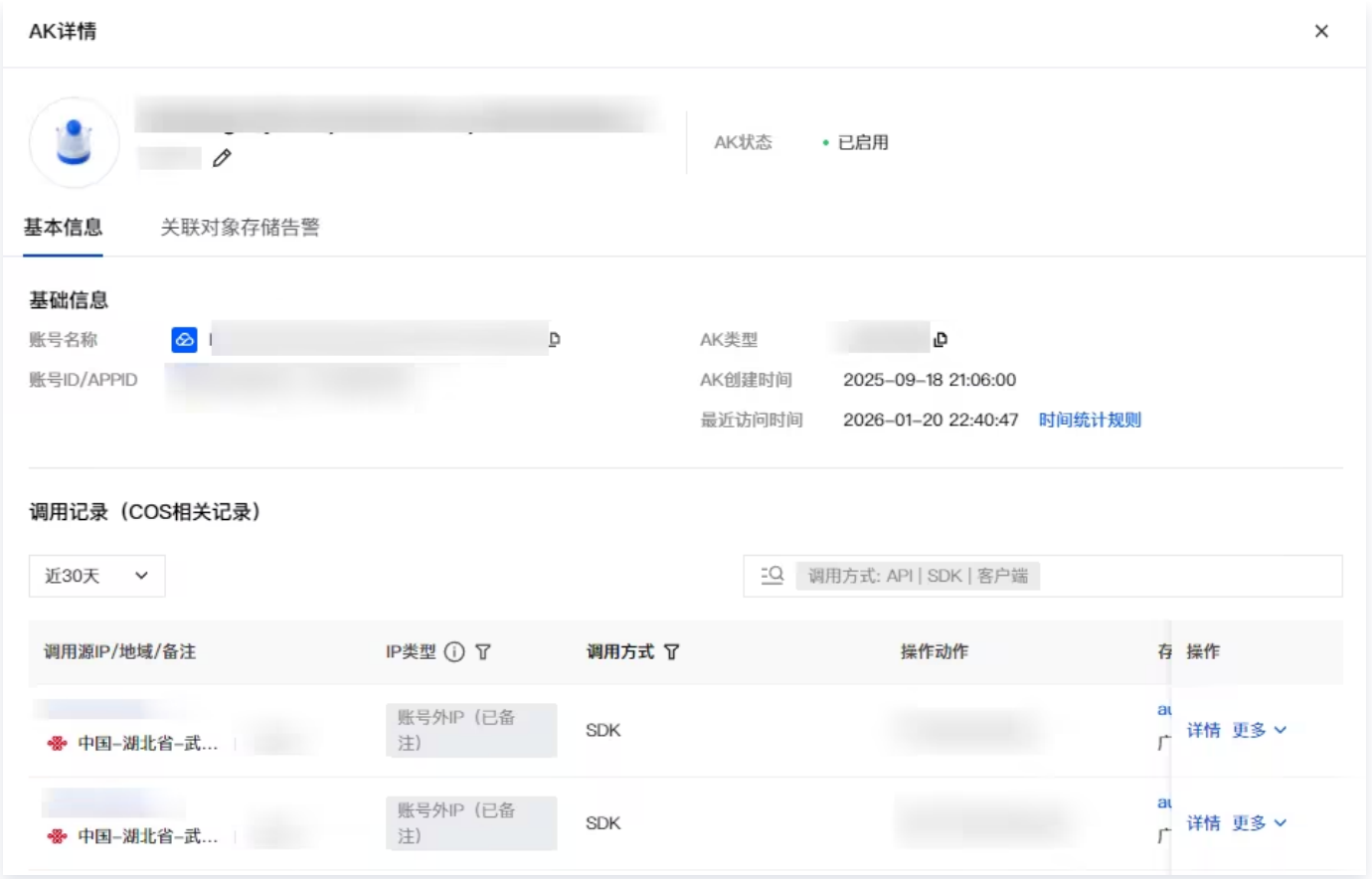
关联 AK 列表将展示对象存储相关的 AK 资产，可通过 AK 视角查看其关联的对象存储资产，以及所关联的对象存储资产告警详情。

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。

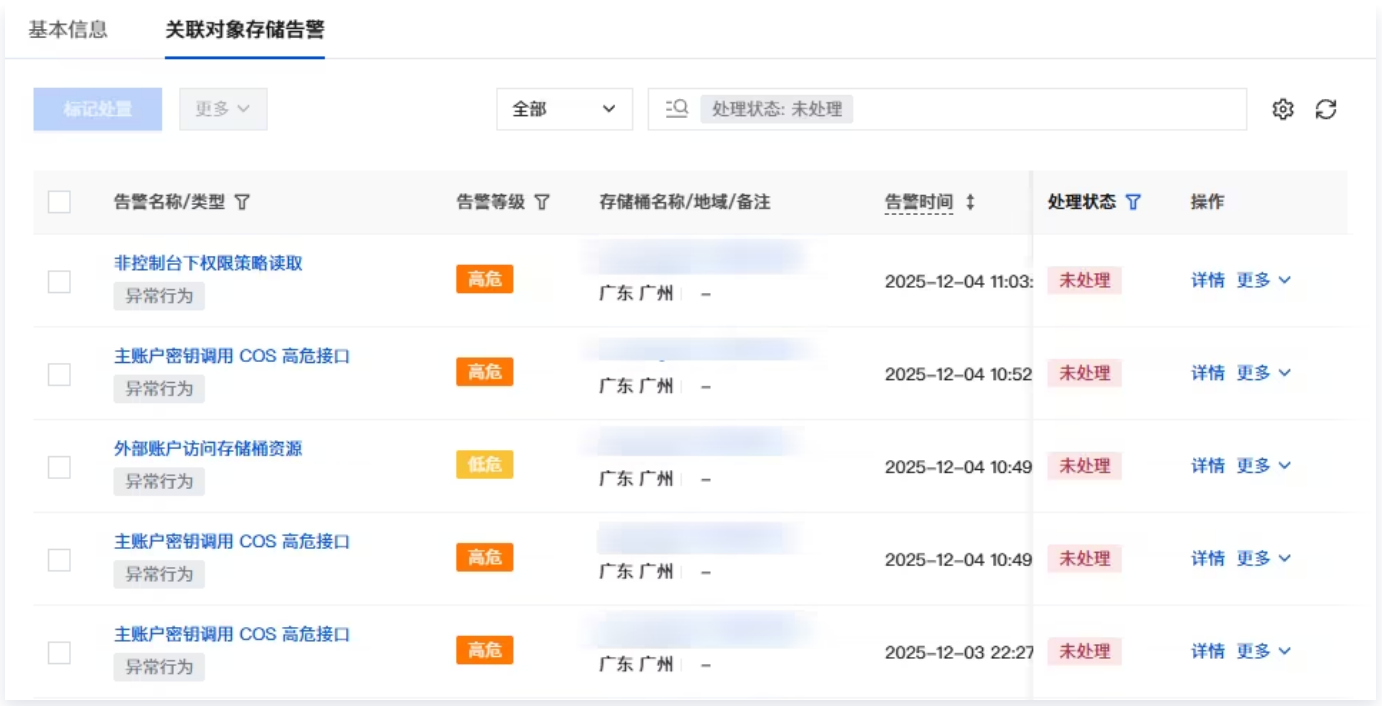


AK 调用记录

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。



告警

最近更新时间：2026-04-30 14:08:12

告警模块是数据安全态势感知中对象存储异常监测的核心风险处置模块，分为异常访问与恶意文件两大子模块，通过策略配置实现实时风险监控，并以告警形式集中呈现安全事件，支持告警分类、筛选、处置与溯源，是保障对象存储资产安全的核心管控入口。

异常访问告警

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

异常访问告警详情查看

1. 在异常访问告警列表中，选择所需异常访问告警，单击**详情**。

2. 在异常访问告警详情页面， 查看异常访问告警信息与异常调用记录。
   - 查看异常访问告警信息，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。

- 查看异常访问的异常调用记录，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。

异常访问告警处置

标记忽略

对误报或无需处理的异常访问告警进行状态标记，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. 在异常访问告警标签页面，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，可以将该异常访问告警所触发的策略添加至规则白名单中。

1. 在异常访问告警标签页面，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**保存**，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。

标记已处置

对已完成应急响应的告警进行状态更新，实现处置闭环。

1. 在异常访问告警标签页面，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置。

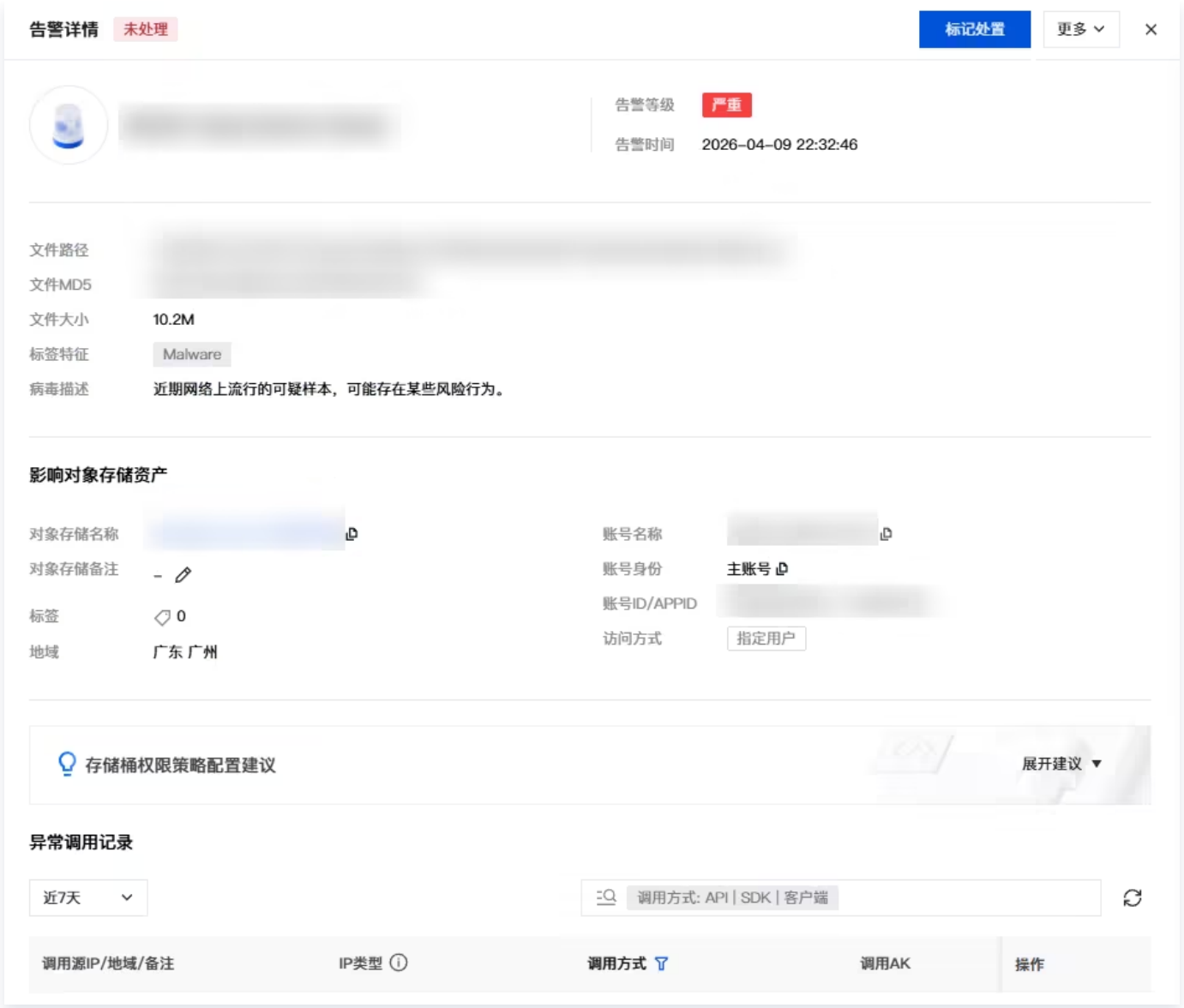
> **说明：**
> 告警处理状态标记为已处置后，该告警将不会纳入风险统计中。

恶意文件告警

1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势管理 > 对象存储异常监测**。
2. 在对象存储异常监测页面，单击**告警 > 恶意文件**标签。
3. 在恶意文件标签页，将展示已检测到的恶意文件信息。同时也可对恶意文件进行处置溯源与整改操作。

恶意文件告警详情查看

1. 在恶意文件标签页，选择需要查看的恶意文件告警，单击操作列的**详情**。
2. 在恶意文件告警详情页，将展示检测到的恶意文件详细信息，包括文件路径、文件 MD5、文件大小、描述。以及影响的对象存储资产信息等。



恶意文件告警处置

标记忽略

对误报或无需处理的恶意文件告警进行状态标记，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**保存**，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。

标记已处置

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置。

说明：
告警处理状态标记为已处置后，该告警将不会纳入风险统计中。

风险

最近更新时间：2026-04-30 14:08:12

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。

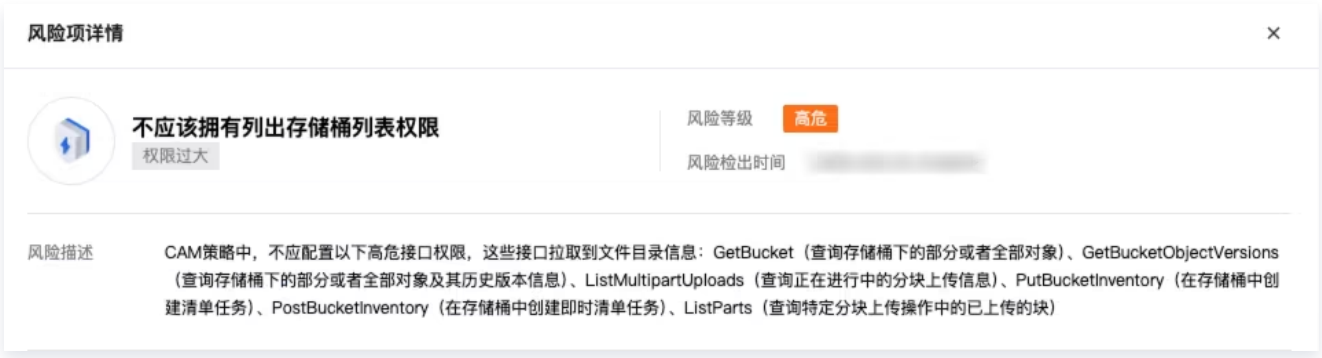
风险列表

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**。

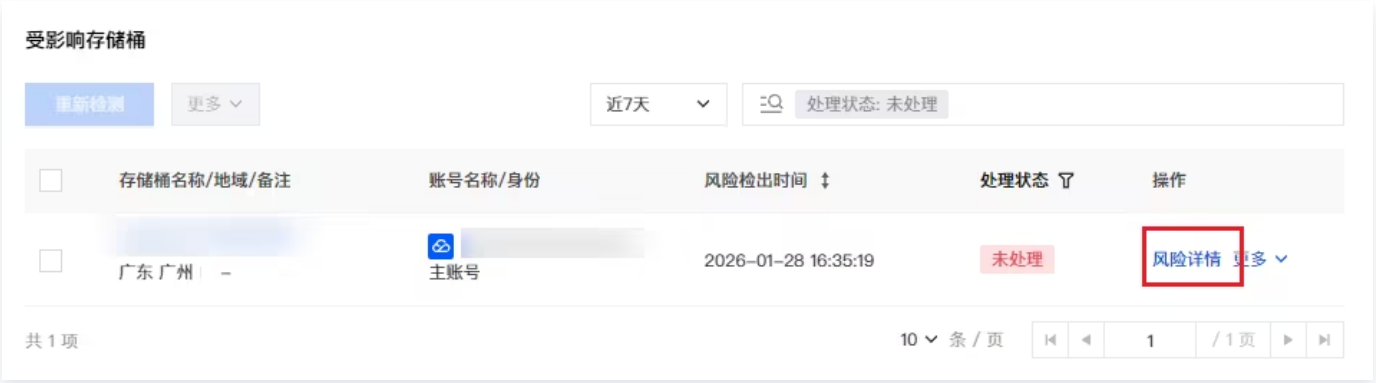
2. 在**风险项详情**页面，查看风险项基本信息、受影响存储桶以及配置建议。
   - 查看风险项基本信息。



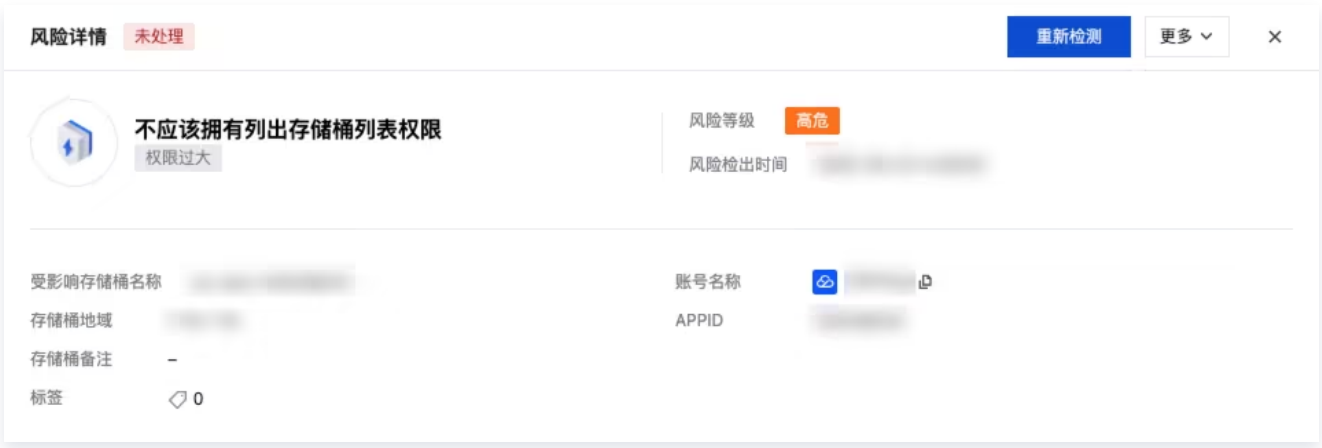
   - 查看受影响存储桶列表，默认显示未处理风险的存储桶。

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。

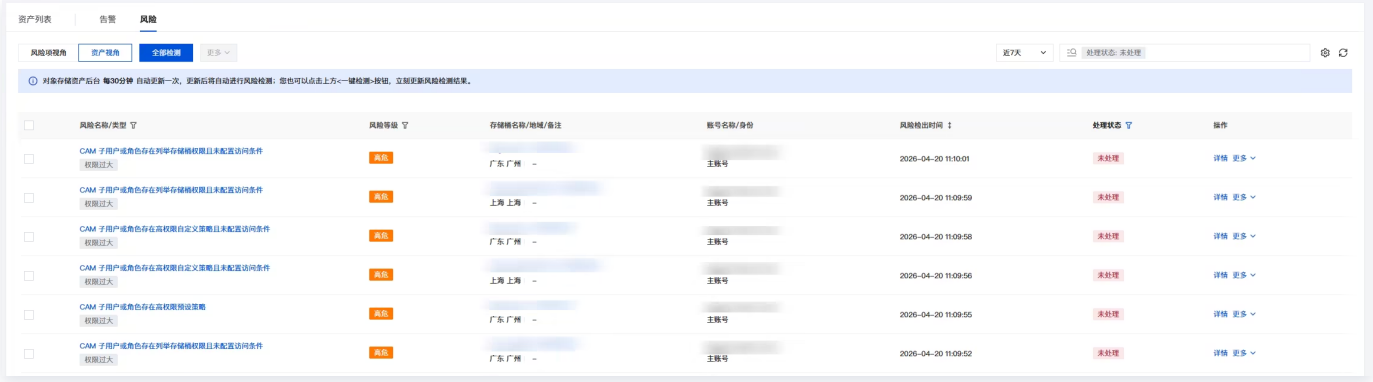
   - 查看风险相关接口调用情况以及配置建议。

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。

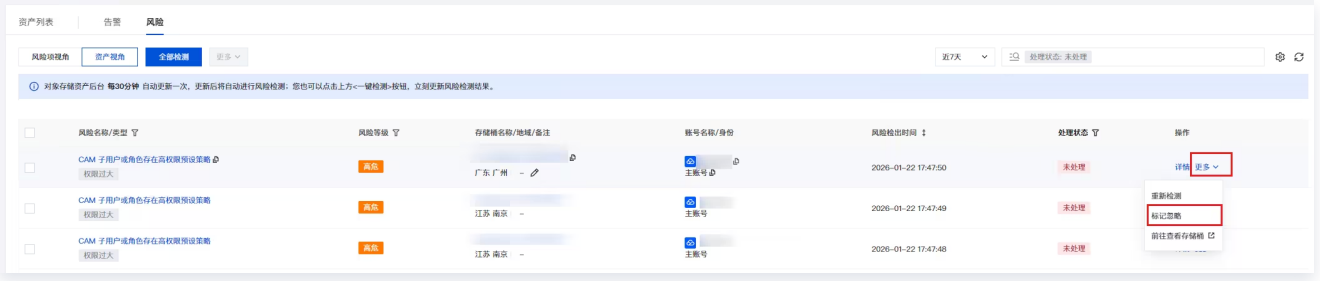
   - 查看风险描述与证据，该风险详情的证据包括：权限来源/内容、策略 ID/授权策略名称、授权资源、授权操作。

   - 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：2026-04-30 14:08:12

告警策略

恶意文件策略

实时监测增量文件中的恶意文件，若存储桶存在恶意文件，将产生恶意文件告警

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，单击右上角的**策略管理**。
3. 在策略管理窗口中，单击**告警策略**标签，可开启或关闭恶意文件全量检测。

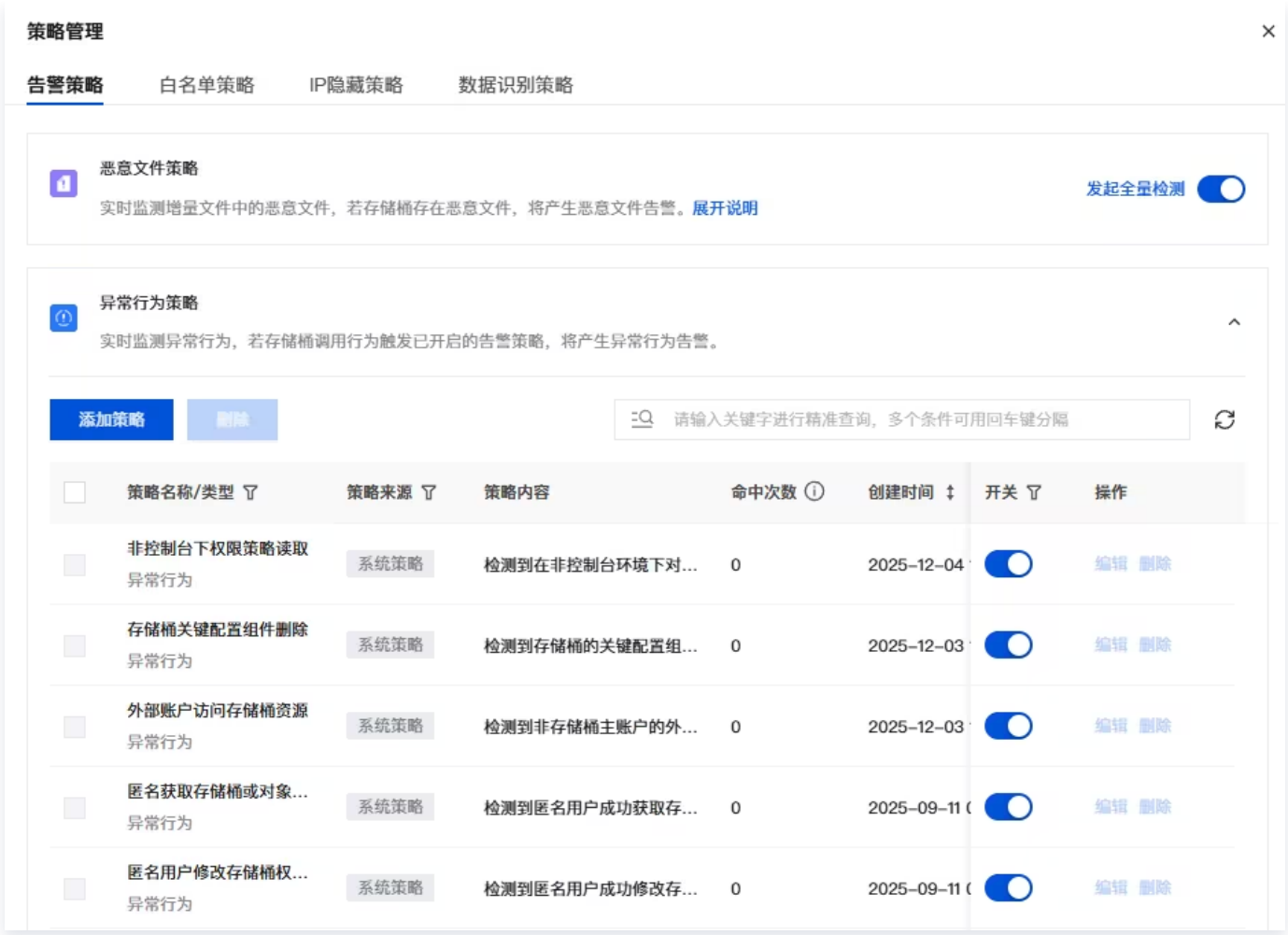
说明：

- **策略说明：**系统后台仅实时检测增量文件，点击「全量识别」可主动对存储桶所有文件进行恶意文件识别。
- **计费说明：**敏感数据识别涉及对象存储的读请求费用，通过资源包/按量计费每日结算，详情可查看 对象存储-计费概述 。

异常行为策略

实时监测异常行为，若存储桶调用行为触发已开启的告警策略，将产生异常行为告警。

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，也支持自定义输入 AK； • 多个 AK 需换行输入，最多150行；	AK1 AK2

	• 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。	
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
告警类型	选择白名单策略的告警类型：异常访问、恶意文件	
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，也支持自定义输入 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，也支持自定义输入 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。

数据识别策略

实时监测存储桶增量文件敏感数据，若识别到敏感数据，将在资产和告警中展示。

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**数据识别策略**标签。可开启/关闭敏感数据识别策略。

说明：

- **策略说明：**系统后台仅实时检测增量文件，可在各对象存储资产详情页点击「全量识别」可主动对存储桶所有文件进行敏感数据识别。
- **计费说明：**敏感数据识别涉及对象存储的读请求费用，通过资源包/按量计费每日结算，详情可查看 对象存储-计费概述 。

数据库风险监测
功能简介

最近更新时间：2026-04-30 14:08:12

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：2026-04-30 14:08:12

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**数据安全态势管理** > **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，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；
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）。

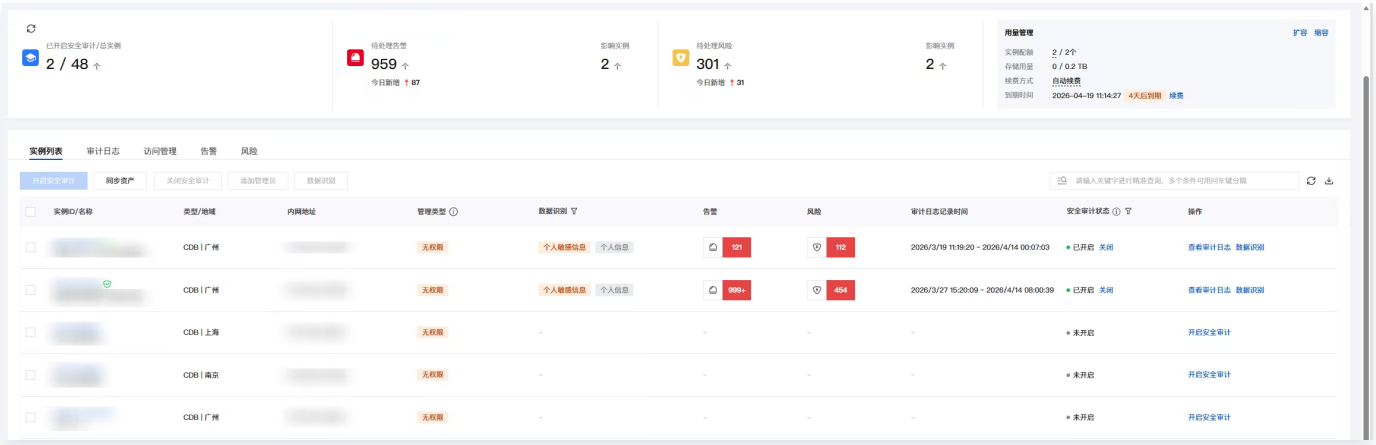
数据资产

最近更新时间：2026-04-30 14:08:12

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

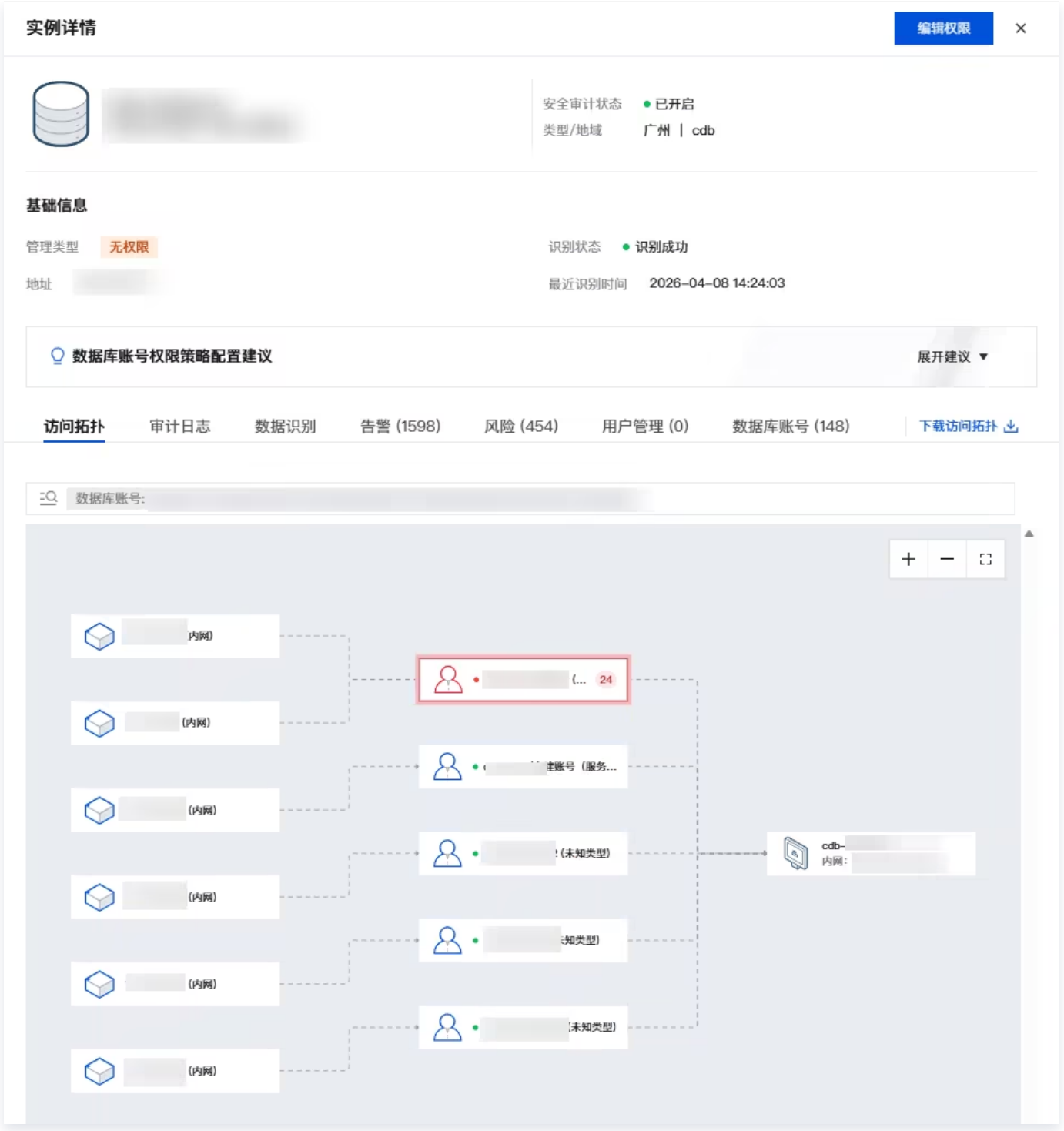
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势管理 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**实例列表**标签。
3. 在实例列表标签页面，将显示已同步的数据库资产。



数据资产详情

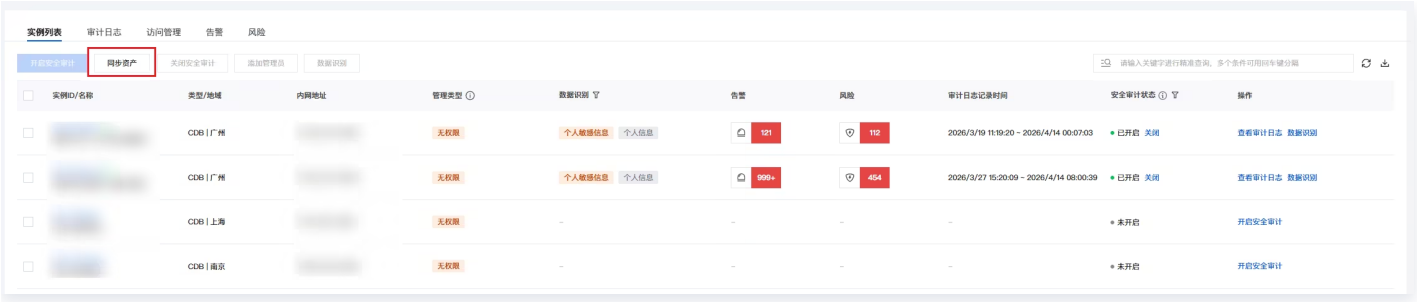
1. 在实例列表标签页面，选择目标数据库资产，单击**资产实例 ID**。

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

在实例列表标签页，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. 在实例列表标签页中，选择目标数据库资产，单击操作列的**开启安全审计**，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. 在实例列表标签页中，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，选择立即识别或周期识别，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：2026-04-30 14:08:12

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。

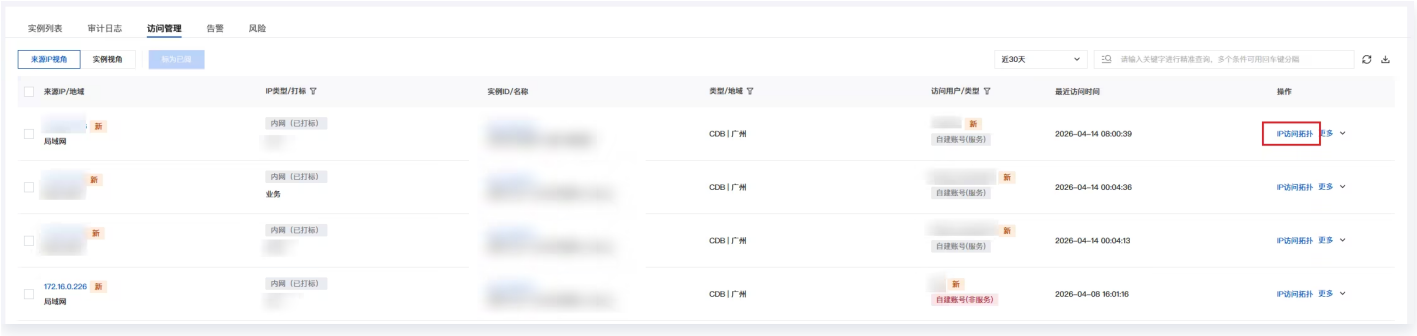
管控视角	描述	适用场景
来源 IP 视角	以访问发起端的来源 IP 为核心管控维度，整合该 IP 对数据库实例的访问数据，提供访问拓扑可视化、IP / 账号精准打标及安全组策略快速调整能力，实现对访问发起端的集中精细化管控。	排查单一 IP 的跨实例访问风险、批量标记某类访问端。
实例视角	以访问目标端的数据库实例为核心资源维度，整合来源 IP 对该实例的访问数据，提供资产访问拓扑可视化、IP / 账号精准打标及安全组策略快速调整能力，实现对访问目标端的集中精细化管控。	梳理单一实例的全量访问来源、针对核心实例做专项管控。

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、类型/地域、访问用户/类型、最近访问时间等信息。

IP 访问拓扑

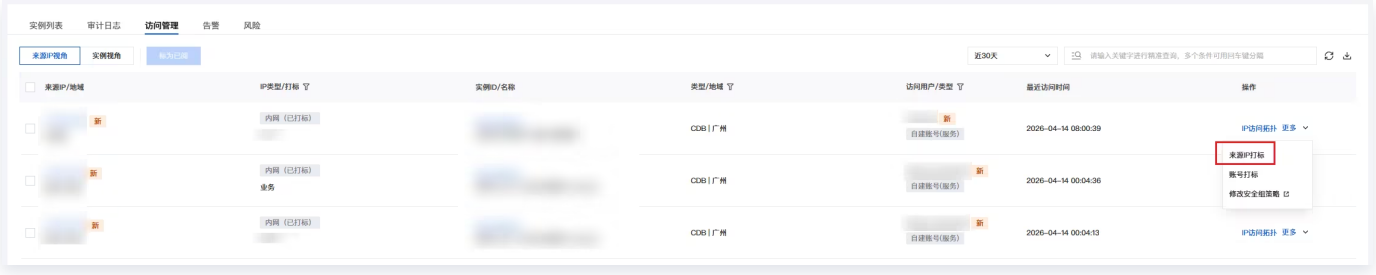
以可视化图谱的形式，直观展示单个来源 IP 与所有关联账号、数据库实例之间的访问关系、访问频率及安全状态。在来源 IP 视角列表，单击目标 IP 对应操作列的 **IP 访问拓扑**，可查看该 IP 与关联数据库实例的访问关系图谱。



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**。



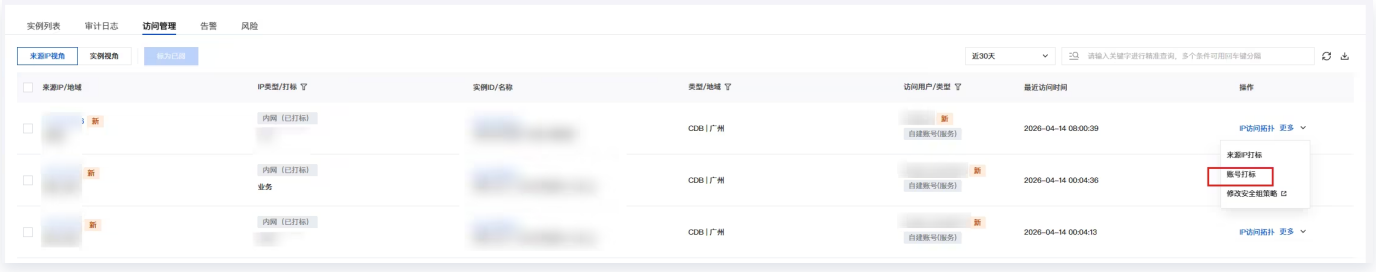
2. 在来源 IP 打标窗口，编辑来源 IP 备注，单击**确定**完成标记。

> **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

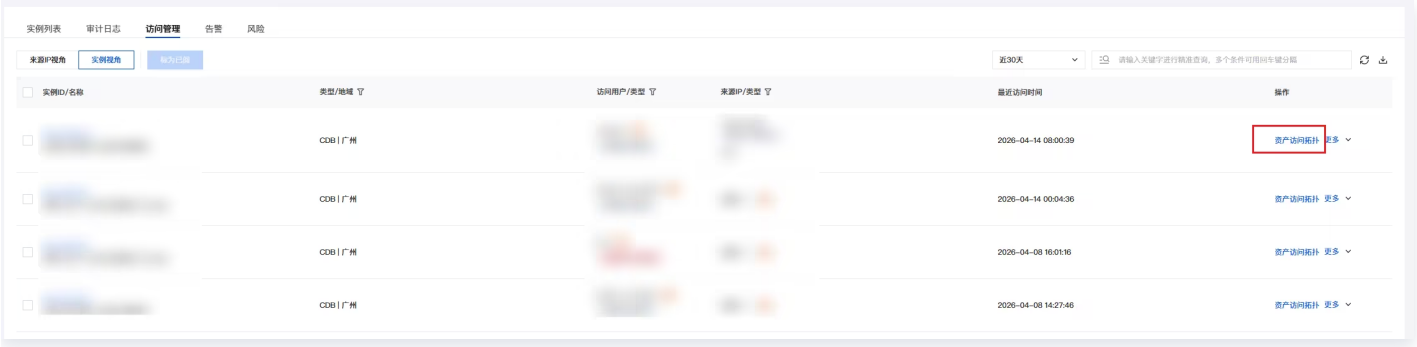
快速跳转至目标 IP 关联的数据库实例资产页面，直接修改安全组策略，实现对该 IP 访问权限的快速管控（允许 / 拒绝访问）。
在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 修改安全组策略**，可前往数据库实例资产页面修改安全组策略。

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。


实例列表
审计日志
访问管理
告警
风险
来源IP视角
实例视角
近30天
实例ID/名称
类型/地域
访问用户/类型
来源IP/类型
最近访问时间
操作
CDB | 广州
自建账号(服务)
内网（已打标）
2026-04-14 08:00:39
资产访问拓扑
更多
来源IP打标
账号打标
修改安全组策略
CDB | 广州
自建账号(服务)
内网IP:
2026-04-14 00:04:36
CDB | 广州
自建账号(非服务)
内网IP:
2026-04-08 16:01:16
资产访问拓扑
更多

告警

最近更新时间：2026-04-30 14:08:12

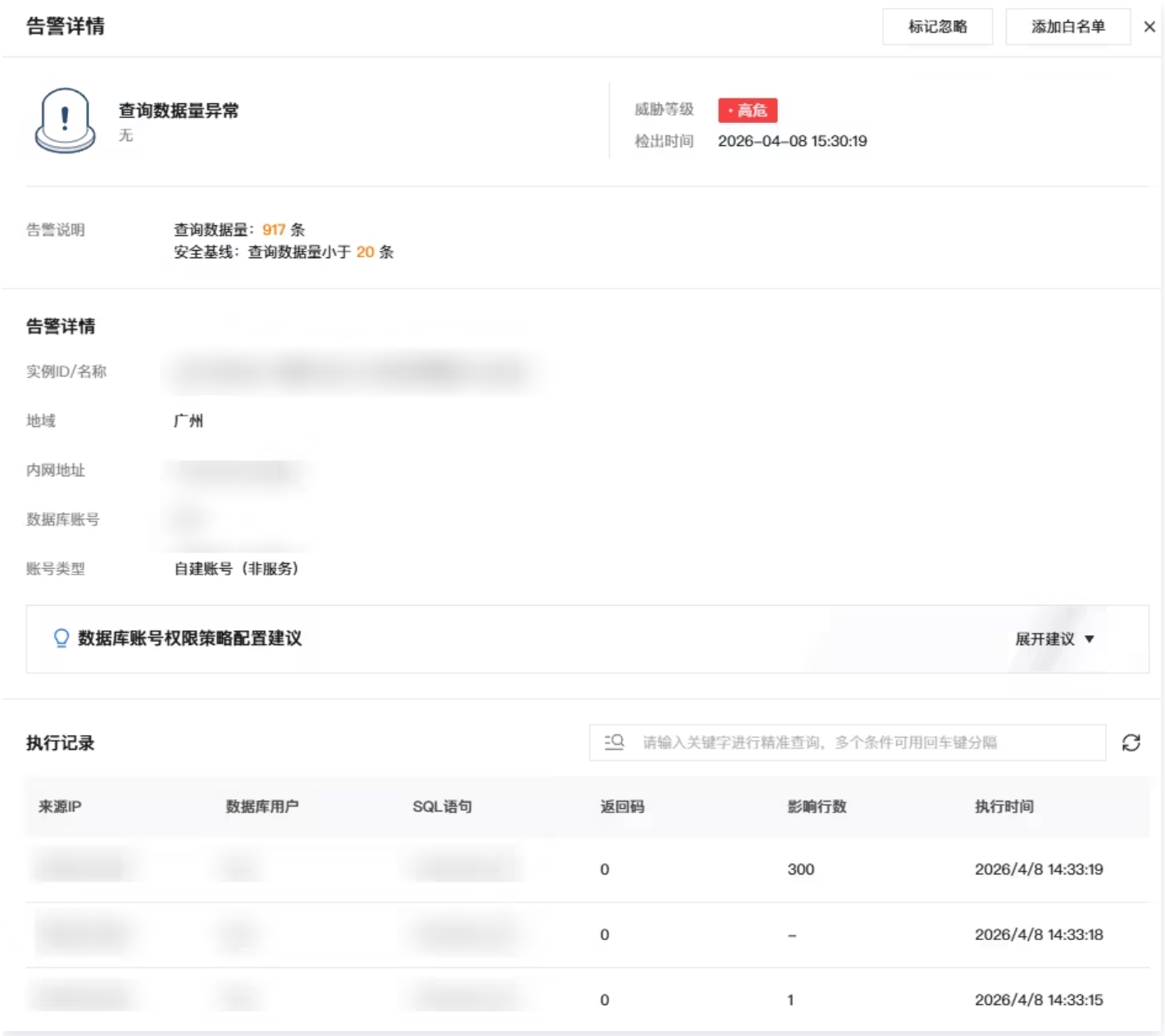
数据库风险监测告警模块，通过对数据库资产的安全事件实时监测与响应体系，实现违规行为精准识别与闭环处理。

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**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**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；

标记已处置

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置。

> **说明：**
> 告警处理状态标记已处置后，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、调整威胁等级、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，可以对威胁等级、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：2026-04-30 14:08:12

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），当其小于配置的比例时，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、威胁等级、实例 ID/名称、数据库账号、所属用户/类型、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**风险名称**，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**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**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置。

> **说明：**
> 风险处理状态标记已处置后，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**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、调整威胁等级、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，可以对威胁等级、策略内容（非服务账号）进行修改。

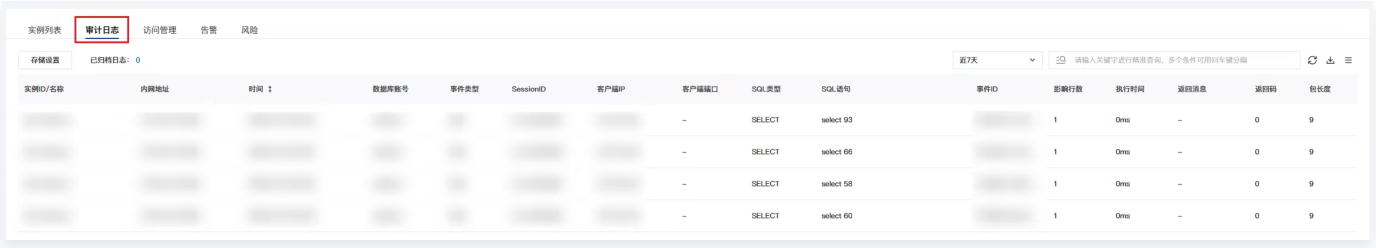
审计日志

最近更新时间：2026-04-30 14:08:12

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。

审计日志

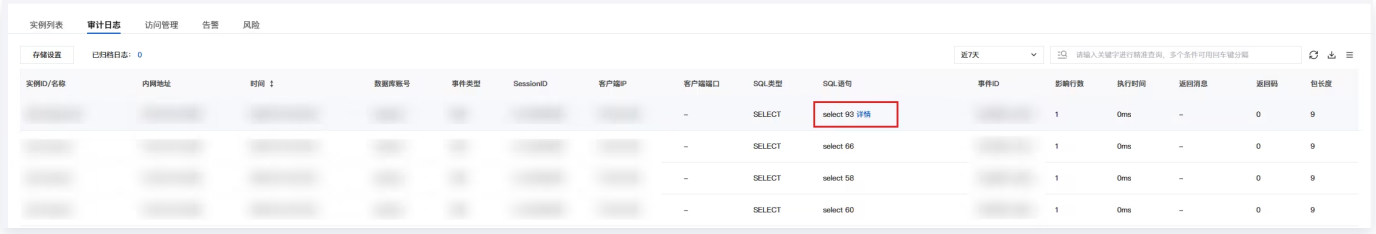
1. 登录 云安全中心控制台，在左侧导览中，单击**数据安全态势管理 > 数据库风险监测**。
2. 在数据库风险监测页面，单击**审计日志**标签。
3. 在审计日志页面中，显示已同步数据库资产的操作记录。



4. 在审计日志页面中，可通过实例、数据库账号、客户端 IP、客户端端口和 SQL 语句进行日志检索。

SQL 语句详情

1. 在审计日志标签页面中，单击目标日志 SQL 语句列的**详情**。



2. 在 SQL 语句详情页，您可查看完整 SQL 语句信息。

存储设置

> **说明：**
> - 当日志量或日志存储时长达到对应量级时，将自动以文件形式归档较早的日志；
> - 归档时，将优先归档最早的日志单元，1个日志单元最大包含45GB 或8千万条日志。
> - 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可查看。

1. 在审计日志标签页面中，单击**存储设置**。
2. 在存储设置窗口，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. 登录 云安全中心控制台 ，在左侧导览中，单击**数据安全态势管理** > **数据库风险监测**。
2. 在数据库风险监测页面，单击**审计日志**标签。
3. 在审计日志页面中，单击已归档日志。

4. 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。

检测响应
告警中心

最近更新时间：2026-04-30 14:08:12

功能简介

用于集中展示和管理主机运行过程中发现的各类安全风险，覆盖恶意文件、异常登录、密码暴力破解、恶意请求、高危命令、本地提权行为、反弹 Shell、网络攻击等入侵风险。通过对安全事件进行统一告警、查看和处置，帮助用户及时发现风险，并开展后续安全加固与处置工作。

操作步骤

1. 登录 云安全中心控制台 ，在左侧导览中，单击**告警中心**。
2. 在告警中心页面，通过左侧栏切换告警类型进行不同类型告警管理，具体告警类型及操作指南如下：

功能名称	功能描述	操作指南
文件查杀	• 用于检测服务器中的木马、病毒、WebShell 等恶意文件，帮助用户识别已落地的恶意样本，并及时进行隔离和处置。 • 用于识别由恶意程序触发的异常进程活动，帮助用户发现恶意文件运行后的进程行为，便于进一步定位和处理安全风险。	文件查杀
异常登录	用于检测不符合常用来源 IP、常用用户名、常用登录地或常用登录时间等特征的登录行为，帮助用户及时发现可疑登录事件。	异常登录
密码破解	用于对 SSH、RDP 等协议的暴力破解行为进行实时监控，并支持自动阻断，帮助用户降低账号被暴力尝试登录的风险。	密码破解
恶意请求	用于监控主机访问恶意域名或恶意地址的行为，帮助用户识别木马回连、恶意外联等异常网络请求风险。	恶意请求
高危命令	用于对系统中的高危命令执行行为进行实时监控和告警，帮助用户发现入侵后可能发生的危险操作行为。	高危命令
本地提权	用于检测低权限账号通过异常方式提升系统权限的行为，帮助用户识别服务器被入侵后的提权风险。	本地提权
反弹 Shell	用于识别服务器上的 Shell 反向连接行为，帮助用户发现攻击者建立远程控制通道的风险。	反弹 Shell
网络攻击	用于对服务器遭受的恶意流量和攻击行为进行监测与分析，帮助用户识别异常攻击流量及漏洞利用风险。	网络攻击

安全运营
日志分析
日志分析概述

最近更新时间：2026-04-30 14:08:12

基本概念

日志分析是云安全中心提供的云上安全日志统一接入与集中管理服务。通过接入云安全中心、主机安全、云防火墙等多种云安全产品及云产品，将分散在各产品中的日志数据统一汇聚存储，为用户提供一站式的日志检索查询入口。日志分析服务覆盖日志从采集、存储、检索到投递的全生命周期管理，帮助用户高效开展安全运营分析、威胁溯源排查与合规审计等工作。

功能特性

统一日志接入与集中存储

支持多种云安全产品及云产品日志的统一接入与集中存储，提供一站式检索查询入口。用户可在统一界面中选择目标产品和日志类型进行检索，消除日志数据孤岛，有助于快速定位安全事件、高效开展日志分析与溯源排查。

强大的 CQL 检索分析

内置 CQL 检索语法，支持语句检索和过滤检索两种模式。语句检索支持丰富的条件组合与复杂查询表达；过滤检索通过选择特定字段和过滤条件实现快捷过滤。同时提供原始数据视图和表格视图两种展示方式，满足多维度、精细化的日志检索与深度分析需求。

灵活的存储策略配置

提供日志存储的全局监控与精细化配置能力，支持查看存储用量监控总览及用量趋势。用户可按产品、按日志类型灵活配置是否存储及存储时长，并支持批量开启、批量关闭、批量配置存储时间等快捷操作。

日志对外投递

支持将日志数据实时投递至 Kafka（消息队列）、CLS（日志服务）、Splunk 等外部平台，满足数据归档、跨平台联动分析及自建安全运营体系等多样化的数据流转需求。

多账号存储共享与统一运营

在多账号场景下，支持管理员账号/委派管理员账号将日志存储容量灵活共享给多个成员账号，并支持跨账号的存储策略配置、日志投递策略配置和配置同步等能力，降低多账号环境下的运营复杂度，实现日志资源的集约化管理。

计费说明

详见 计费概述 。

检索分析

最近更新时间：2026-04-30 14:53:42

本文介绍如何使用检索分析模块对已接入产品的日志进行查询，支持语句检索和过滤检索两种模式，以及原始数据视图和表格视图的切换。

功能概述

提供统一的查询入口，支持对已接入产品的日志进行统一分析与检索。

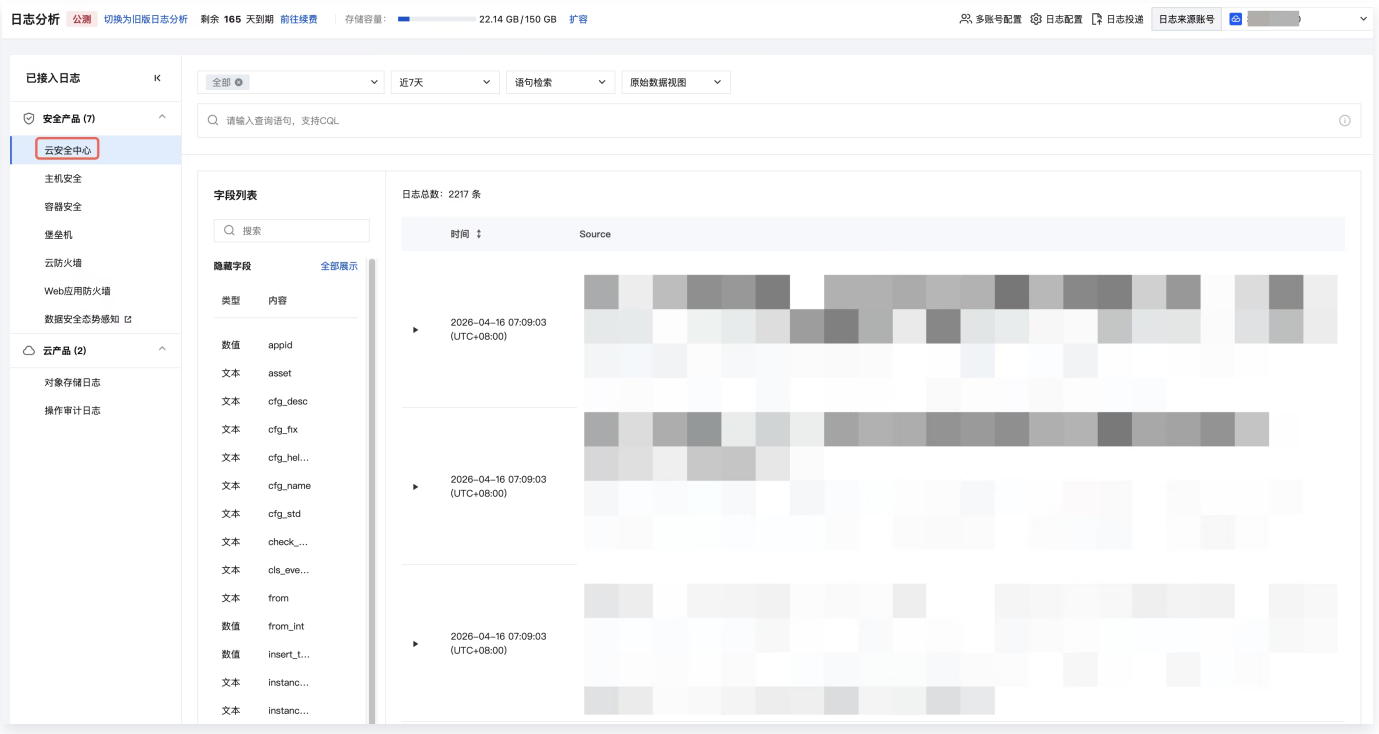
前提条件

1. 已购买 日志分析服务 的账号。
2. 当前的**登录账号**是已经被共享了存储容量的账号。

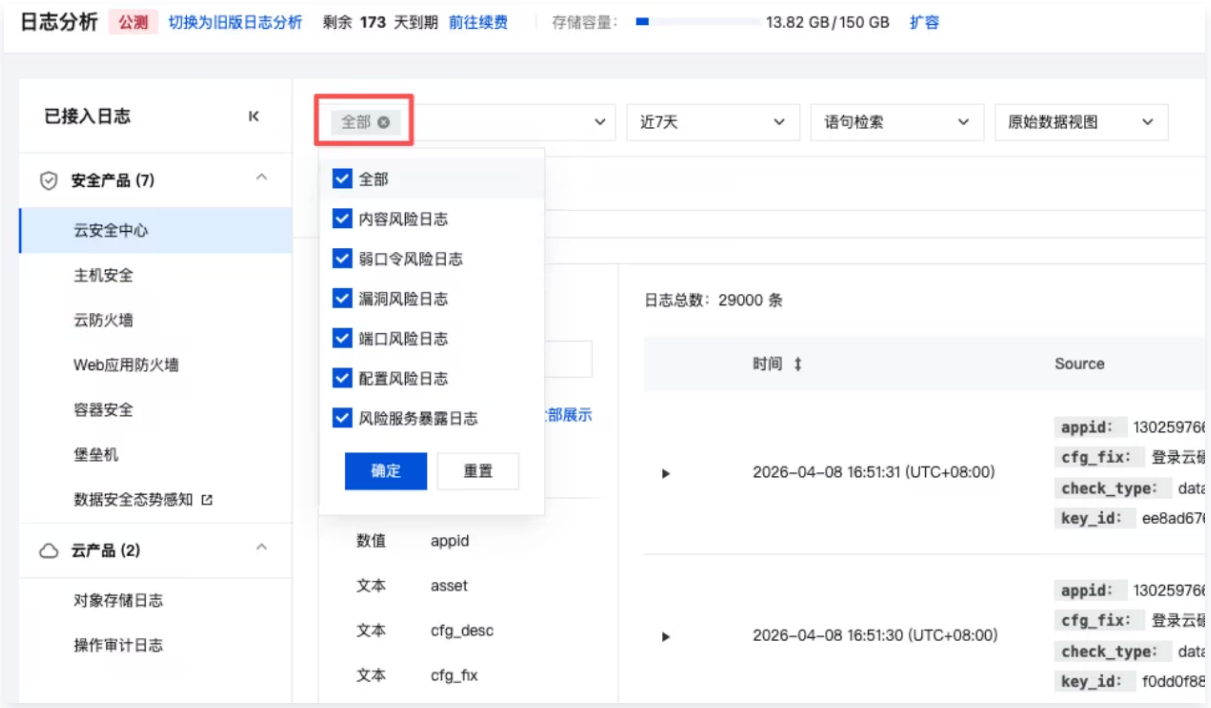
> **说明：**
> 多账号场景下，日志分析服务支持存储容量共享，详情可见操作指南中的多账号配置-日志分析容量共享。

操作步骤

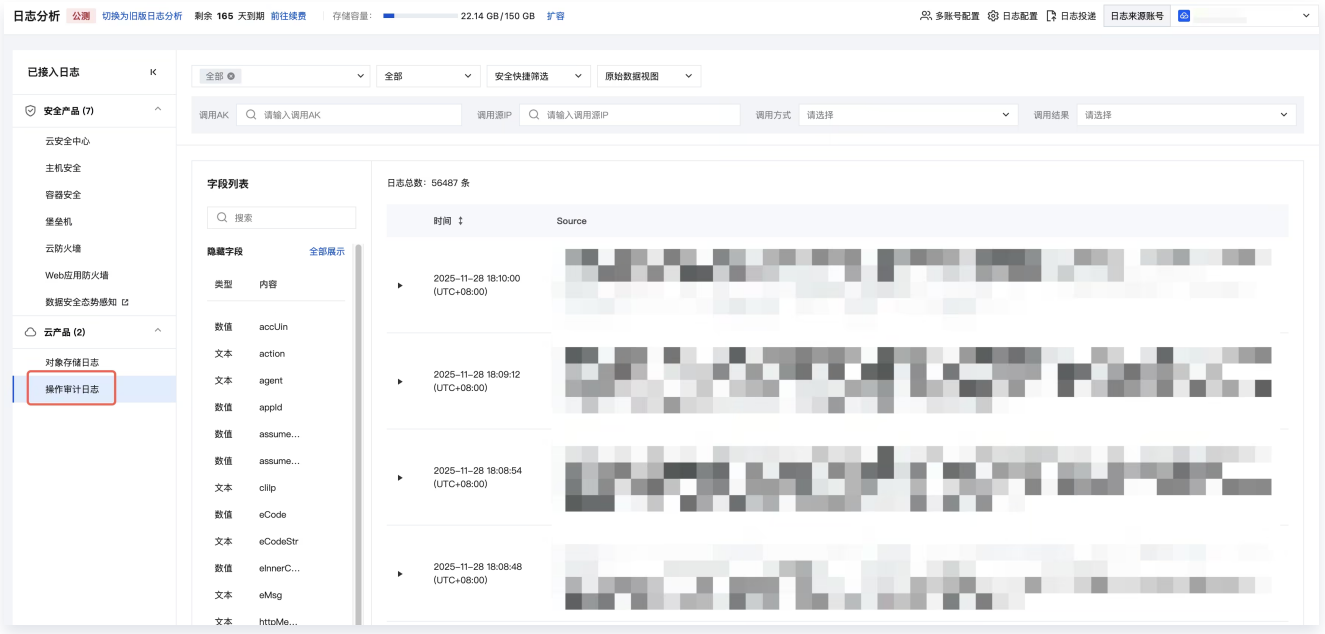
1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，左侧展示已接入的云产品列表，选择需要查询的目标产品（如云安全中心、主机安全、云防火墙等）。



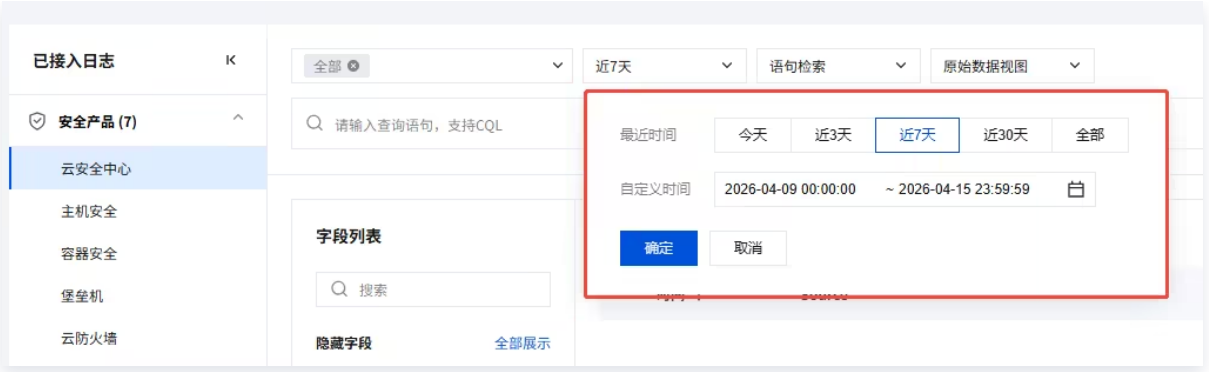
3. 查询的日志类型选择：支持查询指定类型的日志数据，默认情况下会选中全部类型的日志。当前安全产品支持日志类型选择，云产品中则是直接将重要字段罗列出来方便您直接过滤。
   - 安全产品的日志类型选择



   - 云产品的日志类型选择

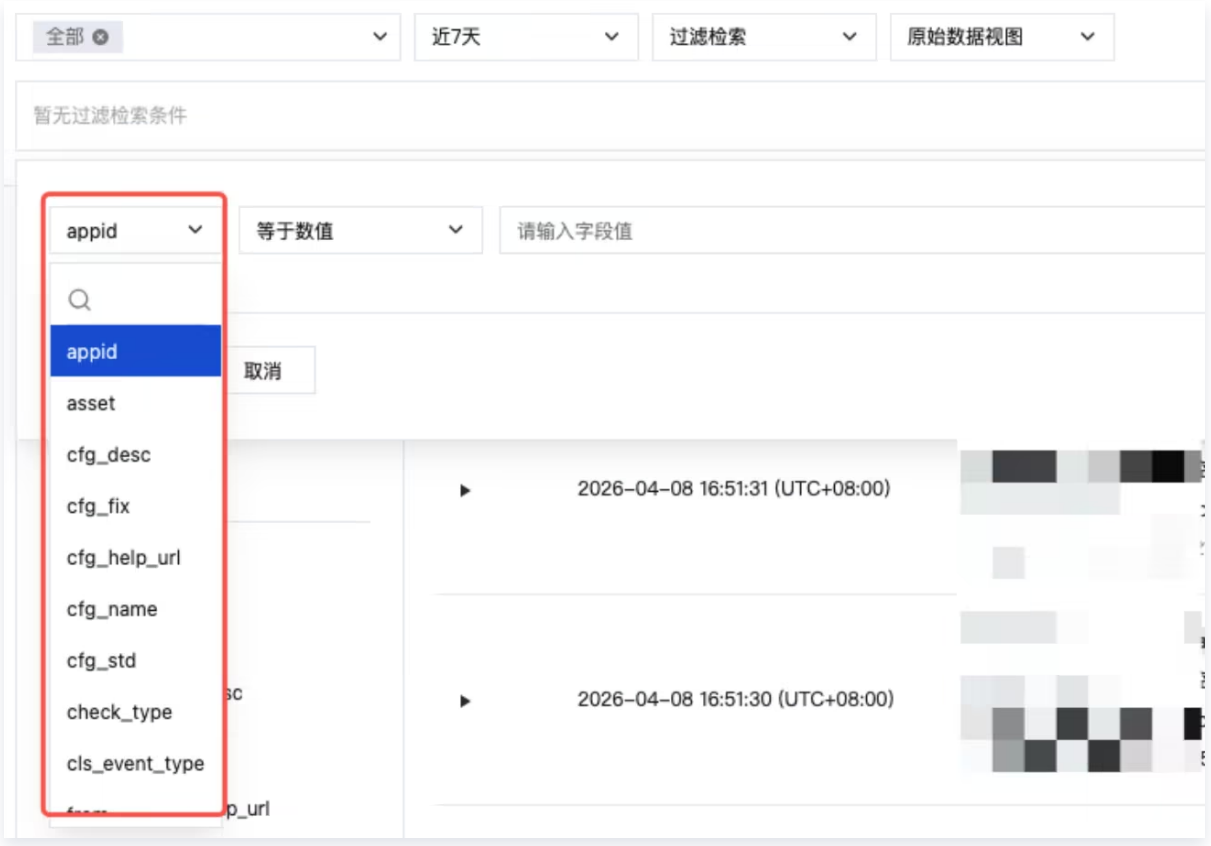


4. 选择检索的时间范围：单击顶部时间选择器，可快速选择“今天”、“近 3 天”、“近 7 天”、“近 30 天”等预设范围，也可自定义起止时间。

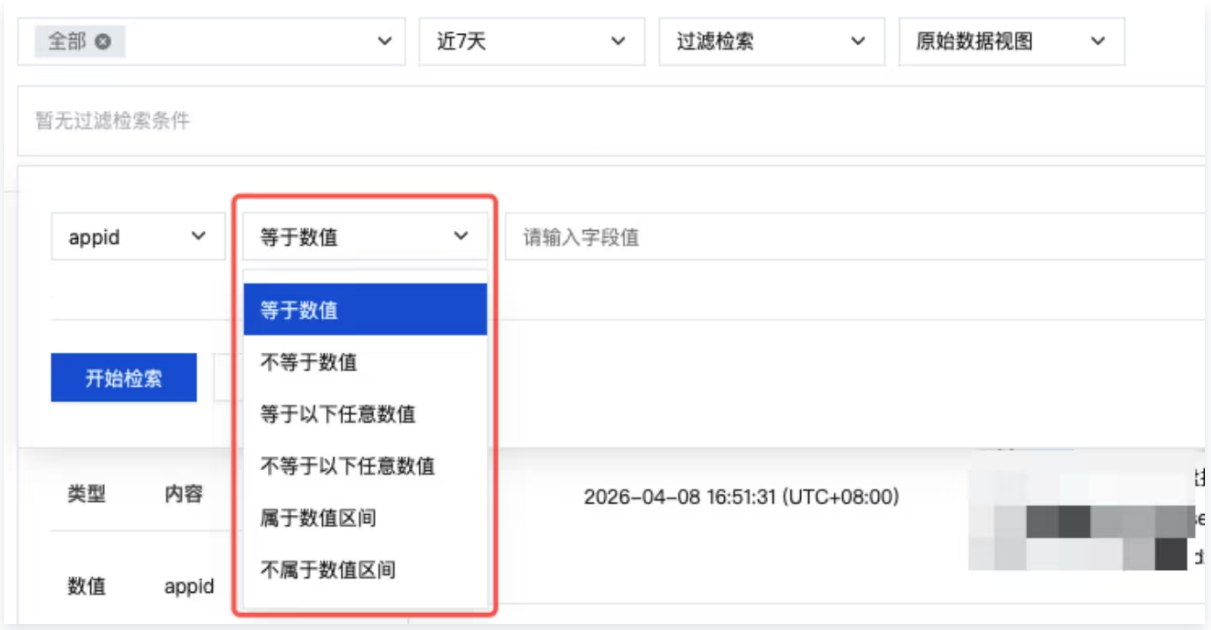


5. 选择检索模式，支持语句检索和过滤检索，CQL 语法规则请参考 CQL 语法规则 。
   - 语句检索：在搜索栏中输入查询语句，支持 CQL 语法，可进行多条件组合的精准检索与复杂分析。
   - 过滤检索：通过选择特定字段以及过滤条件，进行快捷过滤。

   5.1 选择特定字段。

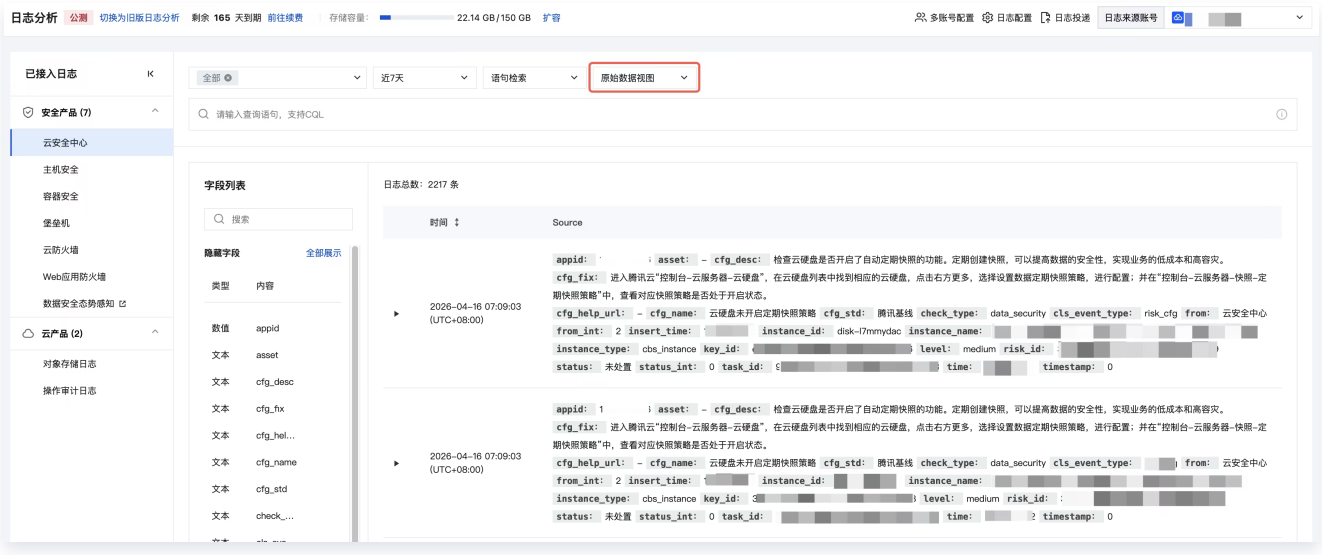


   5.2 选择过滤条件。

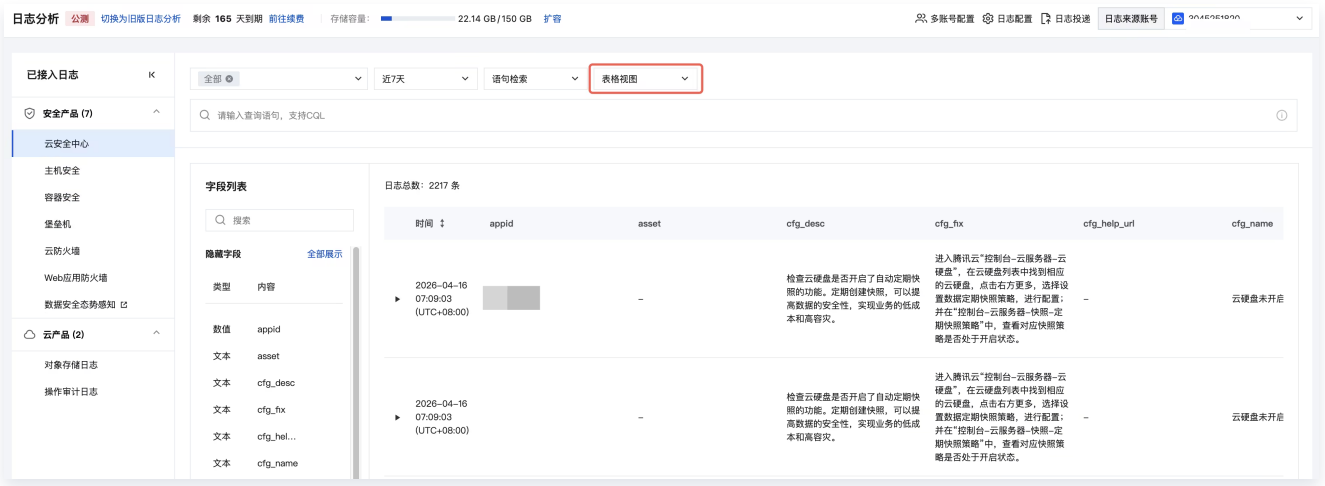


5.3 填写特定的字段值，然后单击**开始检索**。

6. 支持进行视图切换：支持两类视图切换，**原始数据视图**以及**表格视图**。原始数据视图侧重于一条完整的原始日志数据展示，表格视图则是按照字段分列进行展示。
   - 原始数据视图

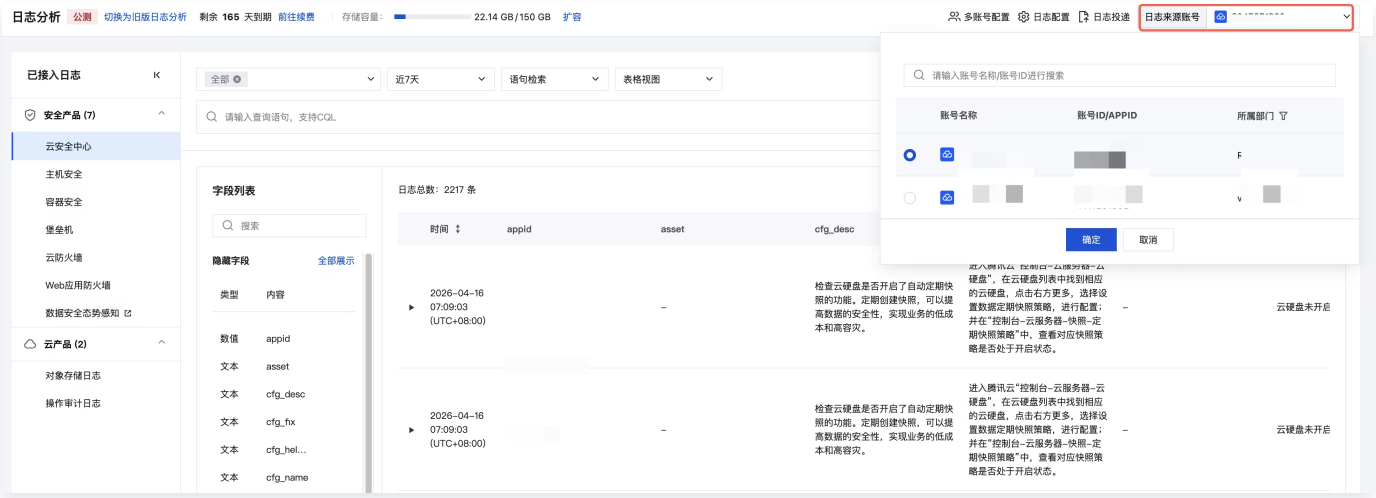


- 表格视图



7. **字段列表：页面左下方展示当前日志的所有可用字段，包括字段名称和类型（文本、数值、时间等）。单击隐藏字段/全部展示可切换字段的显示范围。**

8. 多账号场景下，可以单击**来源账号**选择其他账号，来检索不同账号的日志数据。



多账号配置

最近更新时间：2026-04-30 14:08:12

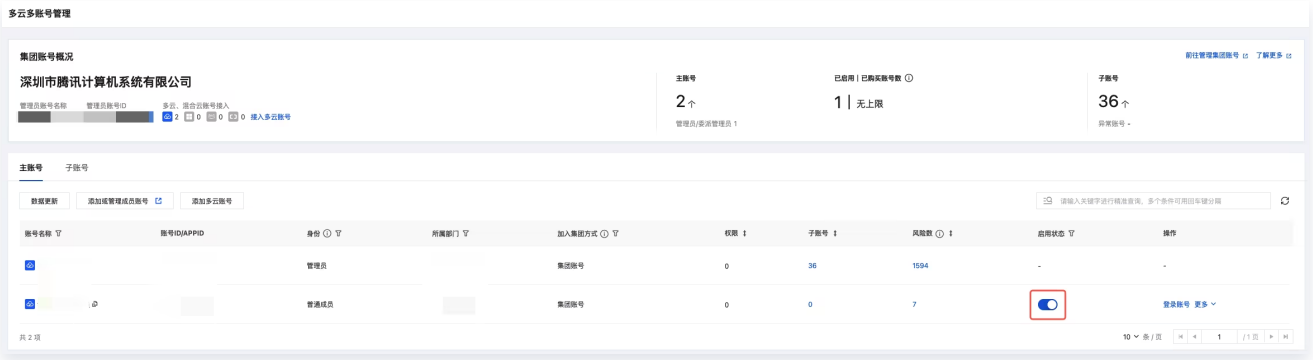
本文介绍多账号场景下，如何将管理员账号的日志存储容量共享给成员账号，包括开启和关闭共享的操作步骤，以及各成员账号标签状态的含义说明。

功能概述

在**多账号场景**下，日志分析模块提供了存储容量共享配置能力，支持管理员账号将日志存储容量灵活共享给多个成员账号，实现跨账号的日志存储资源统一管理与协同运营。

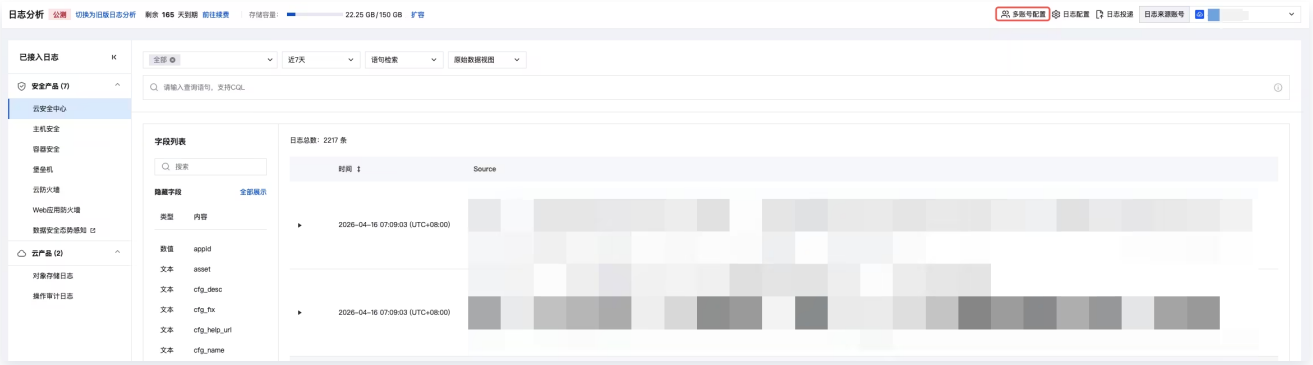
前提条件

1. 当前账号为**管理员账号/委派管理员账号**，并且**已购买**或被**共享了**日志存储容量。
2. 需要在"**多云多账号管理**"中开启成员账号的启用状态，才可以进行存储容量共享。



操作步骤

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**多账号配置**。



3. 在多账号配置-日志分析容量共享页面，通过过滤条件找到需要共享配额的账号，打开共享容量的开关即可实现日志分析容量共享。

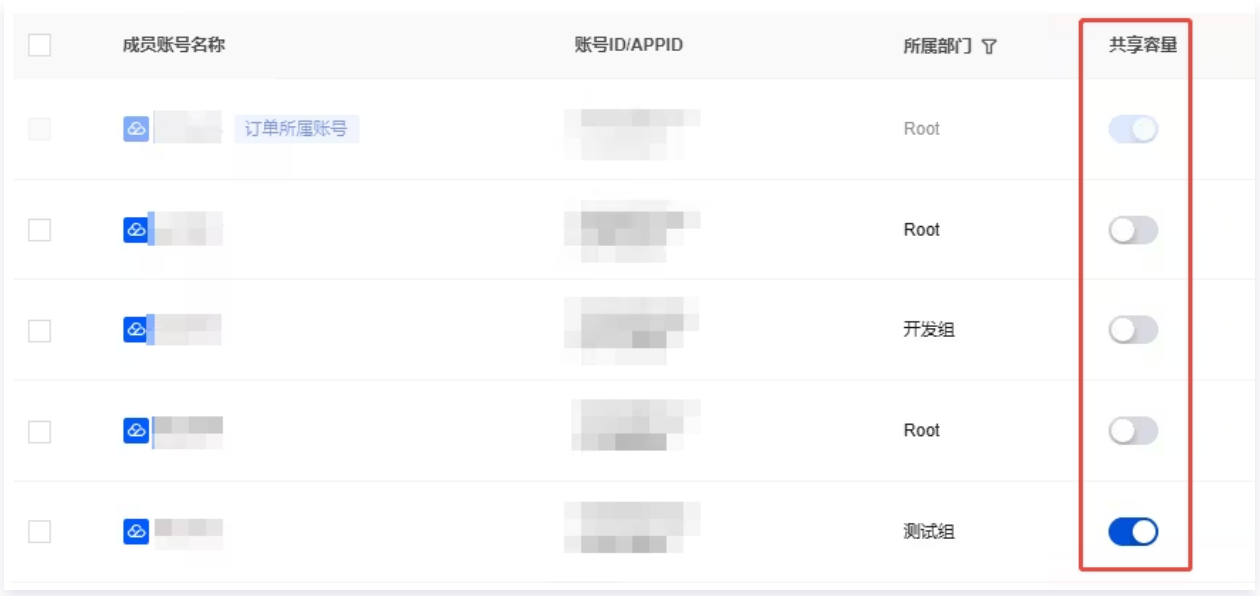
以下为成员账号名称右侧的标签含义说明：

标签	说明
订单所属账号	当前账号购买了日志分析服务的存储容量
自行购买	当前账号已经购买过了日志存储容量，无法共享
已被共享	当前账号已经被其他管理员账号共享了存储容量，无法再次共享
数据清理中	当前账号最近被取消了容量共享，还在清理历史数据，无法开启共享

4. 在多账号配置-日志分析容量共享页面，支持单个或者批量进行容量共享。

> **注意：**
> - 目前只能将容量共享给腾讯云的账号，第三方云账号暂不支持容量配额共享。
> - **取消账号容量共享，将会立即清除该账号的历史数据，且不可恢复。**
> - 开启后，该账号将占用日志分析存储容量，**产生存储容量消耗后将无法退费**。
> - 关闭后，该账号存储的日志数据将**会立即开始清理，请提前做好数据备份**，如通过日志投递到外部存储备份。

- 单个：选择目标成员账号，单击**共享容量开关**，经过二次确认后即可生效。



- 批量开启：选择目标成员账号，单击**批量开启共享/批量关闭共享**，经过二次确认后即可生效。

日志配置

最近更新时间：2026-04-30 14:53:42

本文介绍日志分析服务的日志配置功能，包括存储用量的可视化监控，以及按产品和日志类型配置存储策略的操作步骤。

功能概述

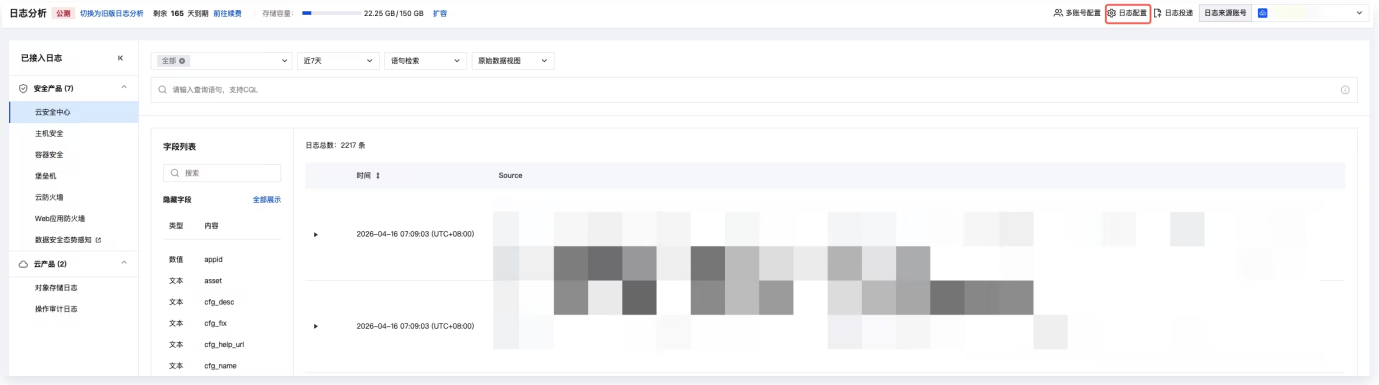
日志配置功能为用户提供日志存储的全局监控与精细化配置能力。

前提条件

1. 已购买 日志分析服务 的账号。
2. 当前的**登录账号**是已经被共享了存储容量的账号。

存储监控

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志配置**。



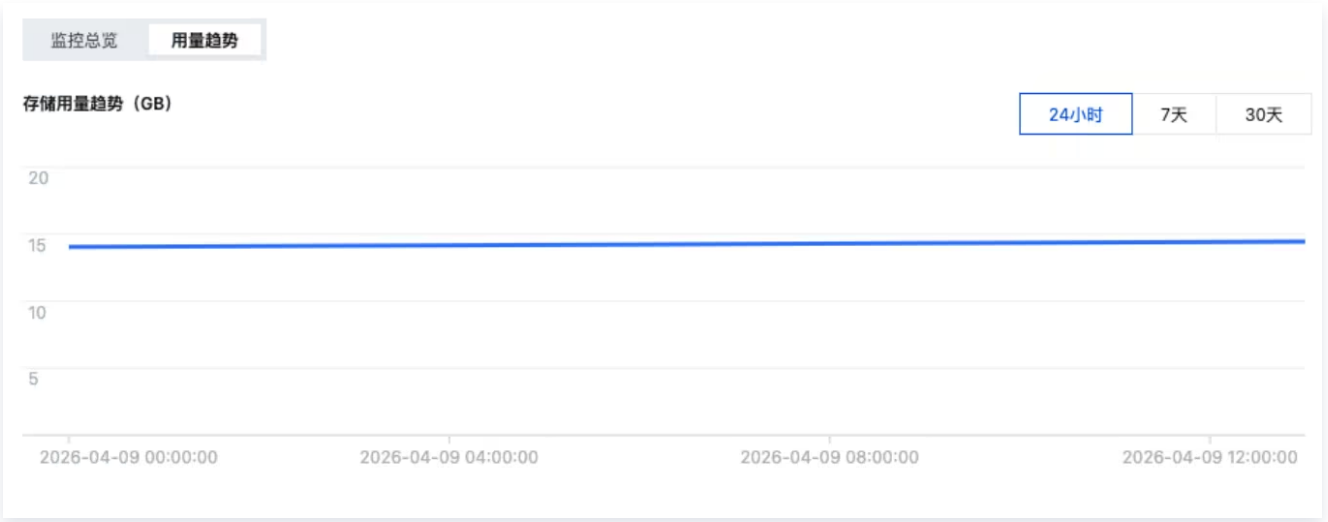
3. 日志配置页面总体分为上下两个模块，上半部分呈现的是存储用量的 可视化监控 ，下半部分是各产品的 存储配置 。

可视化监控

在可视化监控中，支持查看**监控总览**和**用量趋势**。

- **监控总览**：展示总体已使用的存储量及各产品的存储用量分布情况。

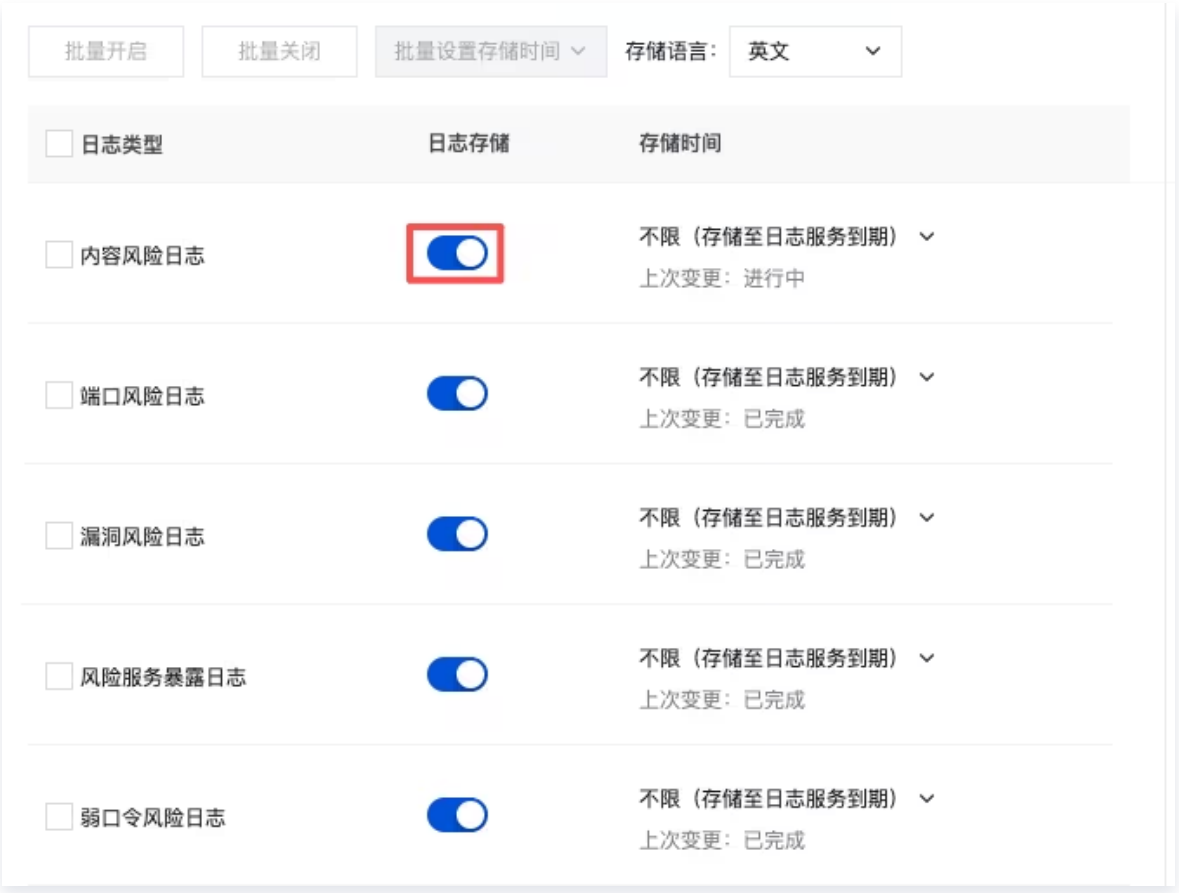
- **用量趋势**：可查看一段时间内的存储用量趋势。默认显示近24小时的用量趋势，您可在右上角切换为"近7天"或"近30天"。



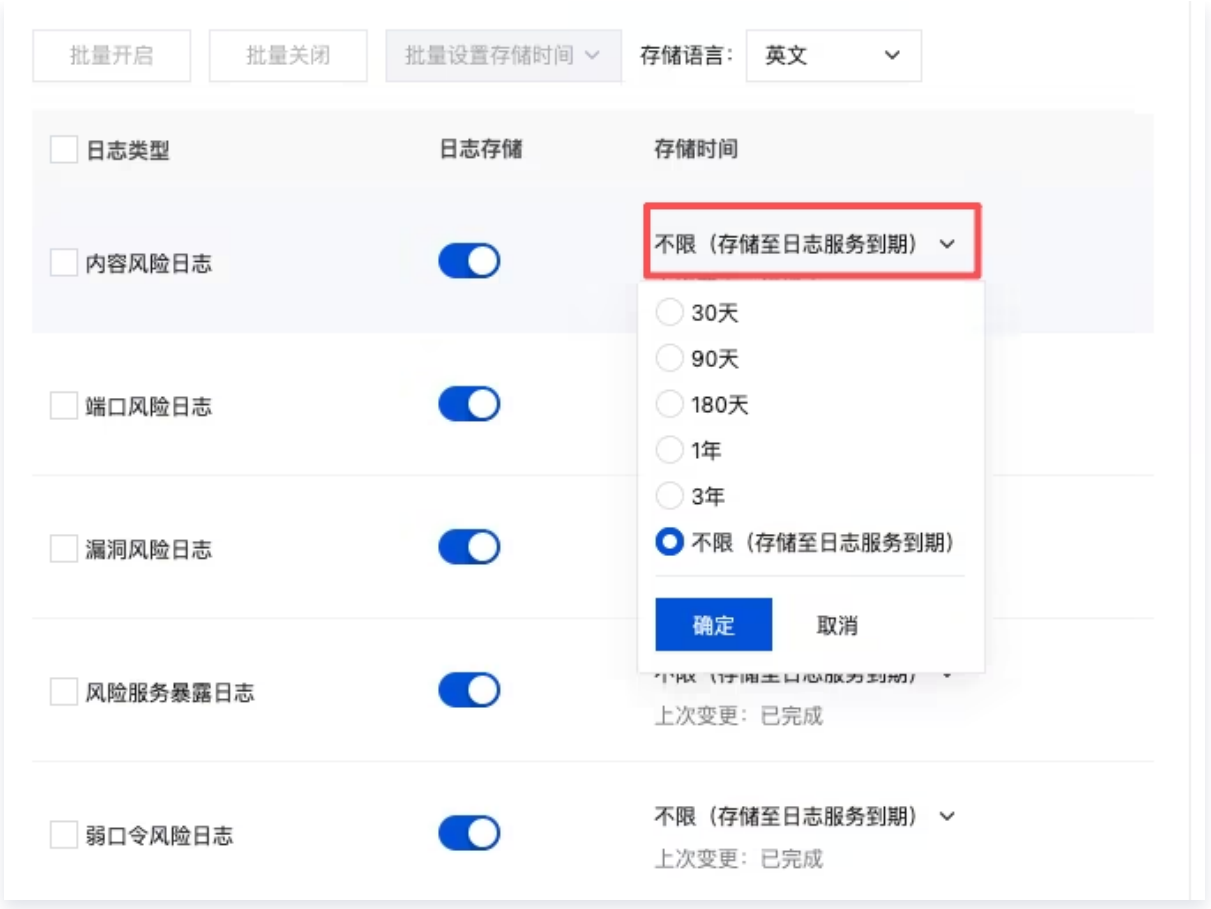
存储策略配置

1. 在存储策略配置中，选择左侧需要**配置存储策略**的产品。

2. 在日志列表中，展示该产品支持配置存储的日志类型，支持按照日志类型配置**是否存储**以及**存储时间**。
   - 打开日志存储开关，则代表该日志类型需要存储。



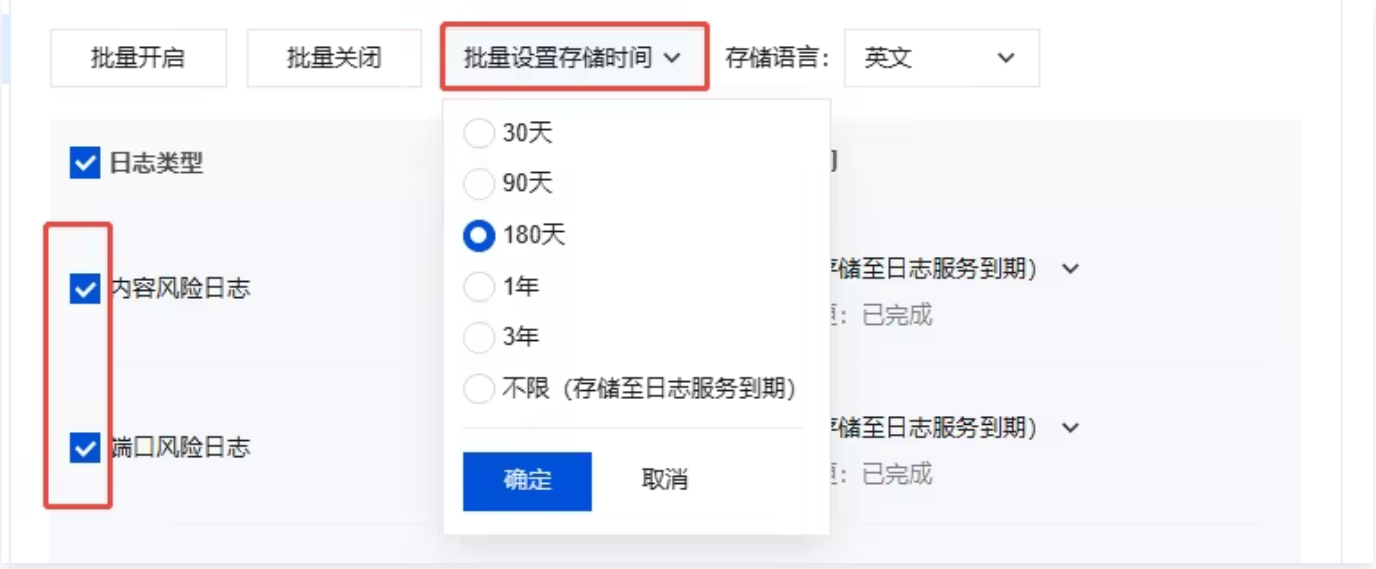
   - 单击**存储时间**，下拉支持修改存储时间，单击**确定**保存。



3. 在日志列表中，支持快捷操作如批量开启、批量关闭、批量配置存储时间。
   - 批量开启：勾选需要操作的日志类型后，单击**批量开启**，经过二次确认即可。

- 批量关闭：勾选需要操作的日志类型后，单击**批量关闭**，经过二次确认即可。

- 批量配置存储时间：勾选需要操作的日志类型后，单击**批量配置存储时间**，选择需要调整的时间，单击**确定**保存。



多账号场景配置说明

多账号场景下，如果您登录的账号是**管理员账号**或者**委派管理员账号**，那么您可以在**日志配置**模块监控您账号管理下的成员账号**存储用量情况**，以及为每一个成员账号**配置存储策略**。

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志配置**。
3. 在日志配置-监控总览中，支持查看各账号用量监控，您可以在上半部分看到各成员账号的存储用量情况。

4. 在日志配置-存储设置中，单击**多账号管理**，选择目标账号，为选中的成员账号配置日志存储策略。

> **说明：**
> 存储策略的配置操作与 常规场景 的配置方式相同。

日志投递
投递至 Kafka

最近更新时间：2026-04-30 14:08:12

本文介绍如何将日志分析模块的安全产品日志实时投递至 Kafka，包括单账号和多账号场景下的完整配置步骤。

功能概述

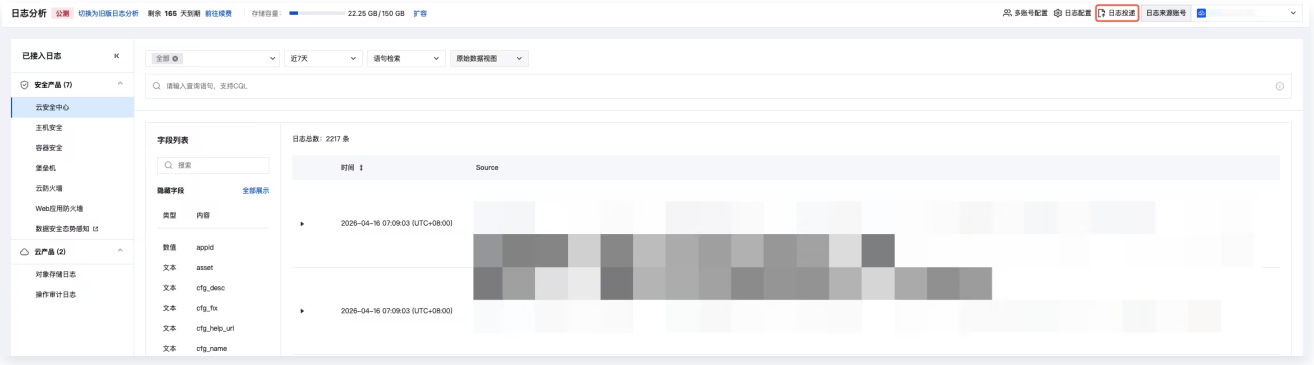
日志投递功能支持将安全产品日志实时投递至 Kafka，满足用户在日志归档、跨平台联动分析及自建安全运营体系等场景下的数据流转需求。同时支持多账号场景下的配置同步，管理员可将投递配置一键同步到其他成员账号。

前提条件

1. 已购买 日志分析服务 的账号。
2. 当前的**登录账号**是已经被 共享了存储容量 的账号。

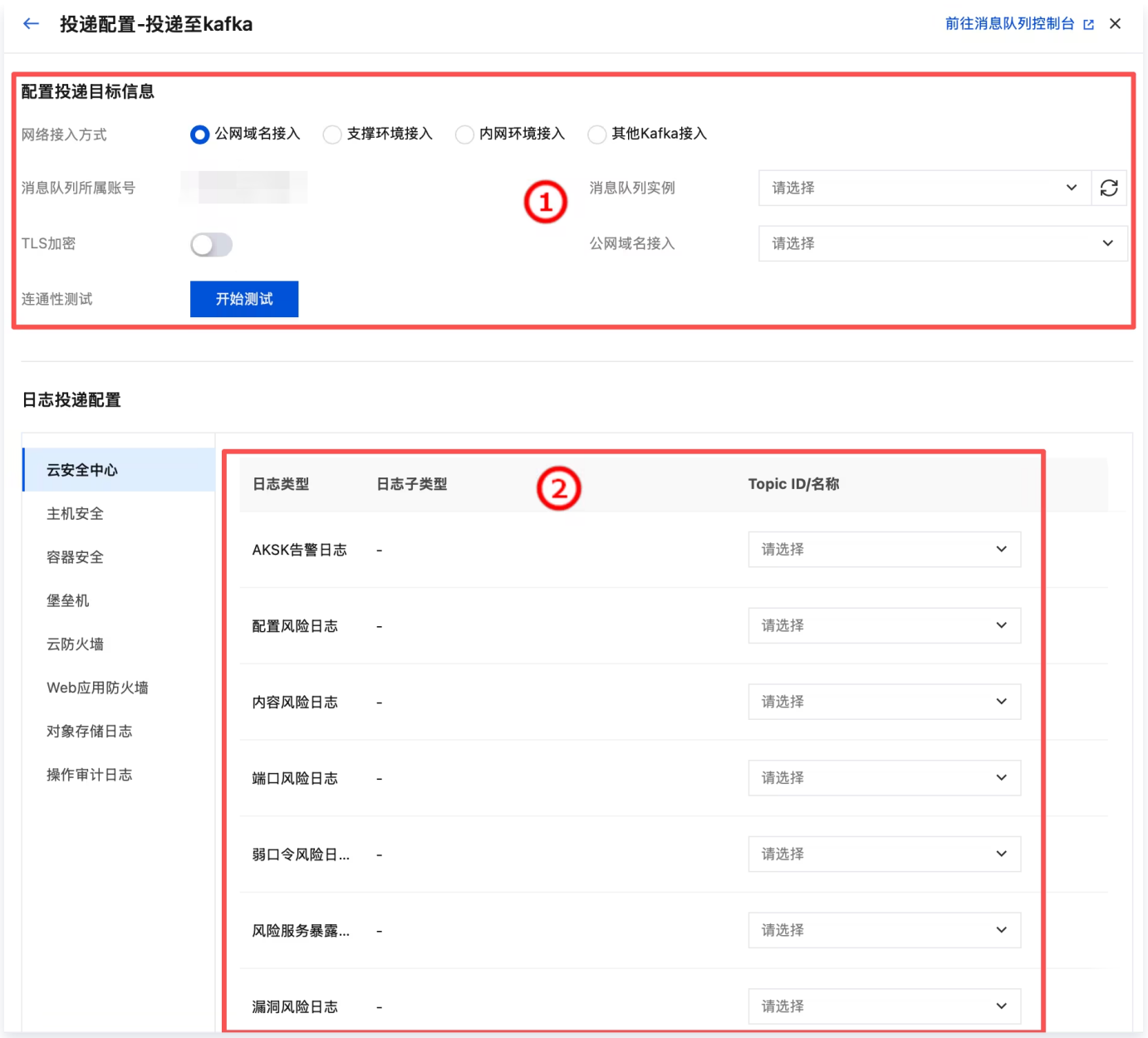
操作步骤

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志投递** > **投递至 Kafka**。



3. 上半部分展示的是投递目标的消息队列详情，下半部分展示的是每一个产品的投递策略配置。

4. 在投递至 kafka 页面，单击右上角的**修改投递配置**。
5. 投递配置策略分为两个配置，①是消息队列的投递目标配置，②是日志投递配置（包括需要投递的日志类型及对应的 kafka 主题）。



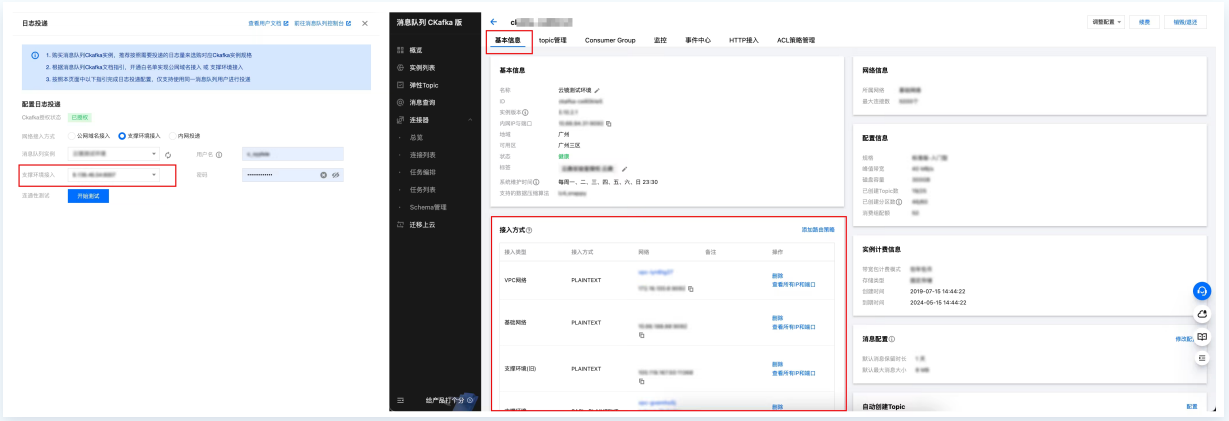
6. 配置消息队列，目前支持四种网络接入方式：公网域名接入、支撑环境接入、内网环境接入、其他 kafka 接入。

接入方式	描述	备注
公网域名接入	通过公网进行日志投递	消息队列实例默认的接入方式
支撑环境接入	通过腾讯云内网进行日志投递，性能稳定，效率更高	是消息队列实例中默认的接入方式，仅支持 SASL_PLAINTEXT 接入方式
内网环境接入	通过腾讯云内网进行日志投递，但路由无需用户在 Ckafka 中进行配置，会自动创建一个不可见的内	-

	部路由来支持接入	
其他 kafka 接入	通过其他 kafka 进行日志投递	-

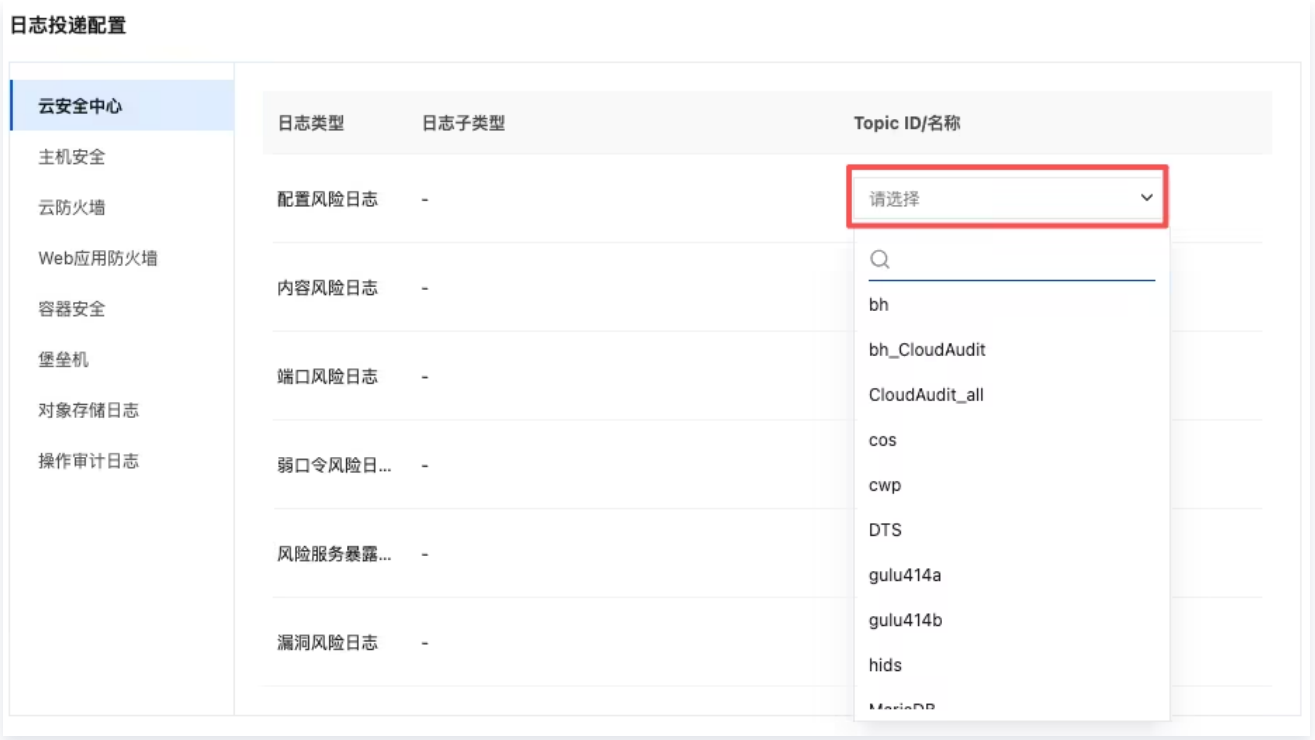
说明：

- 网络接入方式若选择“公网域名接入”、“支撑环境接入”，还需要选择接入路由，路由策略对应 Ckafka 实例列表 详情中的接入方式。

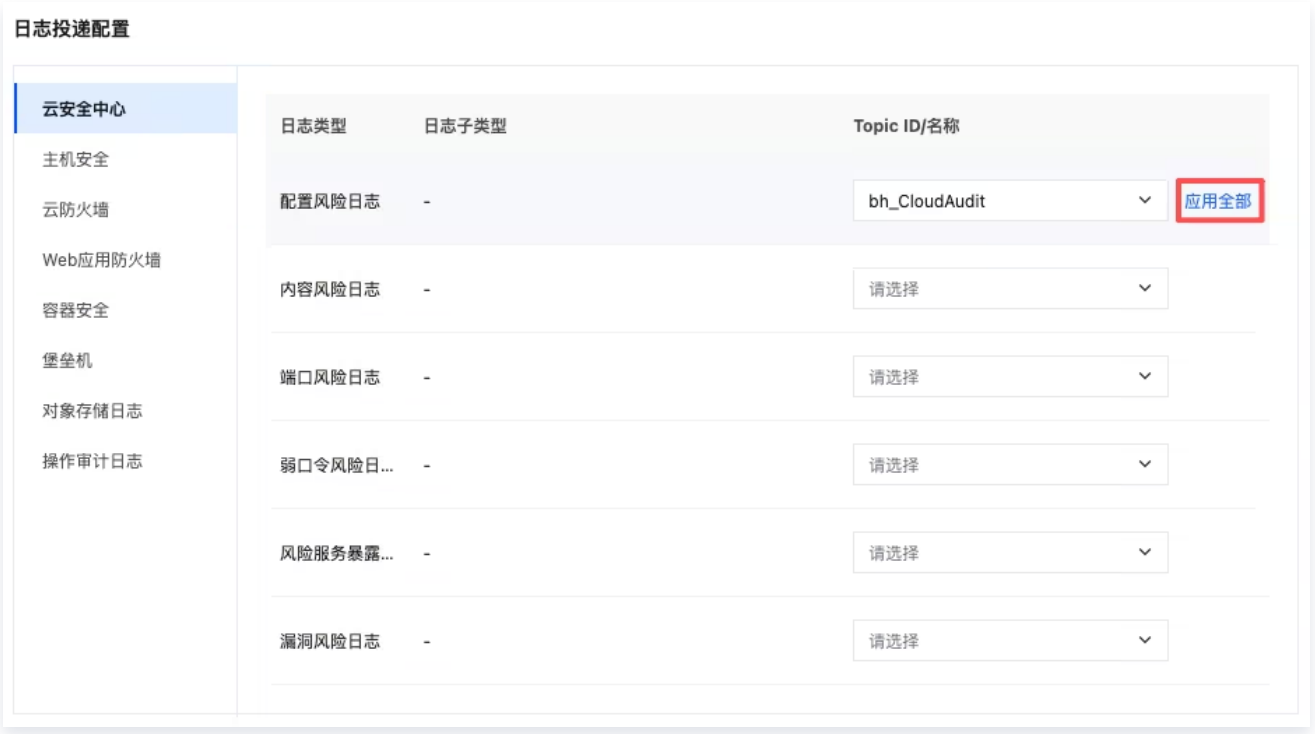


- 网络接入方式若选择“公网域名接入”、“支撑环境接入”，还需要填写 Ckafka 实例的用户名和密码，用户名密码在 Ckafka 实例列表 详情中的 **ACL 策略管理 > 用户管理** 添加。（在配置日志投递时，仅填写#后的用户名即可，无需填写#及其前的 Ckafka 实例 ID。）

7. 完成上述 kafka 配置后需要进行**连通性测试**，测试通过后。您可以给需要投递的日志，配置不同的投递目标（选择目标 Topic）。

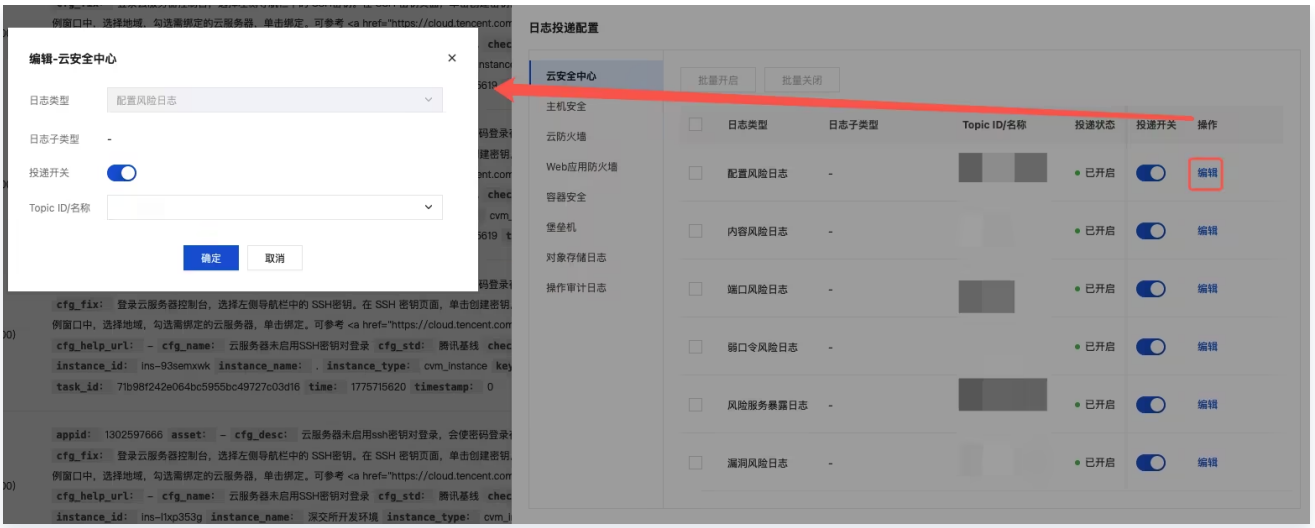


8. 如果所有日志需要投递到同一个 Topic，您可以单击已完成配置的项目，单击右侧的**应用全部**，即可完成**一键应用全部**。



9. 配置完成后单击**确认**，再次进入详情页面，您可以在这里选择开启或中断对应日志的投递开关。支持**单个和批量操作**。

10. 单击**编辑**后，能够修改投递的目标 Topic。



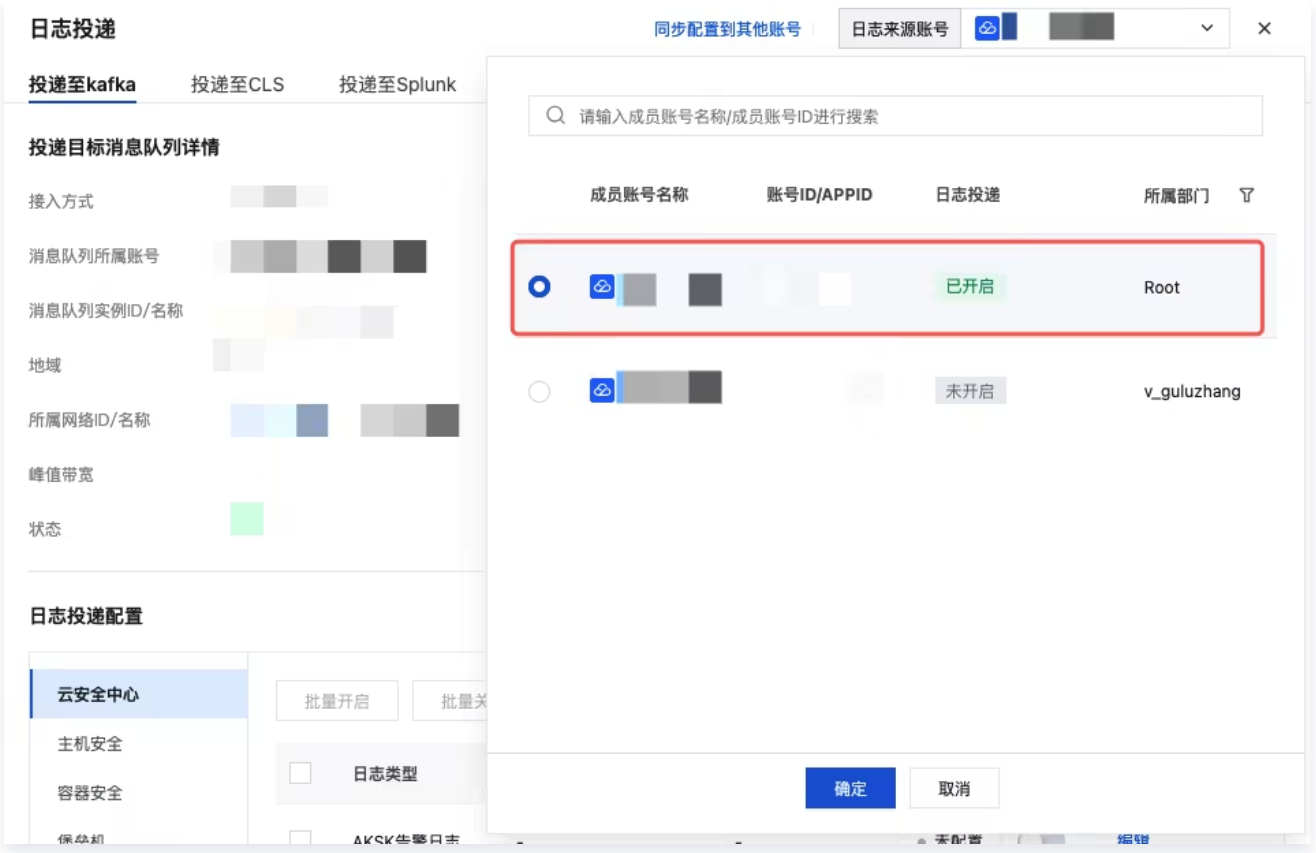
多账号场景

在多账号场景下，如果您使用**管理员账号**或**委派管理员**账号登录，可以在日志投递模块为**成员账号配置投递策略**。与常规使用场景不同，您需要重点关注以下配置项：

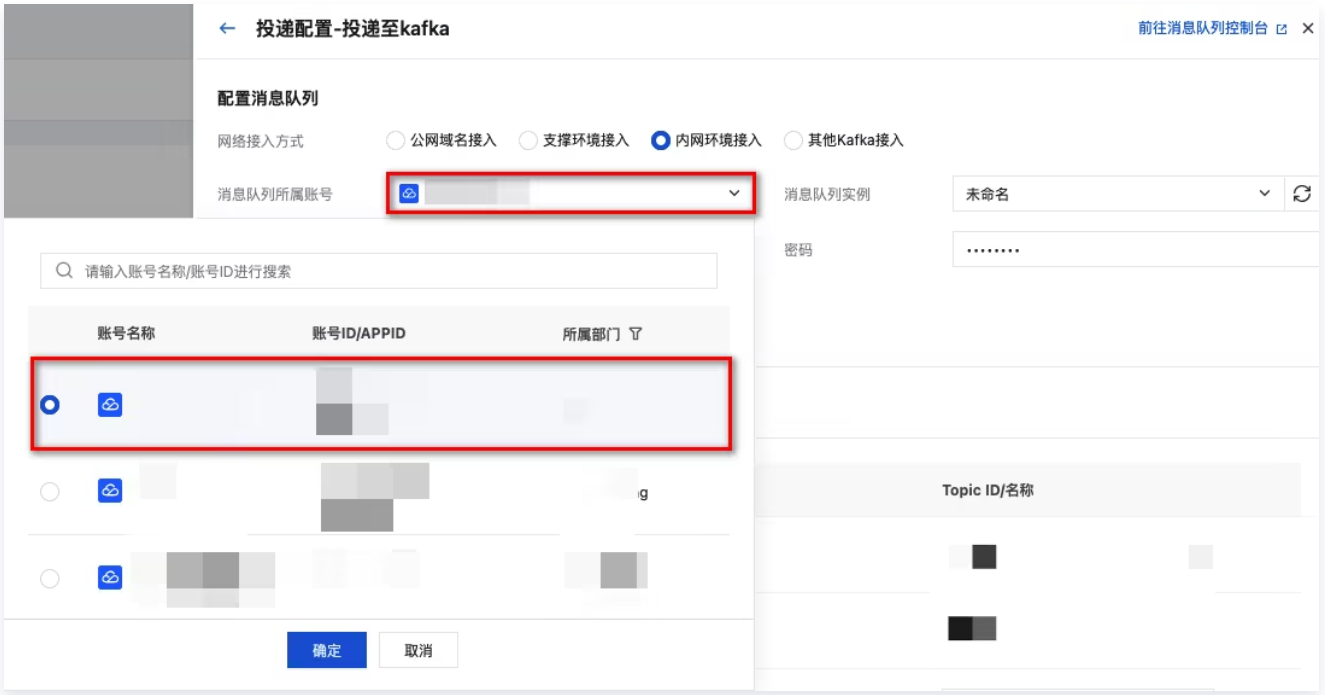
- 日志来源账号（指定要投递的日志所属账号）
- 日志投递目标（指定接收日志的目标账号的 kafka）

> ⚠ **注意：**
> 目标账号需开通 kafka 服务方可使用此功能。

1. 登录 云安全中心控制台，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的日志投递 > 投递至 Kafka。
3. 在日志投递页面，配置日志来源账号和日志投递目标。
   - 日志来源账号，单击左上角的日志来源账号，选择所需成员，单击**确定**即可为当前成员账号的日志配置投递策略。



- 日志投递目标：单击**修改投递配置**，选中**消息队列所属账号**，单击即可切换对应的账号，需要选中的账号开通了 kafka 服务。



4. 其他日志投递配置的操作和常规操作场景一致。

投递至 CLS

最近更新时间：2026-04-30 14:08:12

本文介绍如何将日志分析模块的安全产品日志实时投递至 CLS ，包括单账号和多账号场景下的完整配置步骤。

功能概述

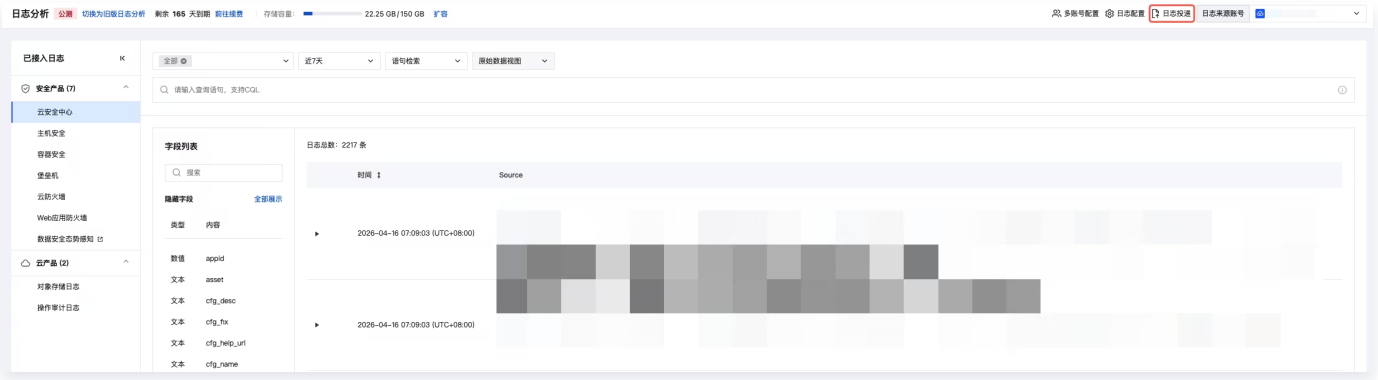
日志投递功能支持将安全产品日志实时投递至 CLS（日志服务），满足用户在日志归档、跨平台联动分析及自建安全运营体系等场景下的数据流转需求。同时支持多账号场景下的配置同步，管理员可将投递配置一键同步到其他成员账号。

前提条件

1. 已购买 日志分析服务 的账号。
2. 当前的**登录账号**是已经被 共享了存储容量 的账号。

操作步骤

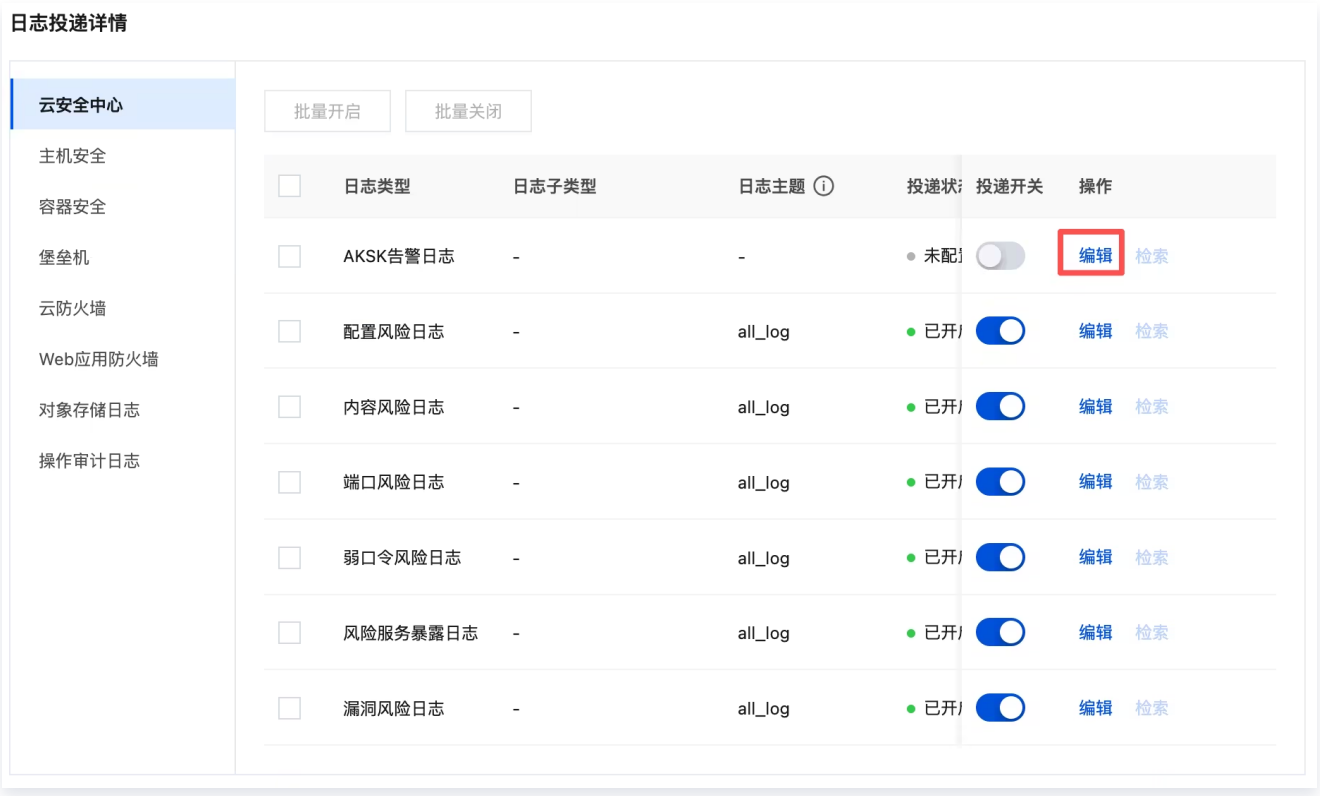
1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志投递 > 投递至 CLS**。



3. 在投递至 CLS 页面，可以为每一个产品进行投递策略配置。

4. 选中需要配置投递策略的产品，单击**编辑**后，可以选择投递目标的日志主题。可以选择已存在的日志集/日志主题，也可以新建日志集/日志主题作为投递目标。

4.1 选中需要配置的日志类型，单击**编辑**。



4.2 选择需要投递的**目标日志集/日志主题**，单击**确定**。

5. 编辑完成后，开启投递开关即可开始投递。投递是实时投递的，没有数据和时间延迟。

6. 投递开关支持批量操作，批量开启和批量关闭。

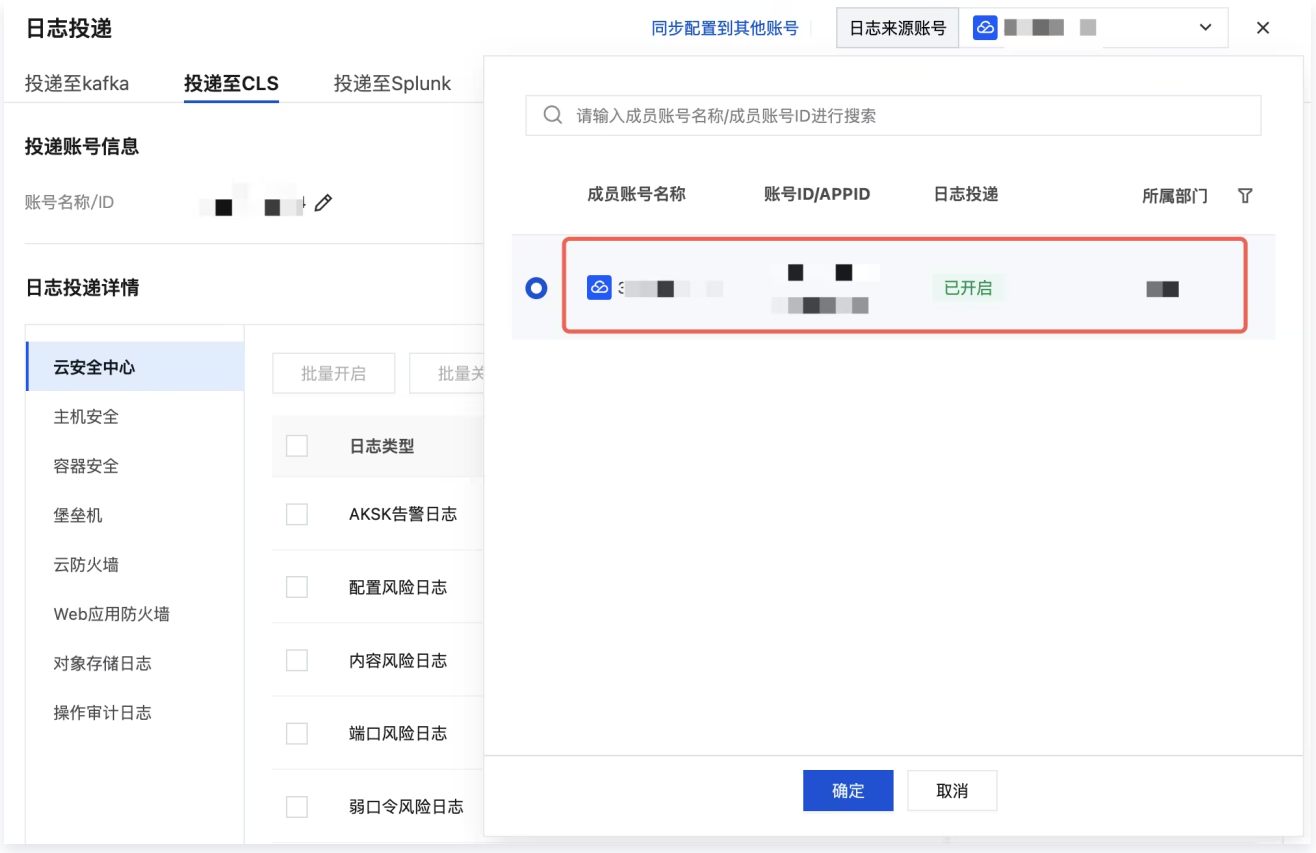
多账号场景说明

在多账号场景下，如果您使用**管理员账号**或**委派管理员**账号登录，可以在日志投递模块为**成员账号配置投递策略**。与常规使用场景不同，您需要重点关注以下配置项：

- 日志来源账号（指定要投递的日志所属账号）
- 日志投递目标（指定接收日志的目标账号的 CLS）

> **注意：**
> 目标账号需开通 CLS 服务方可使用此功能。

1. 登录 云安全中心控制台，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志投递** > **投递至 CLS** 。
3. 在日志投递页面，配置日志来源账号和日志投递目标。
   - 日志来源账号，单击左上角的**日志来源账号**，选择所需成员，单击**确定**即可为当前成员账号的日志配置投递策略。



- 日志投递目标：单击**修改账号名称/ ID 右侧的** ，单击即可切换对应的目标账号，需要选中的账号开通了 CLS 服务。

4. 其他日志投递配置的操作和 常规操作场景 一致。

投递至 Splunk

最近更新时间：2026-04-30 14:08:12

本文介绍如何将日志分析模块的安全产品日志实时投递至 Splunk ，包括单账号和多账号场景下的完整配置步骤。

功能概述

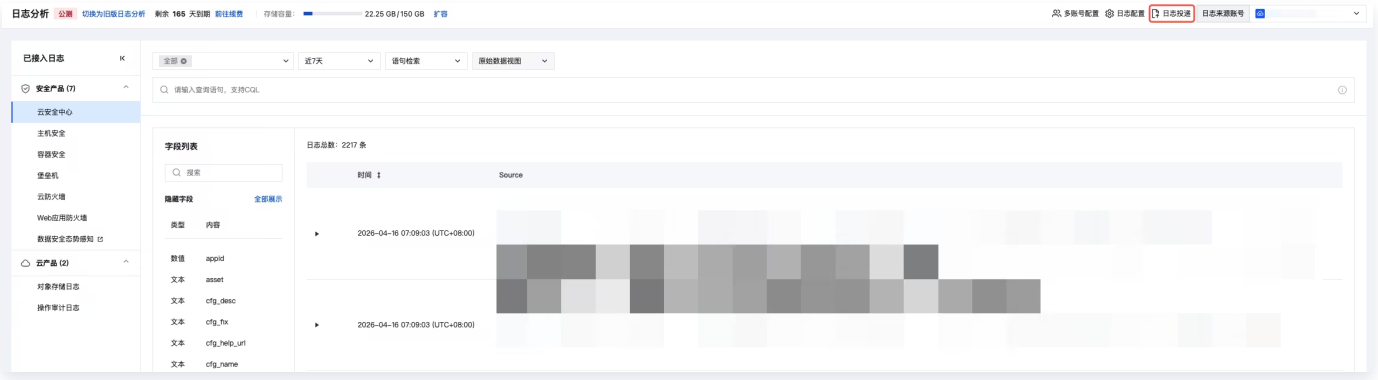
日志投递功能支持将安全产品日志实时投递至 Splunk ，满足用户在日志归档、跨平台联动分析及自建安全运营体系等场景下的数据流转需求。同时支持多账号场景下的配置同步，管理员可将投递配置一键同步到其他成员账号。

前提条件

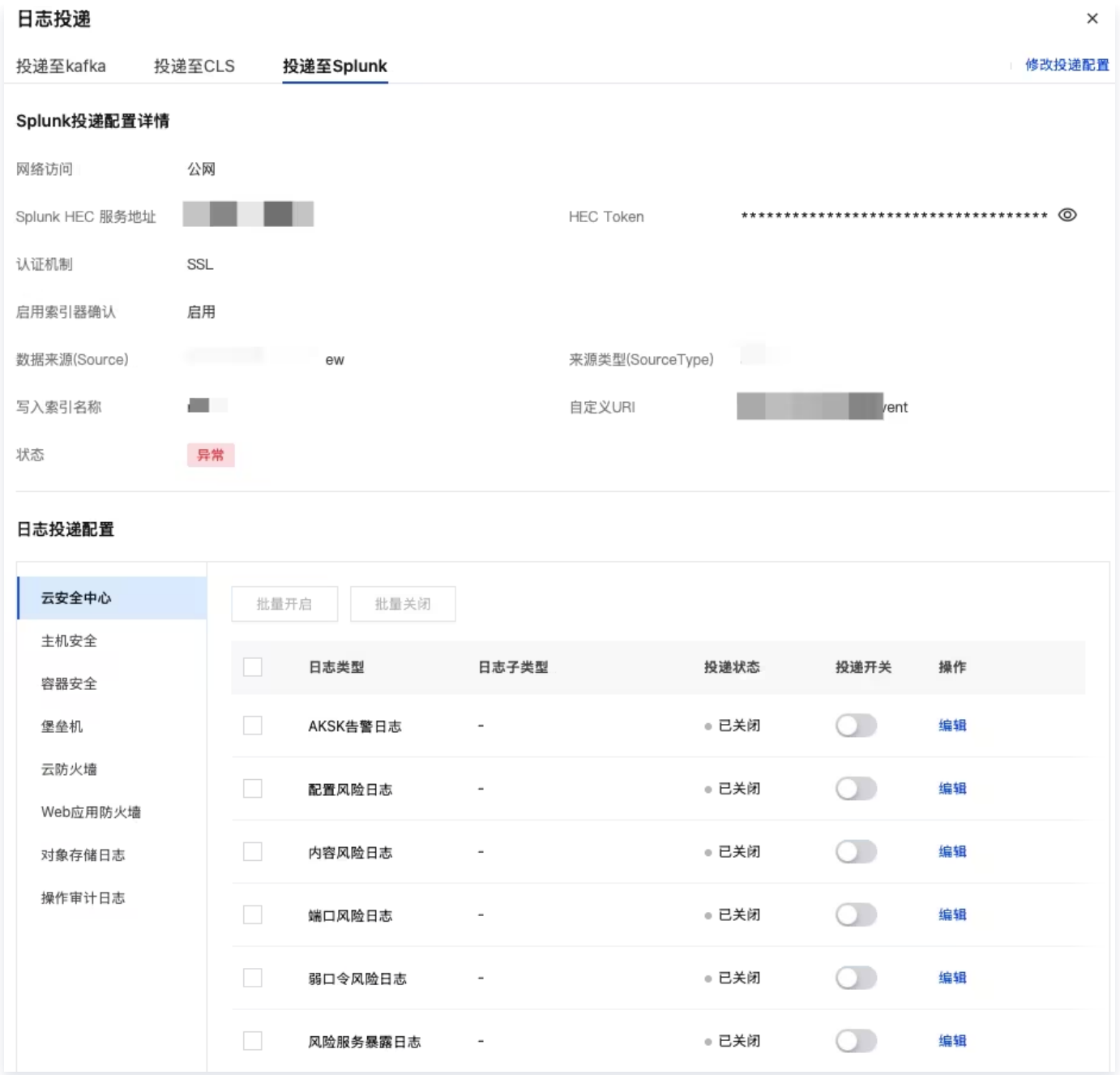
1. 已购买 日志分析服务 的账号。
2. 当前的**登录账号**是已经被 共享了存储容量 的账号。

操作步骤

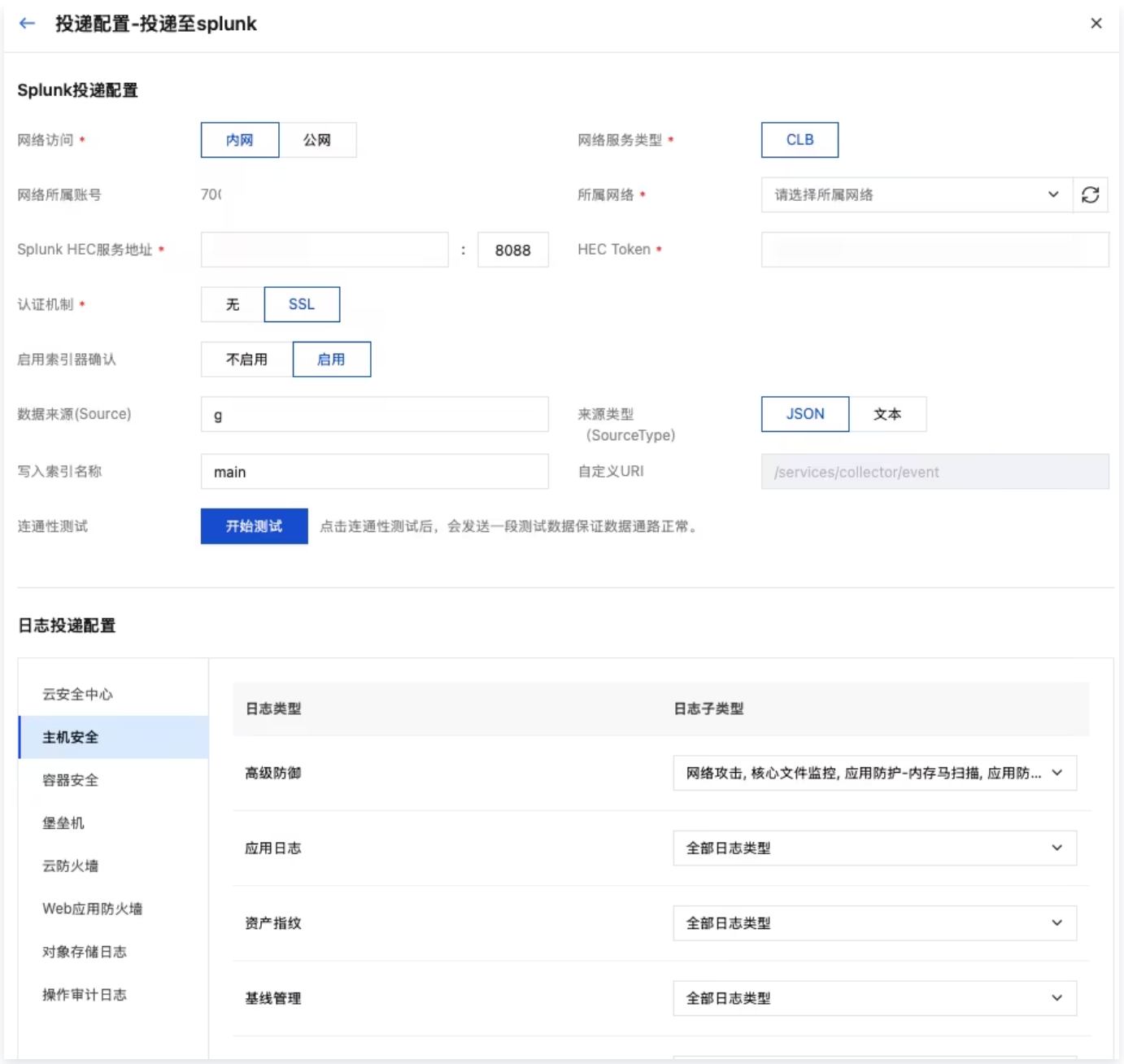
1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 单击日志分析界面右上方的**日志投递 > 投递至 Splunk**。



3. 在投递至 Splunk 页面，上半部分展示的是 Splunk 的配置信息（投递目标信息），下半部分是日志类型的配置项（哪些日志要投递出去）。



4. 在投递至 Splunk 页面，单击右上角的**修改投递配置**。
5. 在投递配置-投递至 Splunk 页面，首先需要编辑 Splunk 的配置信息。



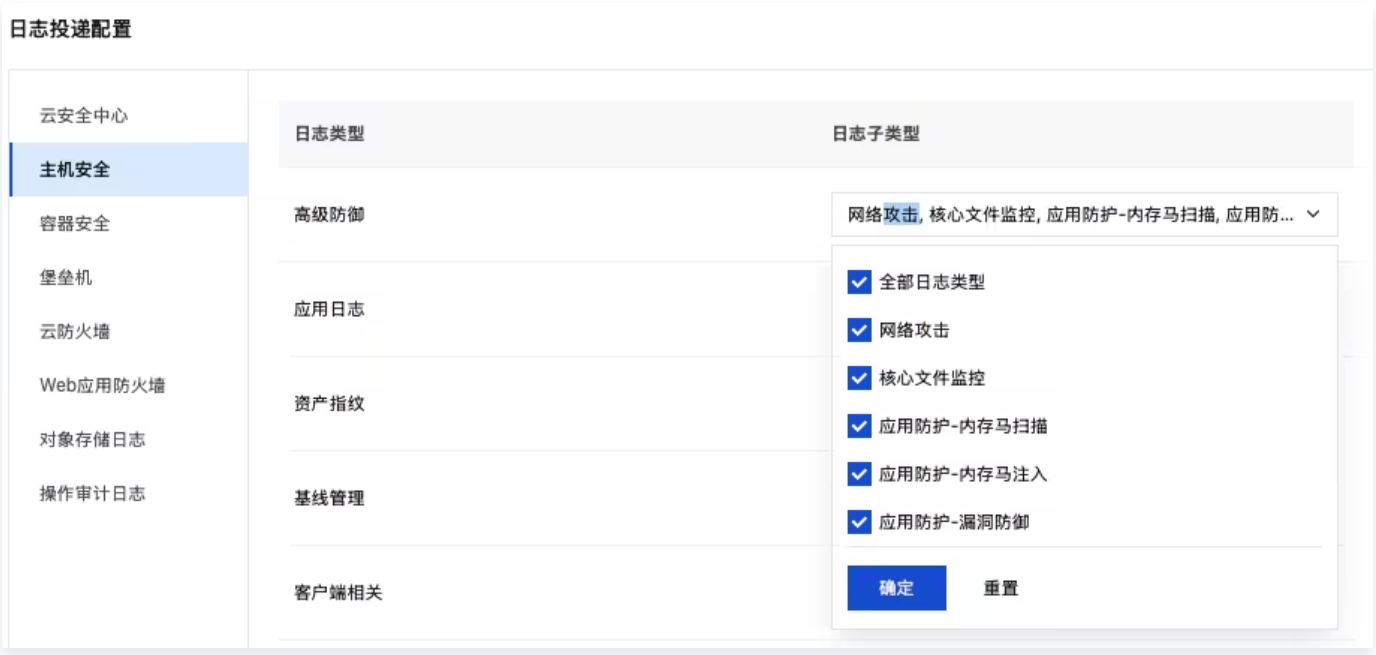
以下为填写配置信息说明：

配置项	说明	示例
网络访问方式	内网：Splunk 部署在腾讯云,或者通过专线/云联网接入腾讯云。 公网：一般指 Splunk Cloud Platform，通过公网访问。	内网/公网
网络服务类型	当前支持 CLB，服务通过 CLB（负载均衡）转发，通常投递目标有多个节点，需要负载均衡。	CLB
网络所属账号	Splunk 部署在当前账号或者其他账号的网络环境中	• 常规场景：当前登录账号，无需选择

		• 多账号场景：可以选择其他账号
所属网络	从下拉列表选择当前账号的 VPC，格式：VpcId|VpcName|CidrBlock。	vpc-r5ABC123
Splunk HEC 服务地址	请在 Splunk 侧获取 详情参考：Splunk Docs - Home	10.0.0.113:8088
HEC Token	请在 Splunk 侧获取 详情参考：Splunk Docs - Home	59f9bXXc-ae2f-43c1-8c93-4360XXXX3ef1
认证机制	如果您在 Splunk 的 HEC 的配置中打开了 SSL 认证，请选择 SSL	SSL
启用索引器确认	Splunk 确认来自 HEC 的数据写入索引后，再处理下一批数据。如果您在 HEC 标记启用了索引器确认，请选择启用	启用
数据来源	日志生成的位置，如目录、网络端口、程序名称	/var/log/syslog
来源类型	日志数据格式/结构，决定了 Splunk 如何解析数据	JSON、文本
写入索引名称	将数据写入该索引	test_index
自定义 URI	目标投递的路径	固定为/services/collector/event
连通性测试	需要进行连通性测试，成功后才可以进行投递	测试数据：hello world

6. 在日志投递配置中，您需要在这里编辑哪些日志需要投递出去。
    - 没有日志子类型的默认选择全部，无需操作。

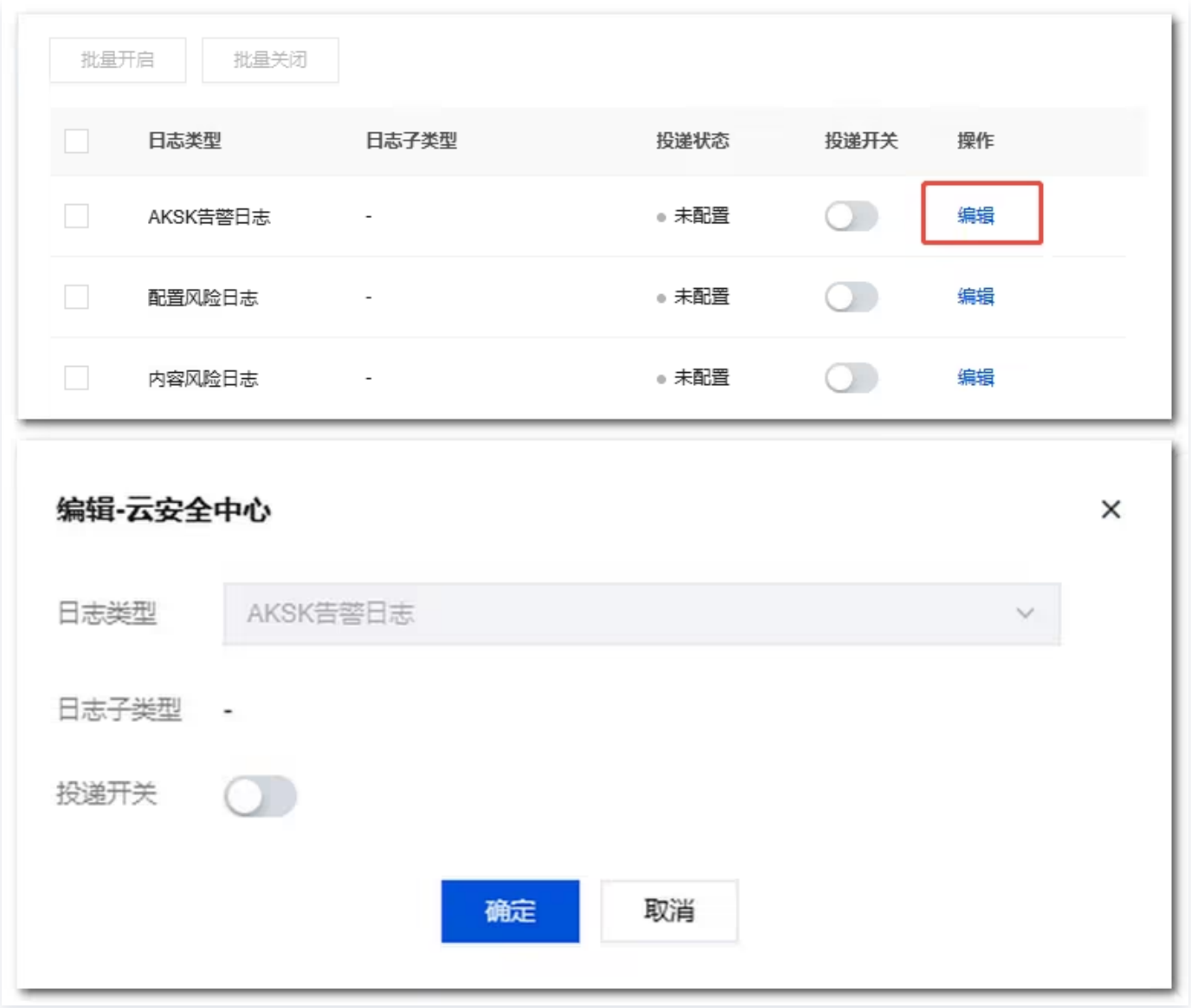
- 存在日志子类型的产品，需要选择哪些日志子类要投递出去。



7. 单击**确定**后，回到详情页面，支持单个或者批量操作。

8. 您也可以在投递至 Splunk 页面修改投递的日志类型，但仅支持具有子类型的日志进行修改。

> **注意：**
> 投递到 Splunk 必须要通过连通性测试，保证通路正常，否则无法投递。连通性测试时会发送一段测试数据到目标 Splunk 用于测试。



多账号场景说明

在多账号场景下，如果您使用**管理员账号**或**被委派管理员**账号登录，可以在日志投递模块为**成员账号配置投递策略**。与常规使用场景不同，您需要重点关注以下配置项：日志来源账号（指定要投递的日志所属账号）。

1. 登录 云安全中心控制台，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志投递** > **投递至 Splunk**。
3. 在投递至 Splunk 页面，配置日志来源账号。
   - 日志来源账号：单击左上角的日志来源账号，选择所需成员，单击**确定**即可为当前成员账号的日志配置投递策略。

4. 日志投递的策略配置操作和 常规场景 一致。

快捷同步配置

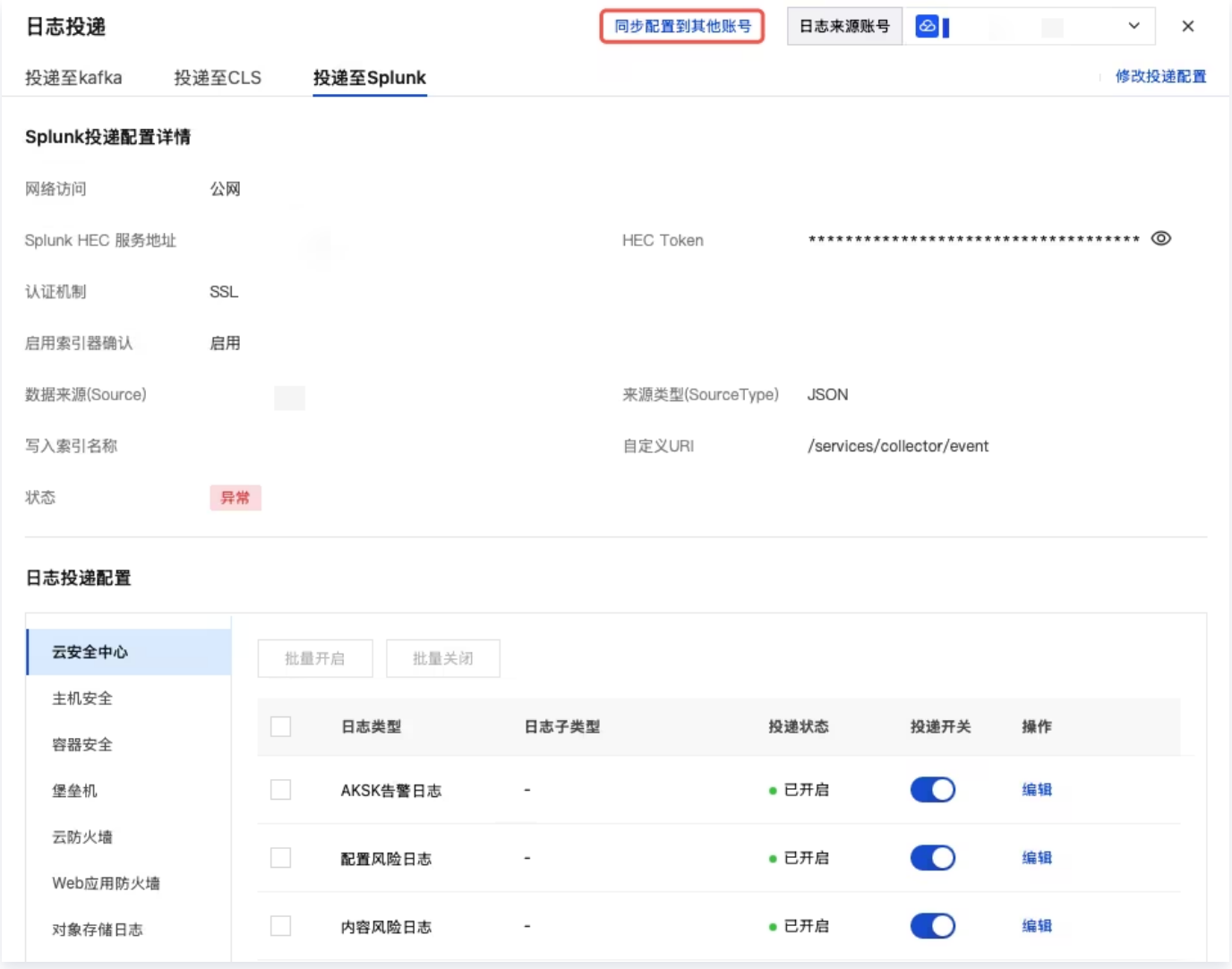
最近更新时间：2026-04-30 14:08:12

功能概述

本文介绍了在多账号场景下，管理员账号/委派管理员账号如何快速的为成员账号进行投递策略配置。

操作步骤

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击右上方的**日志投递**。
3. 在多账号场景下，日志投递的配置支持**快捷的同步配置**操作，单击**同步配置到其他账号**。



4. 在同步配置到其他账号窗口中，需要您确认是否覆盖其他账号的配置信息，单击**全部覆盖**将会把当前的配置同步给列表中的账号。


同步配置到其他账号
预计5分钟内同步完成
该操作会把当前配置同步到订单内所有具备分析权限的账号，以下 1 个账号已有配置，请选择跳过或覆盖 收起
账号名称
账号ID/APPID
已配置
未配置
我的电脑
kafka、cls、splunk
无
全部覆盖（替换已配置账号）
取消

续费与扩容

最近更新时间：2026-04-30 14:08:12

本文介绍日志分析服务的续费与扩容操作，续费用于延长服务到期时间，扩容用于增加日志存储容量，均需通过**订单所属账号**执行。

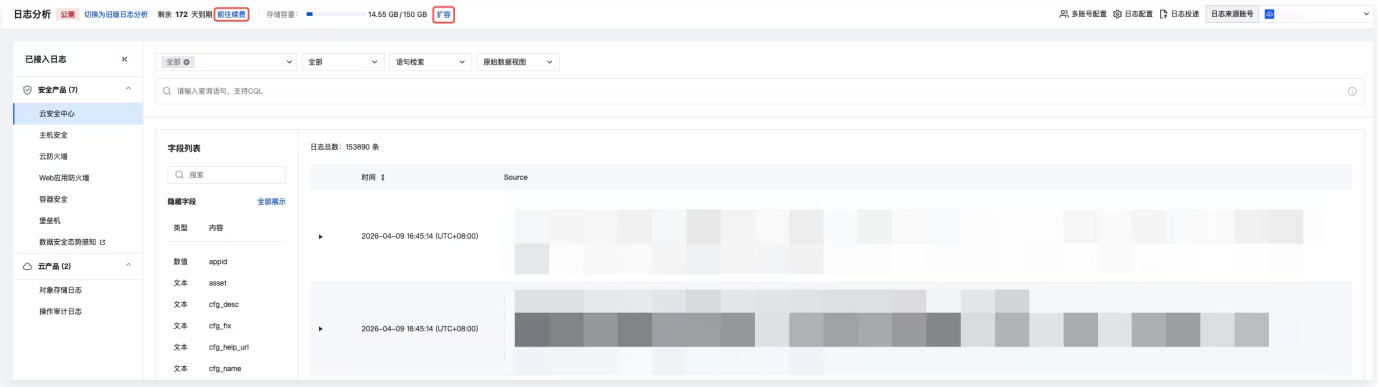
前提条件

1. 当前账号必须已开通并已购买过 日志分析服务 。
2. 多账号场景下，只有订单所属账号能够操作续费和扩容。

续费

续费操作指的是延长当前日志分析的**服务到期时间**，在主页面中能够看到日志分析的**剩余服务时间**，登录**订单所属账号**后，您可以单击**续费**跳转到购买页进行续费。

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击左上方的**续费**。



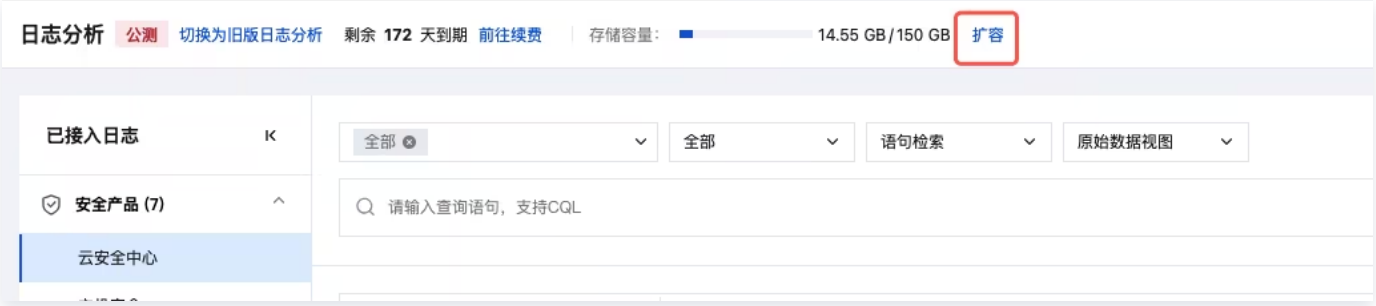
3. 在购买页面，选择需要续期的服务时长，单击**立即购买**即可。

扩容

扩容指的是当前日志存储容量的增加，**该操作不会增加服务时间**。

> **说明：**
> 为了保证数据的完整性，建议您在用量达到 **80%前** 进行扩容。

1. 登录 云安全中心控制台 ，在左侧导航中，单击**日志分析**。
2. 在日志分析页面，单击左上方的**扩容**。



3. 在购买页面，填写需要扩容的容量，单击**立即购买**即可完成购买。

常见问题

最近更新时间：2026-04-30 14:53:42

本文汇总了日志分析服务使用过程中的常见问题与解答，涵盖日志投递、多账号容量共享、存储策略、续费扩容等方面的典型疑问。

服务开通与权限

1. 未购买日志分析服务，是否可以使用?

可以，但需要满足以下条件：您的账号已被管理员账号共享了日志存储容量。在多账号场景下，管理员可以通过多账号配置功能将存储容量共享给成员账号，被共享的账号无需单独购买即可使用日志分析服务。

2. 多账号场景下，如果为成员账号配置日志投递，是否需要成员账号购买 Kafka 或者 CLS 服务?

不需要，您可以选择将日志投递到开通服务的账号中。投递的目标可以是一致的。

日志检索与分析

1. 检索不到日志数据可能是什么原因?

- 日志存储未开启：在日志配置中确认目标产品的日志类型已开启存储开关。
- 时间范围选择不当：检查检索时间范围是否覆盖了目标日志的产生时间。
- 多账号场景下来源账号未切换：在页面右上角日志来源账号中确认已选择正确的来源账号。
- 存储时间已过期：如果存储时间设置较短（如 30 天），超出存储时限的历史日志会被自动清理。

2. 语句检索（CQL）和过滤检索有什么区别? 应该使用哪种?

对比项	语句检索（CQL）	过滤检索
使用方式	在搜索栏中手动输入 CQL 查询语句	通过可视化界面选择字段、条件和值
适用场景	多条件组合的复杂查询、精准分析	快速筛选、简单条件过滤
学习成本	需要了解 CQL 语法规则	无需编写语句，上手简单
推荐人群	安全运维工程师、高级分析师	所有用户

> **注意：**
> 日常快速查询使用过滤检索，复杂分析场景使用 CQL 语句检索。

日志配置与存储

1. 将存储时间从大改小（例如从不限时间改为 180 天），数据会如何处理?

系统会从最晚一条数据开始向上倒推，仅保留最近指定天数的数据，超出时限的历史数据将被清除。例如，将存储时间从不限时间改为 180 天，系统将清除 180 天之前的所有日志数据，且不可恢复。

多账号配置与容量共享

1. 取消容量共享后，成员账号的日志数据会怎样?

取消容量共享后，该成员账号的历史日志数据将被**立即清除，且不可恢复**。

2. 成员账号标签显示数据清理中，何时可以重新开启共享?

数据清理中表示该账号最近被取消了容量共享，系统正在清理历史数据。需要等待数据清理完成后，标签状态更新后方可重新开启共享。清理时间取决于数据量大小。

3. 第三方云账号可以使用容量共享功能吗?

暂不支持。目前容量共享仅支持将容量共享给腾讯云账号，第三方云账号（如 AWS、Azure 等接入的账号）暂不支持容量配额共享。

日志投递

1. 日志投递是实时还是非实时的?

日志投递是实时的，开启投递开关后将会立即进行投递。

2. 日志投递至 Kafka 时，连通性测试失败怎么办?

请按以下步骤排查：

- 检查网络接入方式：确认选择的接入方式（公网域名/支撑环境/内网环境/其他 Kafka）与实际网络环境一致。
- 检查用户名密码：如果使用**公网域名接入**或**支撑环境接入**，需要填写 Kafka 实例的用户名和密码。注意：用户名仅填写 # 号后面的部分，无需填写 CKafka 实例 ID。
- 检查 CKafka 实例状态：确认 CKafka 实例处于正常运行状态。
- 检查 ACL 策略：确认 CKafka 实例的 ACL 策略允许当前用户访问。
- 检查 TLS 配置：如果开启了 TLS 加密，确保 CKafka 实例也已启用对应的 SSL 接入方式。

3. 一个日志类型可以同时投递到 Kafka、CLS 和 Splunk 吗?

可以。Kafka、CLS、Splunk 三种投递通道相互独立，同一日志类型可以同时配置投递到多个目标平台。

4. Splunk 投递是否支持跨账号投递?

Splunk 投递使用内网接入方式时，目前只能选择投递到自己账号的 VPC 资源，暂不支持跨账号投递。

续费和扩容

1. 续费和扩容有什么区别?

对比项	续费	扩容
作用	延长日志分析服务的有效期	增加日志存储容量上限
影响范围	服务到期时间	存储容量
互相关系	不增加存储容量	不延长服务时间

2. 存储容量满了会怎样?

当存储容量达到上限后，新的日志数据将无法继续存储。建议在容量使用接近上限时及时进行扩容，或通过调整存储时间（缩短不常用日志类型的存储时长）释放空间。

附录术语表

术语	英文	说明
CQL	Cloud Query Language	云安全中心内置的日志检索查询语言，支持多条件组合与复杂查询
CLS	Cloud Log Service	腾讯云日志服务，用于日志采集、存储、检索与分析
CKafka	Cloud Kafka	腾讯云消息队列服务，基于 Apache Kafka
HEC	HTTP Event Collector	Splunk 的 HTTP 事件收集器，用于通过 HTTP(S) 接收日志数据
VPC	Virtual Private Cloud	虚拟私有网络
CLB	Cloud Load Balancer	腾讯云负载均衡
ACL	Access Control List	访问控制列表
SASL_PLAINTEXT	–	一种 Kafka 认证接入方式

系统设置
通知中心

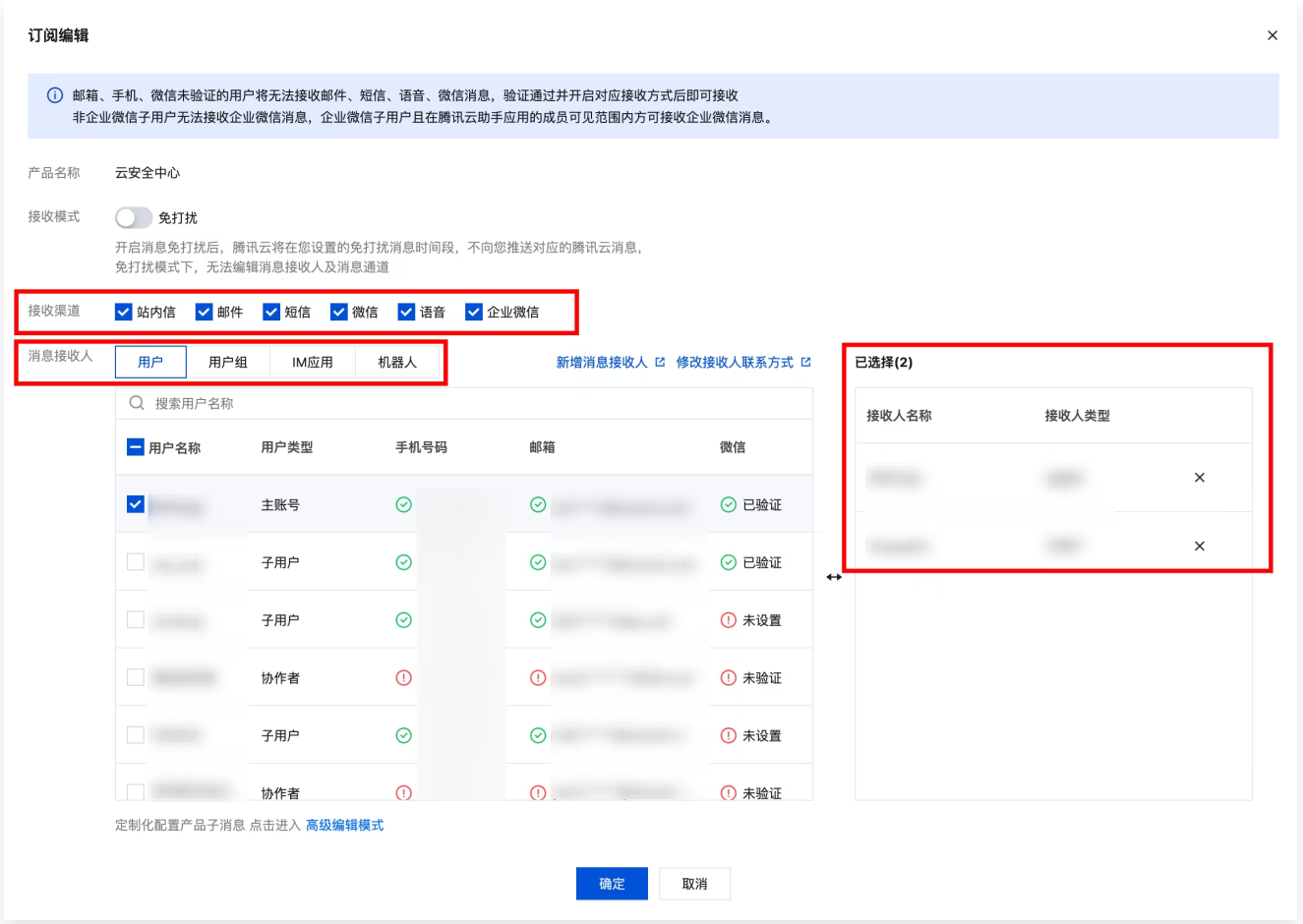
最近更新时间：2026-04-30 14:08:13

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**通知中心** > **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**通知中心 > 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**。

注意：

目前版本云安全中心中包含部分原主机安全的功能，如漏洞治理、告警中心、主机防护、应用防护等，因此这部分的通知无法通过以上章节的配置生效，需通过通知中心 > 主机安全通知配置生效，该配置与主机安全控制台的告警通知设置一致。