

# 云安全中心

## 云安全中心（旧版）

### 产品文档



**【版权声明】**

©2013–2026 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其他腾讯云服务相关的商标均为腾讯集团下的相关公司主体所有。另外，本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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。

# 文档目录

## 云安全中心（旧版）

### 产品简介

#### 产品概述

### 购买指南

#### 计费概述

#### 购买方式

#### 续费说明

#### 欠费说明

#### 退费说明

### 快速入门

### 操作指南

#### 多云多账号管理

##### 多云接入

##### 多账号管理

#### 漏洞与风险中心

#### 告警中心

#### 日志投递（支持多账号多产品多日志）

#### 资产中心

#### 安全体检

##### 功能简介

##### 操作指引

##### 添加白名单 IP

##### 热点问题

#### 云 API 异常监测

##### 功能简介

##### 云 API 密钥安全使用方案

##### 统计面板

##### 资产列表

##### 账号列表

##### 告警

##### 配置风险

##### 策略管理

#### 用户行为分析（UEBA）

#### 报告下载

# 云安全中心（旧版）

## 产品简介

## 产品概述

最近更新时间：2023-09-21 17:24:47

## 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、模拟攻击防护验证。

## 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。

### 立体防护

- 安全全景图：支持企业用户批量开通云防火墙、Web 应用防火墙、主机安全、容器安全、云安全中心的产品试用（具体试用规则以相应产品界面展示为准）。了解云原生三道防线构成，快捷跳转各产品控制台。



- 一站防漏洞：基于安全专家实时更新的热门漏洞列表，一键检测受漏洞影响资产，并使用云防火墙、Web 应用防火墙防御漏洞，使用主机安全修复漏洞。

## 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。

## 模拟攻击

根据用户授权，通过模拟攻击者的思考和工作方式，基于 MITRE ATT&CK 框架自动化模拟战技、战术，从攻击视角看待各种云上安全威胁，帮助用户识别可能被攻击的不同路径和影响力较大的安全威胁，发现安全防护产品的不足及对应安全策略是否配置得当，合理利用安全资源、降低云上风险。

## 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。

## 处置响应

由云安全中心下发到三道防线（云防火墙、Web 应用防火墙、主机安全）的操作，如对告警的响应和风险的处置，会记录在处置响应模块。

## 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。

# 购买指南

## 计费概述

最近更新时间：2025-08-18 17:23:04

### 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    |              | 高级版              | 企业版                  | 旗舰版       | 弹性拓展                |
|---------|--------------|------------------|----------------------|-----------|---------------------|
| 基础价格    |              | 375美元/月          | 1,000美元/月            | 2,667美元/月 | —                   |
| 可购买时长   |              | 3个月、6个月、1年、2年、3年 | 1个月、3个月、6个月、1年、2年、3年 |           | —                   |
| 资产与风险管理 | 资产管理         | 支持               | 支持                   | 支持        | —                   |
|         | 资产体检         | 400次/月           | 1,200次/月             | 4,800次/月  | 0.83美元/次/月，扩展步长300次 |
|         | 扫描任务管理       | 1                | 10                   | 20        | 50，可扩展至不限制          |
|         | 端口扫描         | 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        | —                   |
|         | 内容扫描（网站内容风险） | —                | 支持                   | 支持        | —                   |

|         |                 |           |           |            |                                            |
|---------|-----------------|-----------|-----------|------------|--------------------------------------------|
| 攻击与告警处置 | 日志分析量           | 1,000GB/月 | 3,000GB/月 | 10,000GB/月 | 0.104美元/GB/月，扩展步长1,000GB                   |
|         | 告警接入            | 支持        | 支持        | 支持         | —                                          |
|         | 用户行为分析          | —         | —         | 支持         | —                                          |
|         | 告警聚合、事件调查与关联分析  | 支持        | 支持        | 支持         | —                                          |
|         | 联动处置            | —         | 支持        | 支持         | —                                          |
|         | AI 自动处置         | —         | —         | 支持         | —                                          |
| 安全管理    | 安全报告            | 体检报告      | 巡检解读报告    | 安全专家洞察报告   | —                                          |
|         | 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        | 625美元/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、主机、负载均衡、数据库、对象存储 COS、Elasticsearch Service 等资产的数量 | 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      |
| 日志审计，是否需要统一接入安全产品日志进行分析管理                                           | 否   | 是   | 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、主机、负载均衡、数据库、对象存储 COS、ElasticsearchService 等）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

☒ 云API异常监测

密钥异常、泄露全链路监测

实时发现云API密钥风险配置、泄露事件、异常调用；根据密钥请求调用记录等追溯调用完整路径、关联策略代码与资产。

AK数量

3

服务时长

1个月

3个月

6个月

1年

☒ 账户余额足够时，到期后自动按月续费

元/月

| 基础服务计费  | AK 资产数计费 |
|---------|----------|
| 857美元/月 | 14美元/个/月 |

#### ❶ 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（857 + 14\*4）\*2 = 1,826 （美元）。

### 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共享。

☒ 云API异常监测

密钥异常、泄露全链路监测

实时发现云API密钥风险配置、泄露事件、异常调用；根据密钥请求调用记录等追溯调用完整路径、关联策略代码与资产。

共享配额账号

等2个账号 | AK...

服务时长

1个月

3个月

6个月

1年

☒ 账户余额足够时，到期后自动按月续费

元/月

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<br>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 |

### ① 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  $(857 + 14 \times 10) \times 2 = 1,994$ （美元）

#### 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。

# 购买方式

最近更新时间：2025-09-29 14:11:49

1. 进入 [云安全中心购买页](#)，根据需求选择套餐，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**立即下单**，完成支付流程即购买成功。

# 续费说明

最近更新时间：2025-09-29 14:11:49

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

最近更新時間：2023-09-21 17:27:20

## ① 注意：

如果您是腾讯云合作伙伴的客户，账户欠费下的产品资源处理规则以您与合作伙伴约定的协议为准。

- 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：2026-09-11 16:58:31

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，使用过模拟攻击等功能。
- 购买云安全中心产品后，下载过安全体检报告。

## 退款途径

参与活动购买的产品，如若退款规则与活动规则冲突，以活动规则为准，活动规则中若说明不支持退款，则无法申请退款。

购买产品时使用的代金券/折扣券不支持退还，支付时使用的非优惠券费用按支付方式（现金/赠送金/现金券）按支付比例退还到支付方的腾讯云账户。

注意：

购买现金券的费用不支持退还，使用现金券支付的订单如果需要申请退款，可按比例退券到支付方腾讯云账户上。

## 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。

### ① 说明：

不满足5天内无理由全额退款规则的预付费云产品退货退款，退款的计算方式分为按订单剩余价值退款和按照未使用比例退款（资源包）。

# 快速入门

最近更新时间：2025-09-29 14:11:49

## 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

## 多云多账号管理

### 多云接入

最近更新时间：2025-11-28 15:24:25

## 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**。

### 多云多账号管理

#### 集团账号概况

深圳市腾讯计算机系统有限公司

管理员账号名称

管理员账号ID

多云、混合云账号接入

腾讯云

1234567890123456



5



0

[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 [Azure 账号](#) 或 [AWS 账号](#)，并配置相关参数，单击**确定**。

配置多云、云外、混合云账号

×

选择账号类型

Azure账号

AWS账号

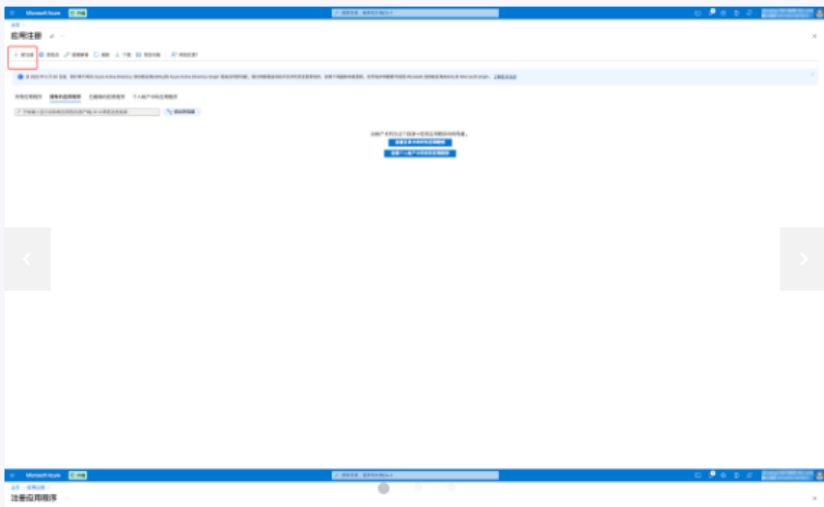
腾讯云子账号

腾讯云账号, 前往集团账号配置

创建子账号的方式

手动配置 5分钟完成, 需要创建“应用注册”与“客户端密码”, 并绑定“订阅”, 赋予“读者”权限。  
[收起配置指引](#) [在文档中查看](#)

< 第1/3步 > 请前往 [www.azure.com/xxx](https://www.azure.com/xxx) 创建一个应用注册, 并根据需要选择支持的帐户类型。



订阅ID

请输入

租户ID

请输入

客户端ID

请输入

客户端密钥

请输入

为确保账号可用, 请为角色分配‘读者’权限, 如账号有效期内发生客户端密钥变更, 请及时在云安全中心修改对应配置

所属部门 (选填)

请选择

从腾讯云集团账号获取部门信息, 为了便于后续管理, 请为当前账号选择一个部门

资产同步频率

请选择

确定

取消

## 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“受支持的帐户类型”，单击注册。

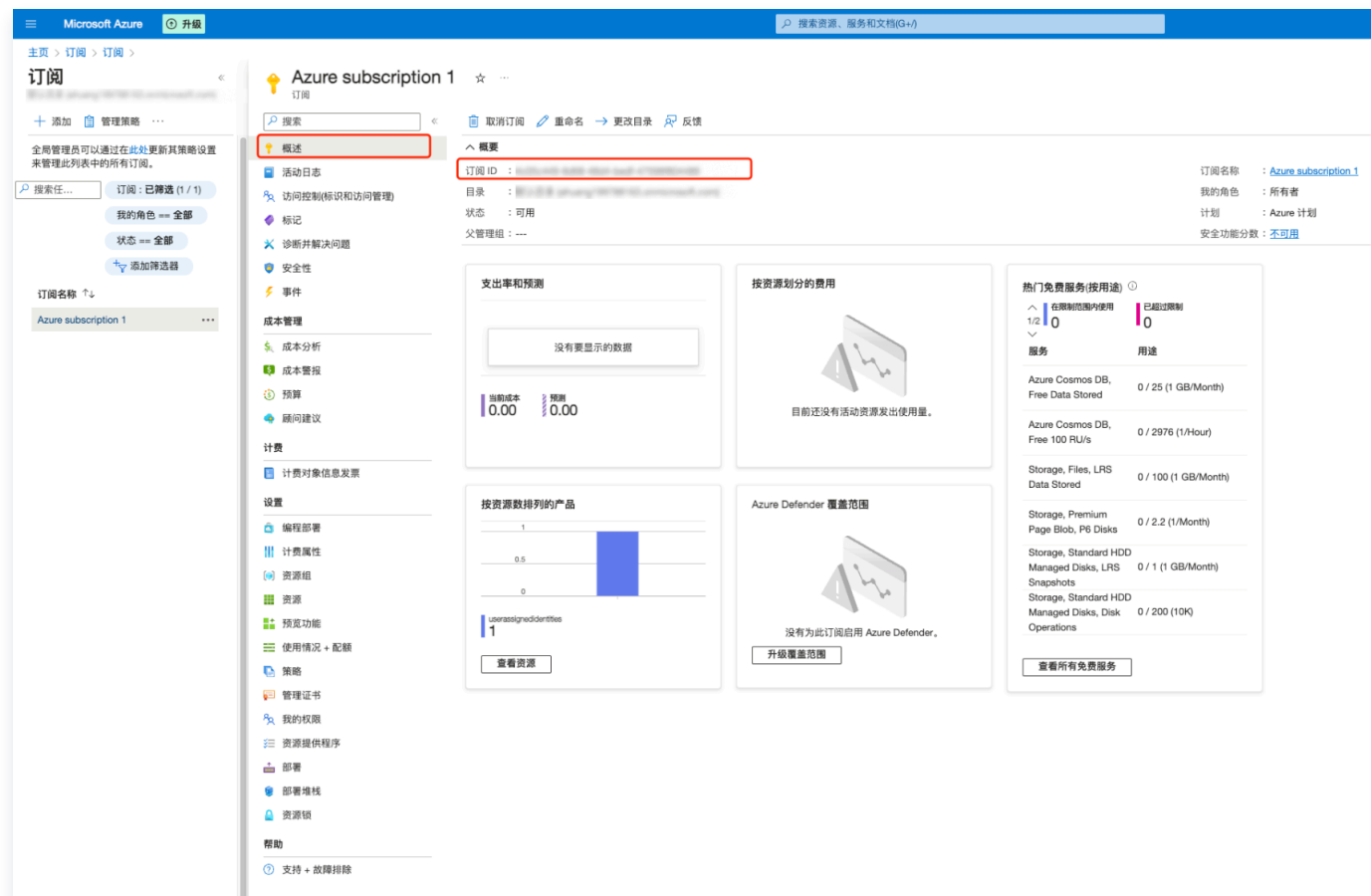
A screenshot of the 'Register an application' page in the Microsoft Azure portal. The page has a blue header with the Microsoft Azure logo and a 'Upgrade' button. The main content area is white. At the top, there is a breadcrumb trail: 'Home > App Registrations > Register an application'. Below this, there is a section for 'Name' with a text input field. A red box highlights the 'Supported account types' section, which contains four radio button options: 'Only accounts in this organization (Default - Single tenant)', 'Any organization (Any Microsoft Entra ID tenant - Multi-tenant)', 'Any organization (Any Microsoft Entra ID tenant - Multi-tenant) and personal Microsoft accounts (e.g., Skype, Xbox)', and 'Only personal Microsoft accounts'. Below the red box, there is a 'Help me choose...' link. Further down, there is a section for 'Redirect URI (optional)' with a text input field and a 'Select platform' dropdown menu. At the bottom, there is a 'Register' button and a link to the Microsoft platform policy.

## 步骤2：获取订阅 ID

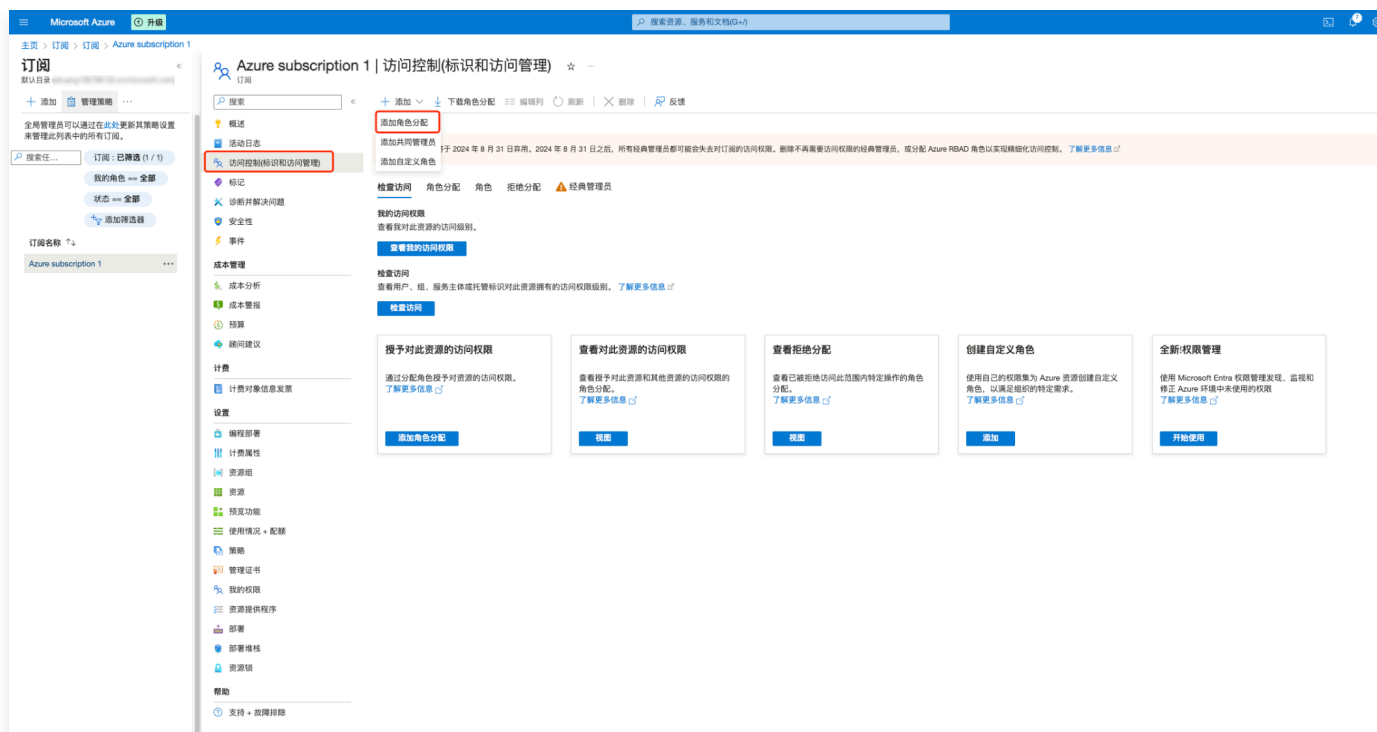
1. 在订阅列表页面，选择将要接入的订阅（应用注册可以绑定多个订阅），单击订阅名称。



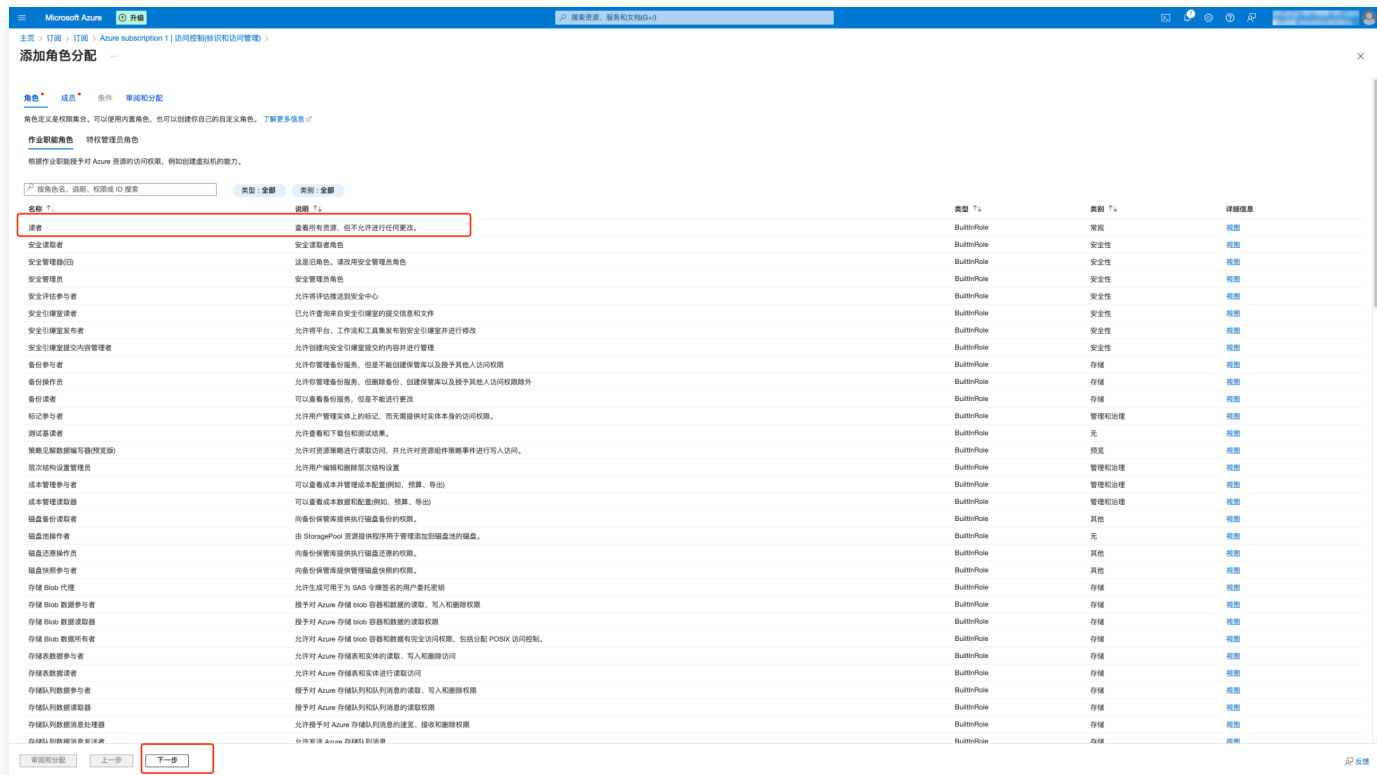
2. 在订阅详情页面，单击概述，获取订阅 ID。



3. 选择访问控制，单击添加，选择添加角色分配。

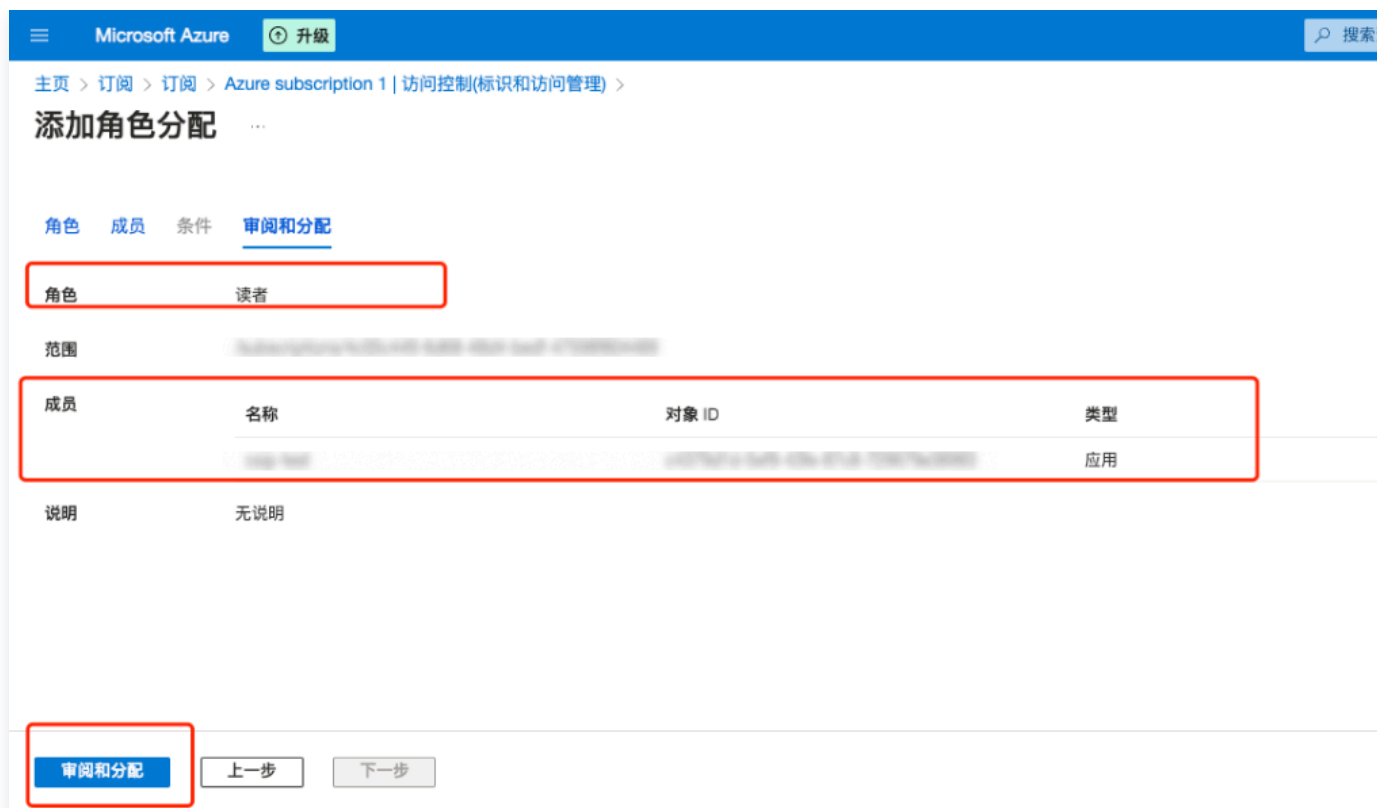


4. 选择需要分配的角色，建议依次选择“读者”和“Azure Kubernetes 服务群集用户角色”，单击下一步。



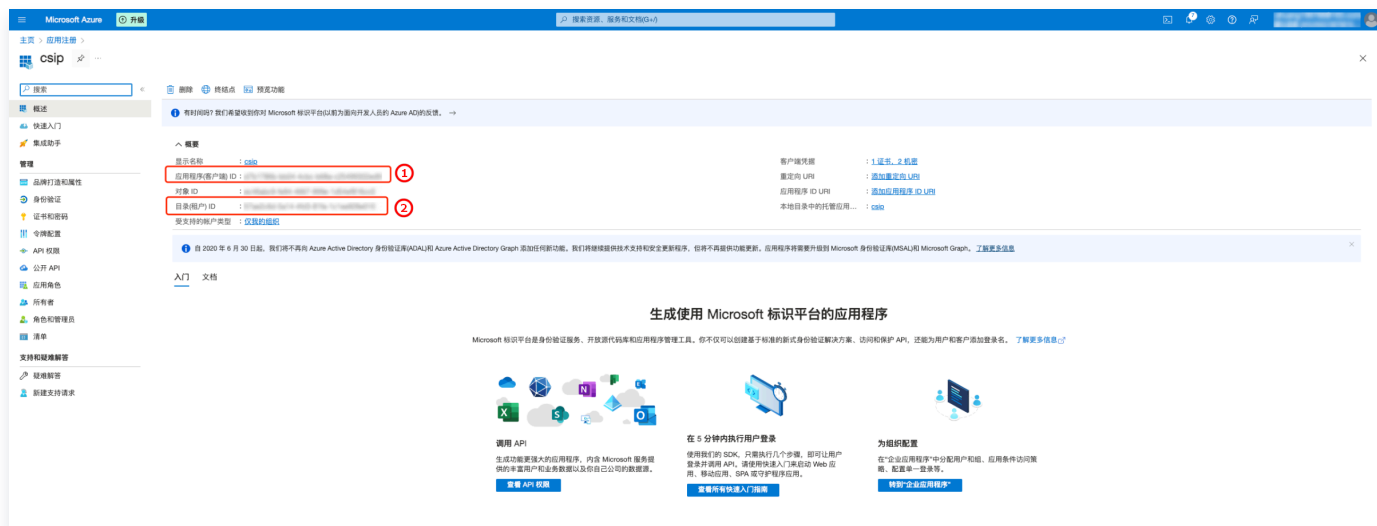
5. 添加需要分配的用户，单击选择成员，在搜索框输入要添加的“应用注册”名称，选择该应用注册，单击下一步。

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。

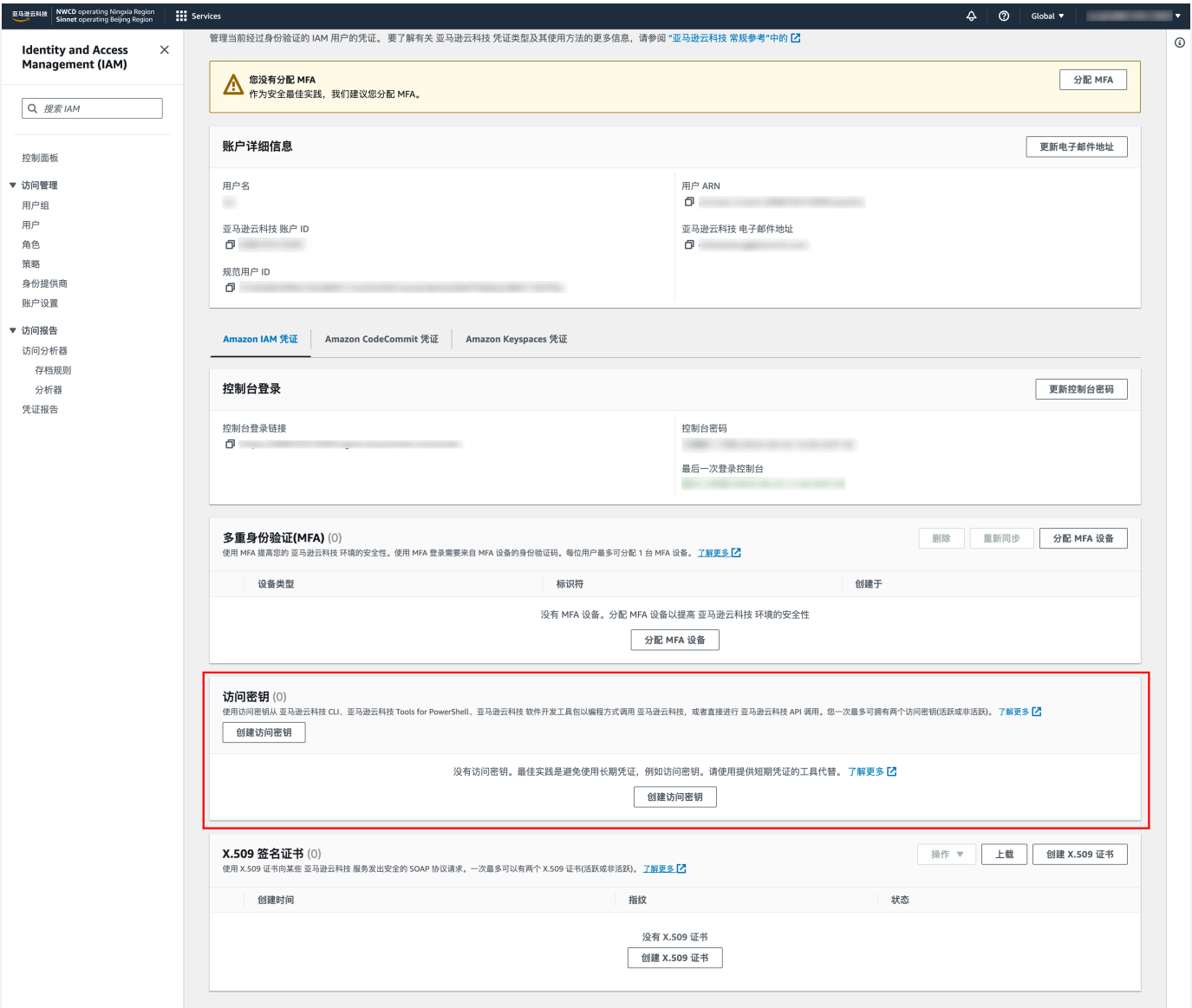


## AWS 账号

### 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。

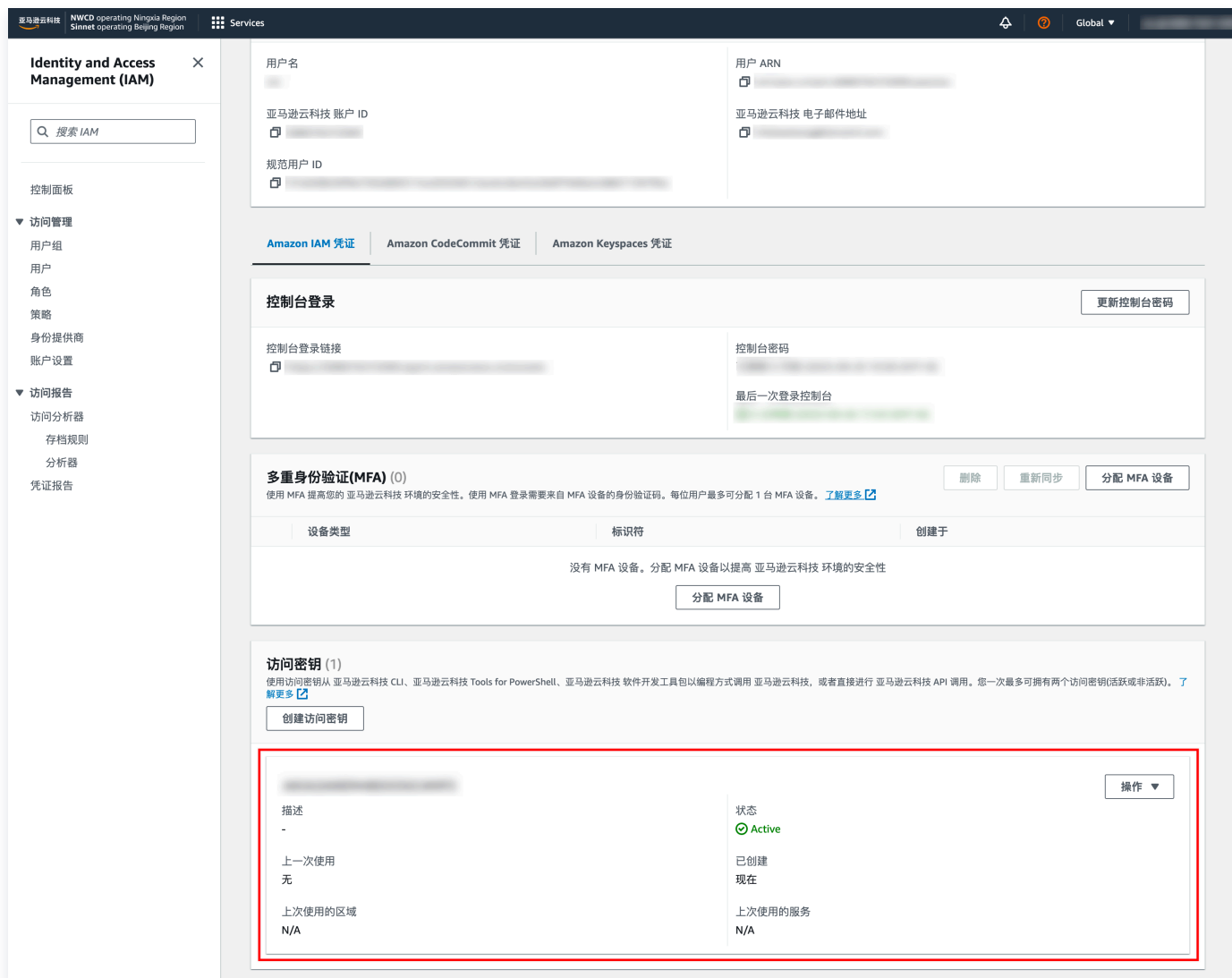
1. 请登录 AWS 后前往 [安全凭证](#) 页面，单击[创建访问密钥](#)生成可用于监控或管理亚马逊云科技资源的“访问密钥”、“秘密访问密钥”。



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”。



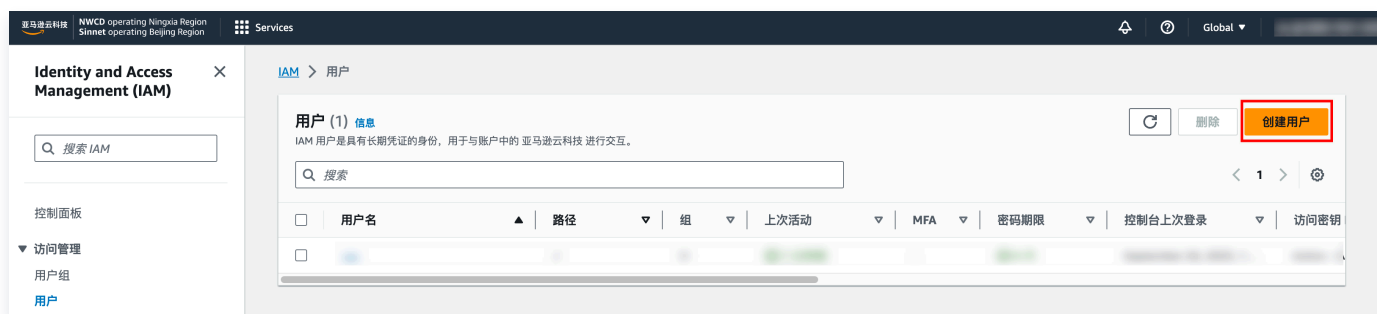
3. 确保“访问密钥”的状态为 Active 后，将“访问密钥”、“秘密访问密钥”填写至“主账号 SecretID”、“主账号 SecretKey”。



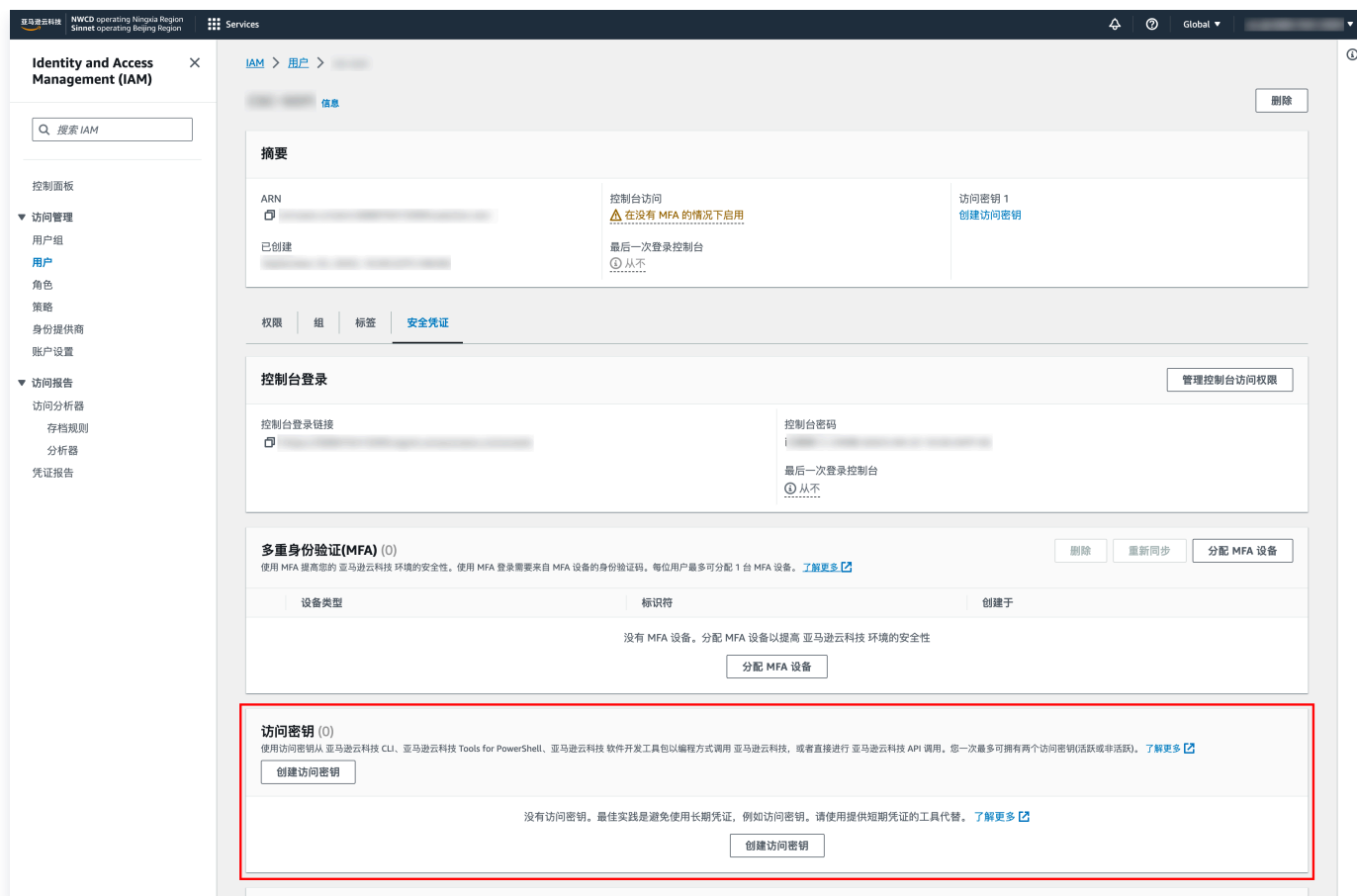
## 手动配置

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”。



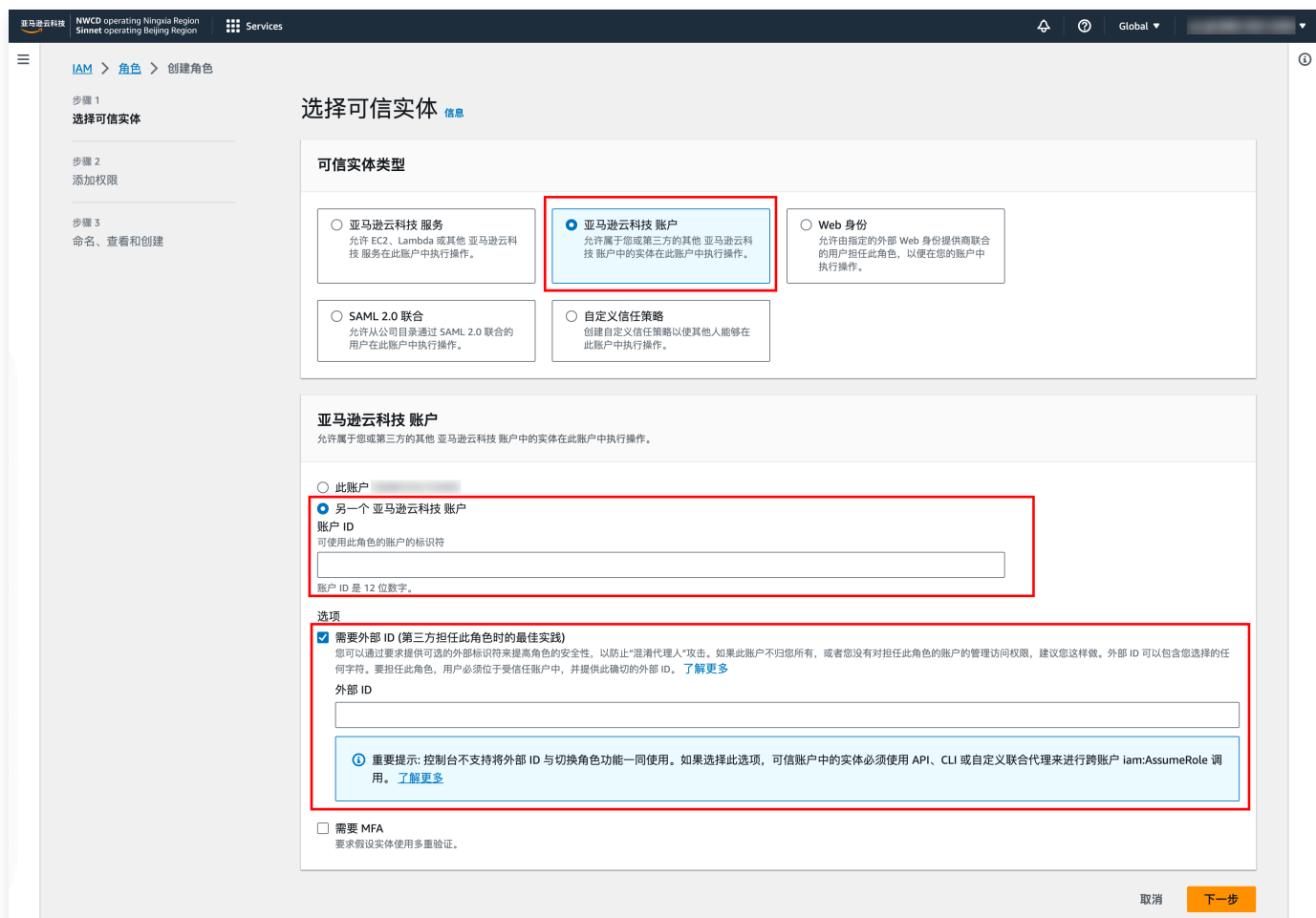
## 高级配置

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。

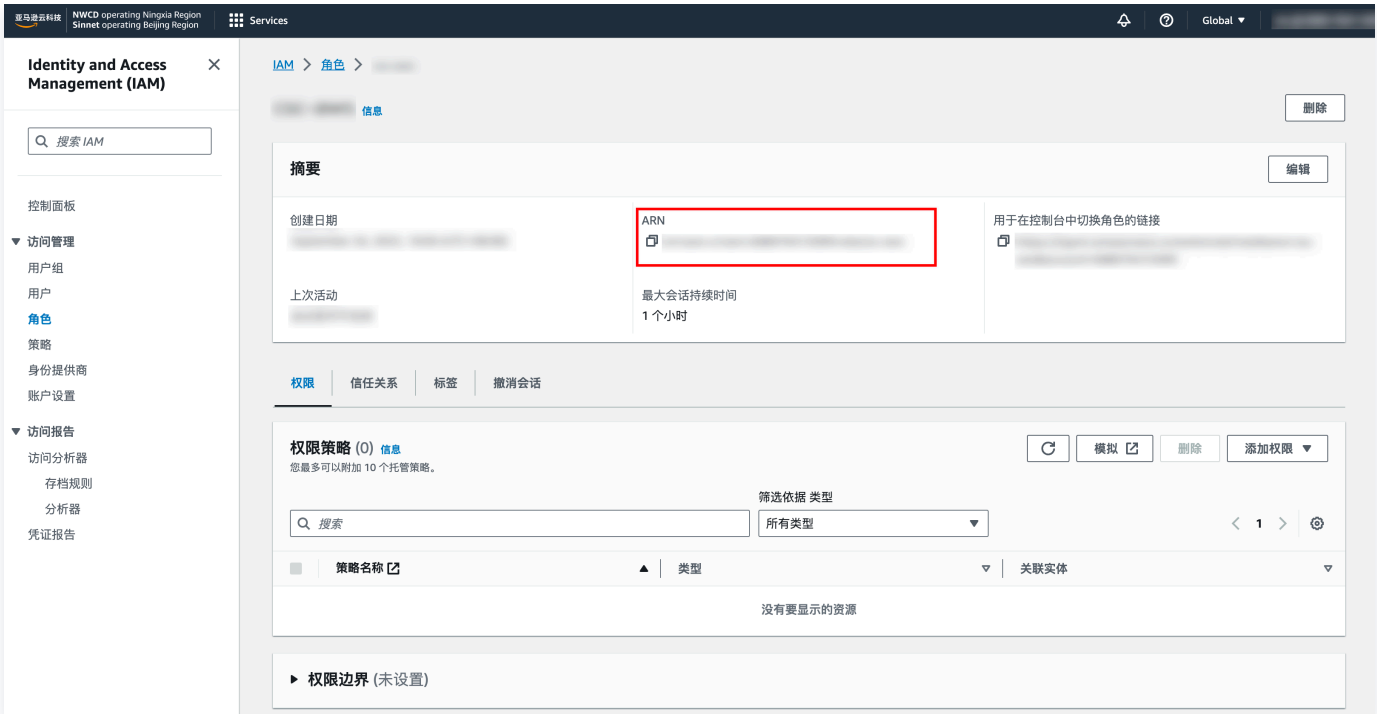
1. 请登录 AWS 后前往 **IAM > 角色** 页面，单击**创建角色**，该身份具有特定权限，凭证在短期内有效。角色可以由您信任的实体承担。



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。



# 多账号管理

最近更新时间：2024-08-12 17:26:36

## 功能简介

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

## 操作场景

### 切换登录账号

支持一键切换成员账号登录，满足高效且安全的免密码切换。

### 集中管理账号

无需部署，集中管理集团所有账号，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。

### ① 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](#)。



## 您好，欢迎使用多账号管理功能

创建集团组织架构，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。

1

### 企业实名认证

• 暂未认证

创建或加入组织，需完成企业实名认证，请先[完成实名认证](#)

2

### 集团组织创建

创建前请先提交工单，创建后不能加入其他集团账号管理，直到集团组织被删除

[提交工单](#)[了解更多](#)

## 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。

### 基本信息

[集团账号管理使用说明书](#)

① 当您创建一个集团组织后，您不能加入其它的集团账号管理中，直到此集团组织被删除。

### 集团账号管理类型：账号、资源、费用管理型组织

#### 多账号管理

创建集团组织架构，将账号成员分类管理

#### 资源共享管理

创建共享单元，为成员账号共享资源

#### 集团财务管理

查看集团财务概览，支持查看成员账单、消费明细，为成员划拨资金、共享优惠等

更多集团账号管理内容[了解详情](#)

[创建](#)

## 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。



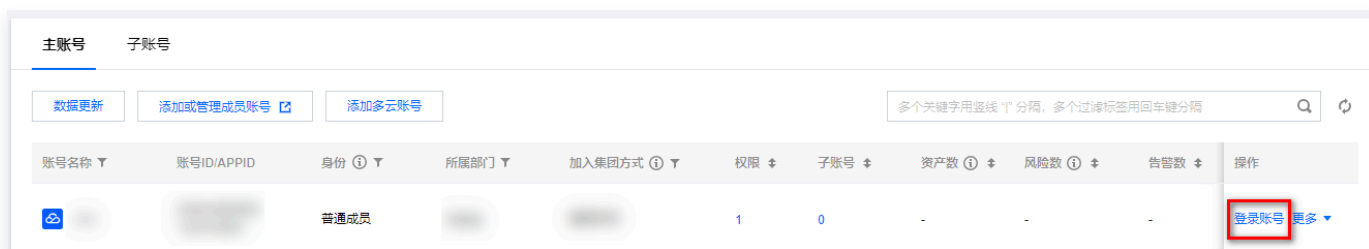
## 二、如何灵活的切换账号登录

### 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。

#### ① 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。

### 登录账号

① 子账号可以通过被授予的访问权限快速登录到成员账号控制台。[查看详情](#)

成员账号



[添加子账号授权](#)

访问权限 ①

| 权限名称 | 策略名称 | 操作                     |
|------|------|------------------------|
|      |      | <a href="#">登录成员账号</a> |
|      |      | <a href="#">登录成员账号</a> |
|      |      | <a href="#">登录成员账号</a> |

## 三、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

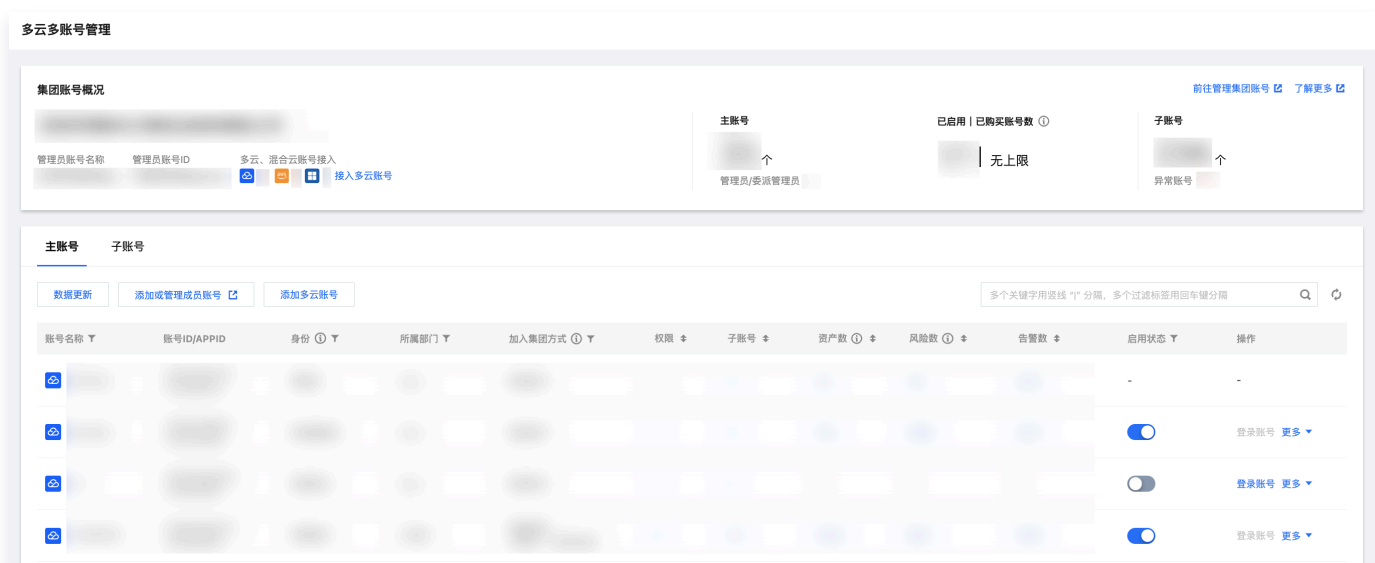
在各功能模块右上角，单击**多账号管理**，下拉筛选框后，可以通过输入**账号名称/账号 ID/APPID** 进行搜索，选中成员账号后单击**确定**，功能模块内数据将切换至该账号所有数据。



## 系统设置-多账号管理

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

- 管理员主账号登录



- 管理员子账号登录



- 成员主账号、子账号登录



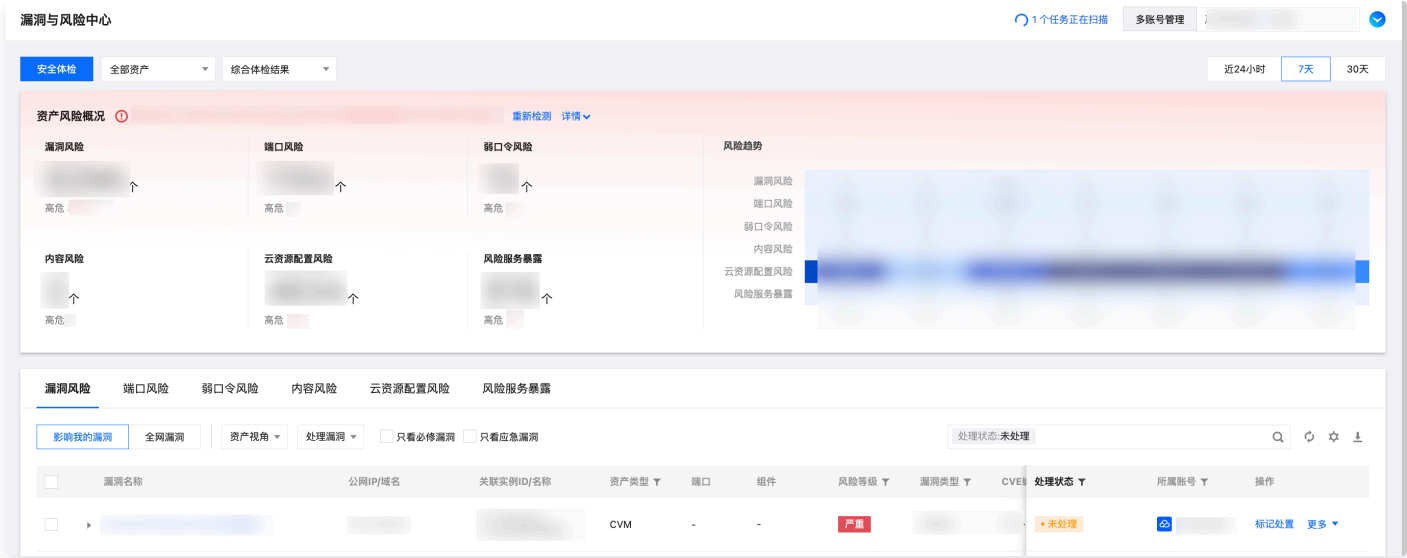
资产中心

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



漏洞与风险中心

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



安全体检

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



报告下载

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



四、常见问题

多账号管理之后的计费标准？

未来新版云安全中心的计费标准请实时关注产品动态。

## 存量用户的数据情况

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

## 如何实现多账号管理，是否需要调整网络架构？

安全产品的系统层数据上打通以实现多账号管理，不需要调整网络架构。

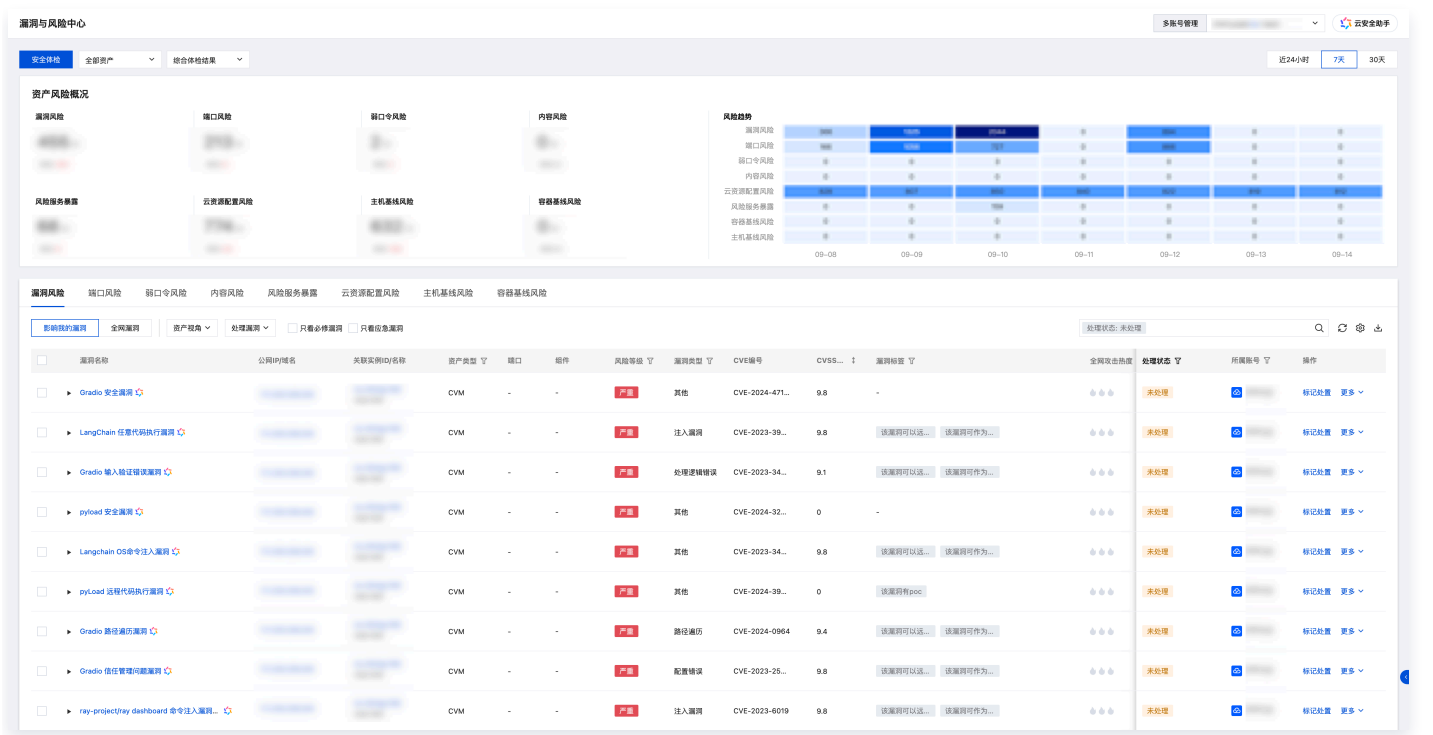
## 使用过程中，有问题如何联系？

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

# 漏洞与风险中心

最近更新时间：2025-09-18 14:36:17

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

- 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。
- 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。
- 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。

## 漏洞与风险中心

安全体检

全部资产

综合体检结果

## 资产风险概况

## 漏洞风险



高危

## 端口风险



高危

## 弱口令风险



高危

## 内容风险



高危

## 风险服务暴露

68个

高危

## 云资源配置风险



高危

## 主机基线风险



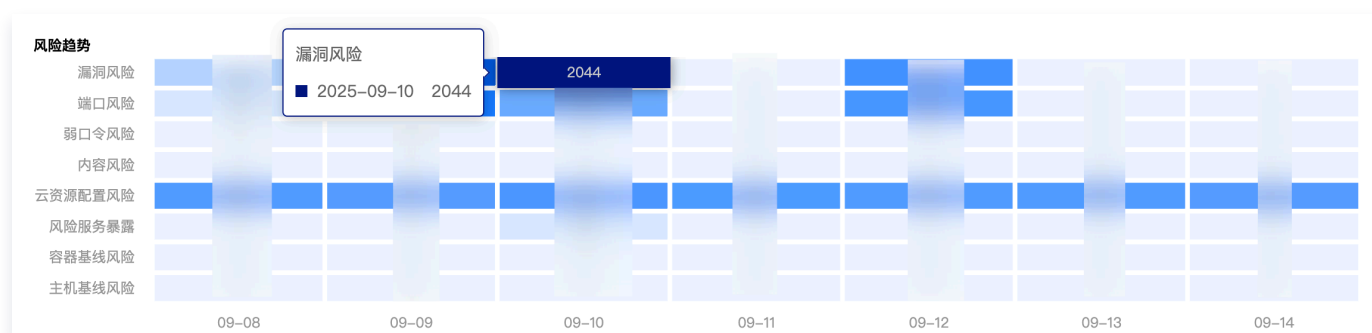
高危

## 容器基线风险



高危

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。

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

漏洞名称

公网IP/域名

关联实例ID/名称

资产类型

端口

所属账号

操作

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

漏洞标签

全网攻击热度

识别来源

处理状态

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

漏洞标签

全网攻击热度

识别来源

处理状态

① 说明：

以漏洞风险为例。

## 影响我的漏洞

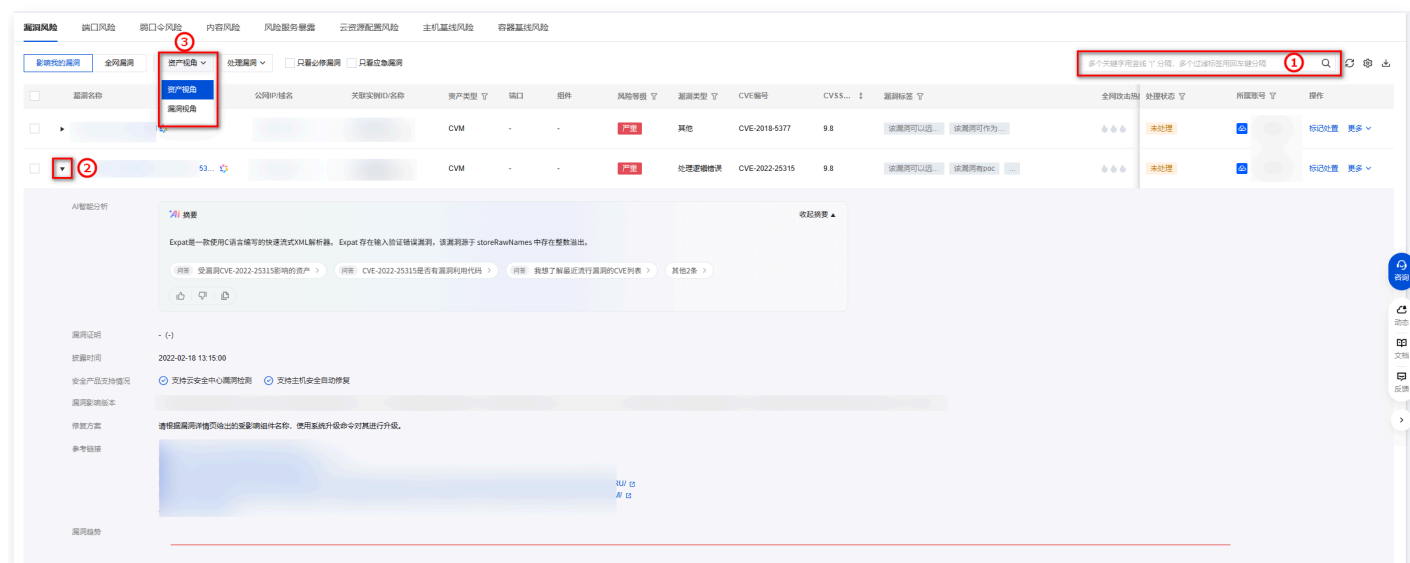
在影响我的漏洞页签，查看已扫描资产的漏洞风险，包括漏洞名称、影响资产、风险等级、端口组件、漏洞类型、CVE 编号、扫描时间、处理状态等。

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。



| 漏洞名称                                 | 风险等级 | 漏洞类型      | CVE编号          | CVSS... | 漏洞标签 | 全网攻击热度    | 影响组件            | 安全产品支持情况                                 | 影响资产 | 时间          | 检测状态 | 操作   |
|--------------------------------------|------|-----------|----------------|---------|------|-----------|-----------------|------------------------------------------|------|-------------|------|------|
| Microsoft SharePoint Server反序列化漏洞    | 高危   | 反序列化      | CVE-2025-53... | 9.8     | 必修   | 该漏洞可以过... | 该漏洞有poc         | 支持云防火墙开启虚拟补丁   支持云安全中心漏洞修复               | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| NVIDIA Container Toolkit 容器逃逸漏洞      | 高危   | 资源管理错误    | CVE-2025-23... | 0       | 必修   | 该漏洞有poc   | -               | -                                        | -    | 最近检测: 披露时间: | 未检测  | 查看详情 |
| Apache Jackrabbit XML 外部实体注入(XSL)    | 高危   | 其他        | CVE-2025-53... | 0       | 必修   | 该漏洞有poc   | (apache) jac... | 支持云安全中心漏洞修复                              | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| Jenkins plugin Git Parameter 安全漏洞    | 高危   | 其他        | CVE-2025-53... | 0       | 必修   | 该漏洞有poc   | (jenkins) gi... | 支持云安全中心漏洞修复                              | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| mscp-remote 操作系统命令注入漏洞               | 严重   | 操作系统命令... | CVE-2025-6514  | 0       | 必修   | 该漏洞有poc   | -               | -                                        | -    | 最近检测: 披露时间: | 未检测  | 查看详情 |
| Git 二进制代码执行漏洞(CVE-2025-48384)        | 高危   | 配置错误      | CVE-2025-48... | 0       | 必修   | 高危        | 该漏洞有poc         | 支持云安全中心漏洞修复   支持云安全中心自动修复                | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| Redis 远程代码执行漏洞(CVE-2025-320...)      | 高危   | 代码执行      | CVE-2025-32... | 0       | 必修   | 高危        | 该漏洞有poc         | 支持云防火墙开启虚拟补丁   支持云安全中心漏洞修复   支持云安全中心自动修复 | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| Linux Kernel 拒绝服务漏洞 (CVE-2025-38...) | 高危   | 拒绝服务      | CVE-2025-38... | 0       | 必修   | 该漏洞有poc   | -               | 支持云防火墙开启虚拟补丁   支持云安全中心漏洞修复   支持云安全中心自动修复 | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| Ulama-Factory vhead_file 代码执行漏洞      | 高危   | 代码注入      | CVE-2025-53... | 0       | 必修   | 该漏洞可以过... | -               | 支持云安全中心漏洞修复                              | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |
| DataSet 远程代码执行漏洞 (CVE-2025-49...)    | 高危   | 其他        | CVE-2025-49... | 9.8     | 必修   | 该漏洞可以过... | (dataset) ...   | 支持云安全中心漏洞修复                              | 0    | 最近检测: 披露时间: | 已检测  | 重新检测 |

- 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。

NVIDIA Container Toolkit 容器逃逸漏洞 [ ... ] 高危

漏洞管理错误 CVE-2025-23268 0 必修 该漏洞poc

最近修改: -

创建时间: 2025-07-18 04:15:00

未检测

查看详情

AI智能分析

摘要

NVIDIA Container Toolkit是NVIDIA推出的开源工具包，用于在容器化环境中实现GPU加速计算。它通过标准化、自动化的方式，将GPU设备、驱动程序（如CUDA、cuDNN）与容器运行时（如Docker、Containerd）无缝集成，使开发者无需手动配置即可直接在容器中使用GPU资源。支持多GPU场景及精确的资源隔离，已成为云厂商GPU容器服务的底层技术基础。NVIDIA Container Toolkit <= 1.17.7版本存在容器逃逸漏洞，攻击者可构造恶意Dockerfile，结合ID\_PHELOAD 造成容器逃逸。

关联 CVE-2025-23268影响的资产

关联 CVE-2025-23268是否有漏洞利用代码

关联 我想了解最近流行漏洞的CVE列表

其他2条

安全产品支持情况

暂无支持的安全产品

漏洞影响版本

-

修复方案

1.官方已发布漏洞补丁及修复版本，请评估业务是否受影响后，酌情升级至安全版本(1.17.8)。【备注：建议在升级前做好数据备份工作，避免出现意外。 https://nvidia.custhelp.com/app/answers/detail/a\_id/5659/2/ 临时缓解方案： - 若NVIDIA Container Runtime处于legacy mode,可以修改/etc/hwloc... 展开详情

相关链接

https://nvidia.custhelp.com/app/answers/detail/a\_id/5659/2/

## 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。

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

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

选择资源属性进行过滤

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

漏洞标签

全网攻击热度

识别来源

处理状态

所属账号

操作

| <input type="checkbox"/> | 漏洞名称 | 公网IP/域名 | 关联实例ID/名称 | 资产类型 | 端口 | 所属账号 | 操作      |
|--------------------------|------|---------|-----------|------|----|------|---------|
| <input type="checkbox"/> |      |         |           | CVM  | -  |      | 标记处置 更多 |
| <input type="checkbox"/> |      | -253... |           | CVM  | -  |      | 标记处置 更多 |
| <input type="checkbox"/> |      |         |           | CVM  | -  |      | 标记处置 更多 |
| <input type="checkbox"/> |      | Sqj...  | x         | CVM  | -  |      | 标记处置 更多 |
| <input type="checkbox"/> |      | VE-2... |           | CVM  | -  |      | 标记处置 更多 |
| <input type="checkbox"/> |      |         | x         | CVM  | -  |      | 标记处置 更多 |
| <input type="checkbox"/> |      |         |           | CVM  | -  |      | 标记处置 更多 |

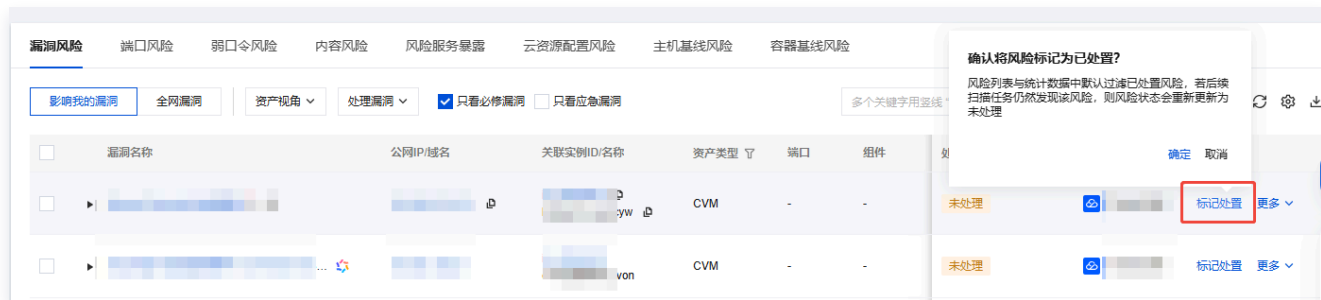
### 标记状态

#### 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

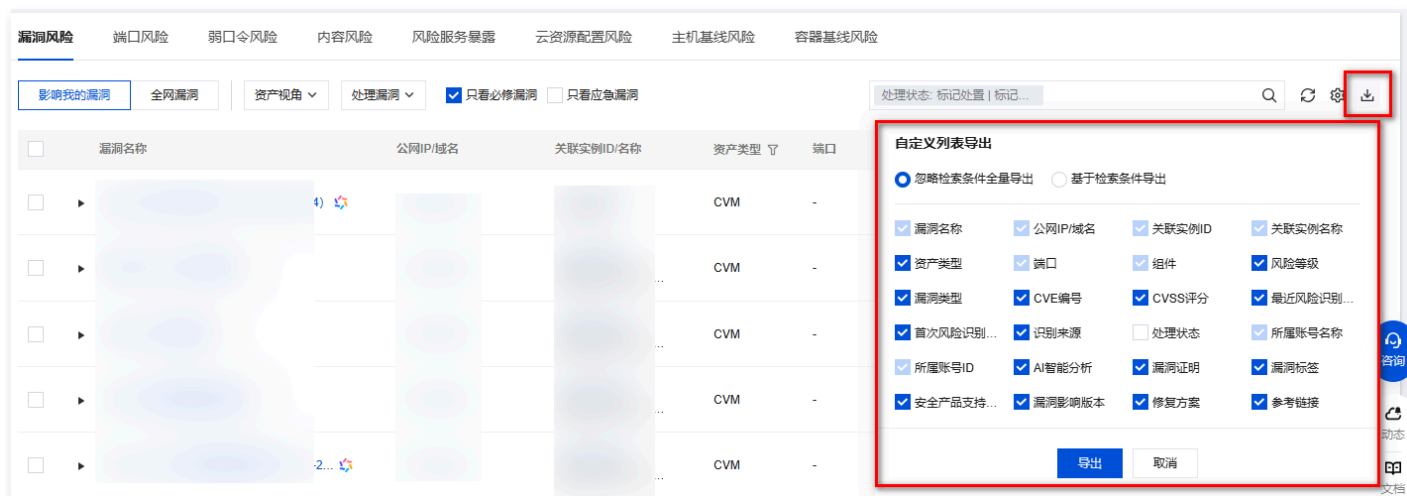
当告警需要重新研判时，取消标记后处理状态将恢复为未处理。

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。



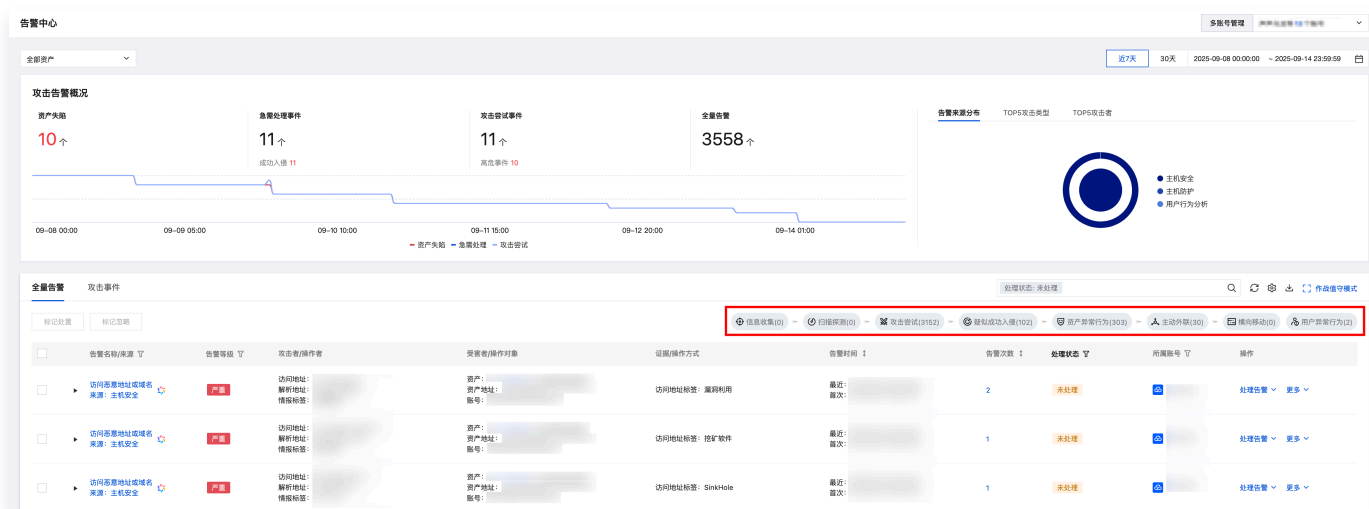
# 告警中心

最近更新时间：2025-09-18 14:35:44

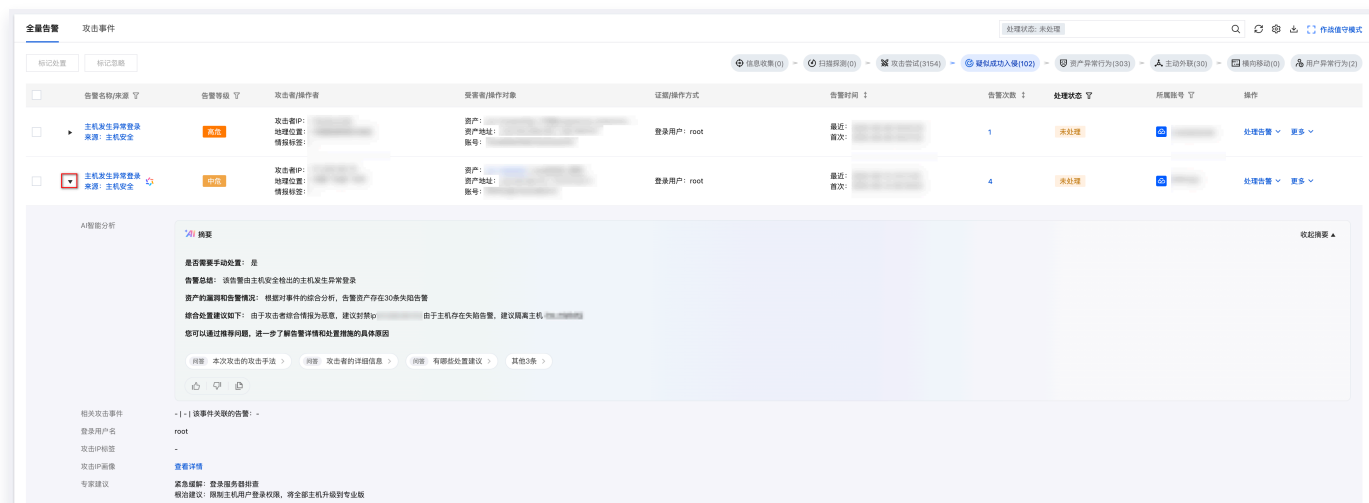
告警中心是一个集中监控和分析云上安全威胁的一体化功能，通过汇聚云安全中心、主机安全、容器安全、云防火墙和 Web 应用防火墙等来源的告警，基于 ATT&CK 框架进行告警关联分析，实现统一的安全威胁发现与管理，帮助用户快速发现和处置安全隐患。

## 告警定位

1. 登录 [云安全中心控制台](#)，在左侧导航中，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](#)，在左侧导航中，单击告警中心。

2. 在全量告警页签，单击搜索框，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。 | <ol style="list-style-type: none"><li>支持单个或批量将告警状态标为已处置。<ul style="list-style-type: none"><li>单个：选择目标告警，单击操作列的<b>标记已处置</b>。</li><li>批量：选择一个或多个告警，单击左上角的<b>标记已处置</b>。</li></ul></li><li>在确认窗口中，单击<b>确定</b>，即可将目标告警标记为已处置。</li></ol> |
| 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。                | <ol style="list-style-type: none"><li>支持单个或批量将告警状态修改为忽略。<ul style="list-style-type: none"><li>单个：选择目标告警，单击操作列的<b>忽略</b>。</li><li>批量：选择一个或多个告警，单击左上角的<b>忽略</b>。</li></ul></li><li>在确认窗口中，单击<b>确定</b>，即可将目标告警状态修改为忽略。</li></ol>      |
| 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，可单击操作列的 <b>取消标记处置</b> 或 <b>取消标记忽略</b> ，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。

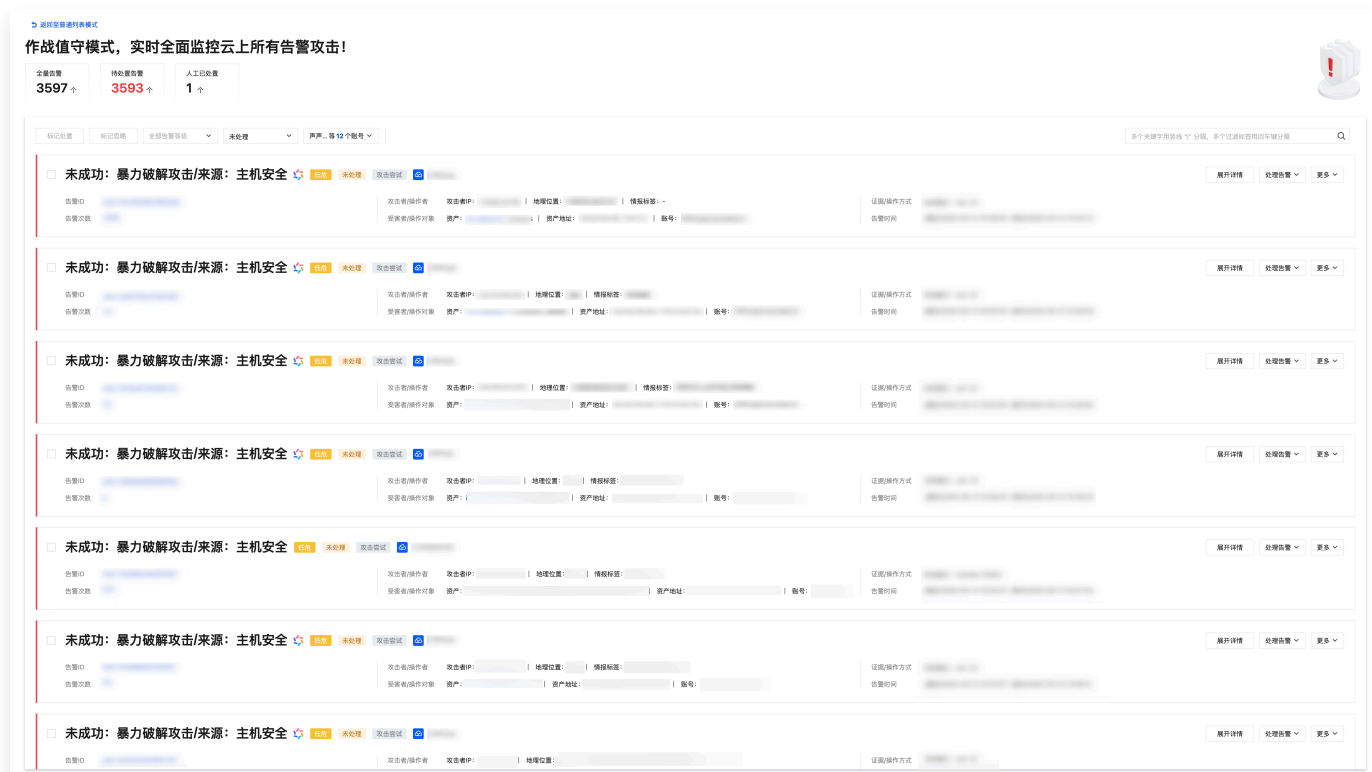


## 作战值守模式

1. 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。



# 日志投递（支持多账号多产品多日志）

最近更新时间：2024-08-12 17:28:05

## 功能背景

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

## 应用场景

### 日志存储

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

### 离线分析

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

## 日志投递至 Kafka

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

#### ① 前提条件：

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

### Ckafka 公网域名接入

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

日志投递

投递至kafka

投递至CLS

[前往消息队列控制台](#)

1. 购买消息队列Kafka实例，推荐按照需要投递的日志量来选购对应Kafka实例规格

2. 根据消息队列Kafka文档指引，开通白名单实现公网域名接入或支撑环境接入

3. 按照本页面中以下指引完成日志投递配置，仅支持使用同一消息队列用户进行投递

配置消息队列

网络接入方式

☒ Ckafka公网域名接入

☐ Ckafka支撑环境接入

☐ 其他Kafka公网接入

TLS加密

☐

消息队列所属账号

消息队列实例

请选择

公网域名接入

请选择

用户名

请输入用户名

密码

请输入密码

配置日志投递

| 日志来源                | 日志类型              | 账号来源            | Topic ID/名称           | 操作            |
|---------------------|-------------------|-----------------|-----------------------|---------------|
| <div>云防火墙</div>     | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>Web应用防火墙</div> | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>主机安全</div>     | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>云安全中心</div>    | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>云审计</div>      | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |

新增日志投递配置

| 参数名称     | 说明             |
|----------|----------------|
| 网络接入方式   | Ckafka 公网域名接入。 |
| TLS 加密   | 选择是否开启 TLS 加密。 |
| 消息队列所属账号 | 投递目标所属账号。      |



|             |                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 消息队列实例      | 云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、选择所需消息队列实例。                                                                                                                                                |
| 公网域名接入      | 选择所需公网域名。                                                                                                                                                                                |
| 用户名         | 请输入所选消息队列实例的用户名。                                                                                                                                                                         |
| 密码          | 请输入所选消息队列实例的密码。                                                                                                                                                                          |
| 日志来源        | 支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。                                                                                                                             |
| 日志类型        | 根据所选的日志来源不同则日志类型也有所不同。                                                                                                                                                                   |
| Topic ID/名称 | 选择所需 Topic。                                                                                                                                                                              |
| 操作          | <div><div>● 新增：单击<b>新增日志投递配置</b>，支持新增多个日志来源。</div><div>● 删除：单击目标日志操作列的<b>删除</b>，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。</div><div>● 编辑：如非首次配置日志投递，则支持在日志投递页面，单击<b>修改配置</b>，修改相关日志投递。</div></div> |

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

日志投递

修改配置 前往消息队列控制台

消息队列详情

接入方式

Ckafka公网域名接入

接入对象

消息队列实例ID/名称

实例版本

地域

可用区

所属网络ID/名称

所在子网ID/名称

峰值带宽

磁盘容量

状态

用户名

日志投递详情

全部开启 全部关闭 查看监控

| 日志来源     | 日志类型              | 账号来源 | TopicId/名称 | 投递状态 | 投递开关        | 操作      |
|----------|-------------------|------|------------|------|-------------|---------|
| 云防火墙     | 访问控制日志、零信任防护日志... |      |            | 正常   | <div></div> | 编辑 查看监控 |
| Web应用防火墙 | 攻击日志、访问日志         |      |            | 正常   | <div></div> | 编辑 查看监控 |
| 主机安全     | 入侵检测日志、客户端相关日志... |      |            | 正常   | <div></div> | 编辑 查看监控 |

Ckafka 支撑环境接入

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

日志投递

投递至kafka

投递至CLS

[前往消息队列控制台](#)

1. 购买消息队列Ckafka实例，推荐按照需要投递的日志量来选购对应Ckafka实例规格

2. 根据消息队列Ckafka文档指引，开通白名单实现公网域名接入或支撑环境接入

3. 按照本页面中以下指引完成日志投递配置，仅支持使用同一消息队列用户进行投递

配置消息队列

网络接入方式

☐ Ckafka公网域名接入

☒ Ckafka支撑环境接入

☐ 其他Kafka公网接入

TLS加密

☒

消息队列所属账号

消息队列实例

请选择

支撑环境接入

请选择

配置日志投递

| 日志来源                | 日志类型              | 账号来源            | Topic ID/名称           | 操作            |
|---------------------|-------------------|-----------------|-----------------------|---------------|
| <div>云防火墙</div>     | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>Web应用防火墙</div> | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>主机安全</div>     | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>云安全中心</div>    | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |
| <div>云审计</div>      | <div>全部日志类型</div> | <div>全部账号</div> | <div>请选择Topic名称</div> | <div>删除</div> |

新增日志投递配置

| 参数名称   | 说明             |
|--------|----------------|
| 网络接入方式 | Ckafka 支撑环境接入。 |
| TLS 加密 | 选择是否开启 TLS 加密。 |

©2013-2026 腾讯云版权所有

第46 共160页

|             |                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 消息队列所属账号    | 投递目标所属账号。                                                                                                                                                                                                |
| 消息队列实例      | 云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、选择所需消息队列实例。                                                                                                                                                                |
| 支撑环境接入      | 选择所需支撑环境。                                                                                                                                                                                                |
| 日志来源        | 支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。                                                                                                                                             |
| 日志类型        | 根据所选的日志来源不同则日志类型也有所不同。                                                                                                                                                                                   |
| Topic ID/名称 | 选择所需 Topic。                                                                                                                                                                                              |
| 操作          | <ul style="list-style-type: none"><li>新增：单击<b>新增日志投递配置</b>，支持新增多个日志来源。</li><li>删除：单击目标日志操作列的<b>删除</b>，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。</li><li>编辑：如非首次配置日志投递，则支持在日志投递页面，单击<b>修改配置</b>，修改相关日志投递。</li></ul> |

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

日志投递

修改配置 前往消息队列控制台

消息队列详情

接入方式Ckafka支撑环境接入

接入对象

消息队列实例ID/名称

实例版本

地域

可用区

所属网络ID/名称

所在子网ID/名称

峰值带宽

磁盘容量

状态健康

用户名

日志投递详情

全部开启 全部关闭 查看监控

| 日志来源 | 日志类型              | 账号来源 | TopicId/名称 | 投递状态 | 投递开关                                | 操作      |
|------|-------------------|------|------------|------|-------------------------------------|---------|
| 云防火墙 | 访问控制日志、零信任防护日志... |      |            | 正常   | <input checked="" type="checkbox"/> | 编辑 查看监控 |
| 主机安全 | 入侵检测日志、客户端相关日志... |      |            | 正常   | <input checked="" type="checkbox"/> | 编辑 查看监控 |

其他 Kafka 公网接入

1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**日志分析**。

2. 在日志分析页面，单击日志投递 > 投递至 kafka。
3. 在投递至 kafka 页面，选择其他 Kafka 公网接入，配置相关参数。

日志投递

投递至kafka

投递至CLS

[前往消息队列控制台](#)

1. 购买消息队列Ckafka实例，推荐按照需要投递的日志量来选购对应Ckafka实例规格

2. 根据消息队列Ckafka文档指引，开通白名单实现公网域名接入或支撑环境接入

3. 按照本页面中以下指引完成日志投递配置，仅支持使用同一消息队列用户进行投递

配置消息队列

网络接入方式

☐ Ckafka公网域名接入

☐ Ckafka支撑环境接入

☒ 其他Kafka公网接入

TLS加密

☒

公网接入

请输入

用户名

请输入用户名

密码

请输入密码

配置日志投递

| 日志来源     | 日志类型   | 账号来源 | Topic名称    | 操作 |
|----------|--------|------|------------|----|
| 云防火墙     | 全部日志类型 | 全部账号 | 请输入Topic名称 | 删除 |
| Web应用防火墙 | 全部日志类型 | 全部账号 | 请输入Topic名称 | 删除 |
| 主机安全     | 全部日志类型 | 全部账号 | 请输入Topic名称 | 删除 |
| 云安全中心    | 全部日志类型 | 全部账号 | 请输入Topic名称 | 删除 |
| 云审计      | 全部日志类型 | 全部账号 | 请输入Topic名称 | 删除 |

[新增日志投递配置](#)

| 参数名称   | 说明               |
|--------|------------------|
| 网络接入方式 | 其他 Kafka 公网接入。   |
| TLS 加密 | 选择是否开启 TLS 加密。   |
| 公网接入   | 根据实际需求填写公网信息。    |
| 用户名    | 请输入所选消息队列实例的用户名。 |

|          |                                                                                                                                                                                                          |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 密码       | 请输入所选消息队列实例的密码。                                                                                                                                                                                          |
| 日志来源     | 支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。                                                                                                                                             |
| 日志类型     | 根据所选的日志来源不同则日志类型也有所不同。                                                                                                                                                                                   |
| Topic 名称 | 输入所需 Topic 名称。                                                                                                                                                                                           |
| 操作       | <ul style="list-style-type: none"><li>新增：单击<b>新增日志投递配置</b>，支持新增多个日志来源。</li><li>删除：单击目标日志操作列的<b>删除</b>，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。</li><li>编辑：如非首次配置日志投递，则支持在日志投递页面，单击<b>修改配置</b>，修改相关日志投递。</li></ul> |

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

日志投递

修改配置 前往消息队列控制台

消息队列详情

接入方式

其他Kafka公网接入

接入对象

状态

健康

用户名

test

日志投递详情

全部开启

全部关闭

| 日志来源 | 日志类型              | 账号来源 | Topic名称 | 投递状态 | 投递开关        | 操作 |
|------|-------------------|------|---------|------|-------------|----|
| 云防火墙 | 入侵防御日志、流量日志、操作... |      |         | 正常   | <div></div> | 编辑 |

## 日志投递至 CLS

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

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

日志投递

投递至kafka 投递至CLS

前往日志服务控制台

投递至CLS (日志服务) • 已开通

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

✓ 开通日志服务

>

2 配置日志投递

开始投递

#### ① 说明：

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

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

日志投递

投递至kafka 投递至CLS

前往日志服务控制台

授权和开启日志投递到CLS后，将为您自动在CLS服务中创建后付费的存储空间，同时也会生成后付费账单。[CLS计费详情](#)

投递账号

投递所属账号

请选择账号

投递内容

日志来源

请选择日志来源

日志类型

请选择日志类型

日志来源账号

请选择

投递目标

目标地域

请选择目标地域

日志集操作

选择已有日志集

创建日志集

日志集

请输入日志集名称

日志主题操作

选择已有日志主题

创建日志主题

日志主题

请输入日志主题名称

确定

取消

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

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

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

日志投递

投递至kafka

投递至CLS

前往日志服务控制台

投递账号信息

账号名称/ID

所属部门

日志投递详情

新增投递

批量开启

批量关闭

日志检索

删除

刷新

| <input checked="" type="checkbox"/> | 日志来源      | 日志类型   | 来源账号    | 日志主题 | 投递状态 | 投递开关                                | 操作    |
|-------------------------------------|-----------|--------|---------|------|------|-------------------------------------|-------|
| <input checked="" type="checkbox"/> | Web应用防... | 多个 (2) | 多个 (15) |      | 正常   | <input checked="" type="checkbox"/> | 编辑 更多 |

共 1 项

10 条 / 页

1 / 1 页

## 投递及被投递对象

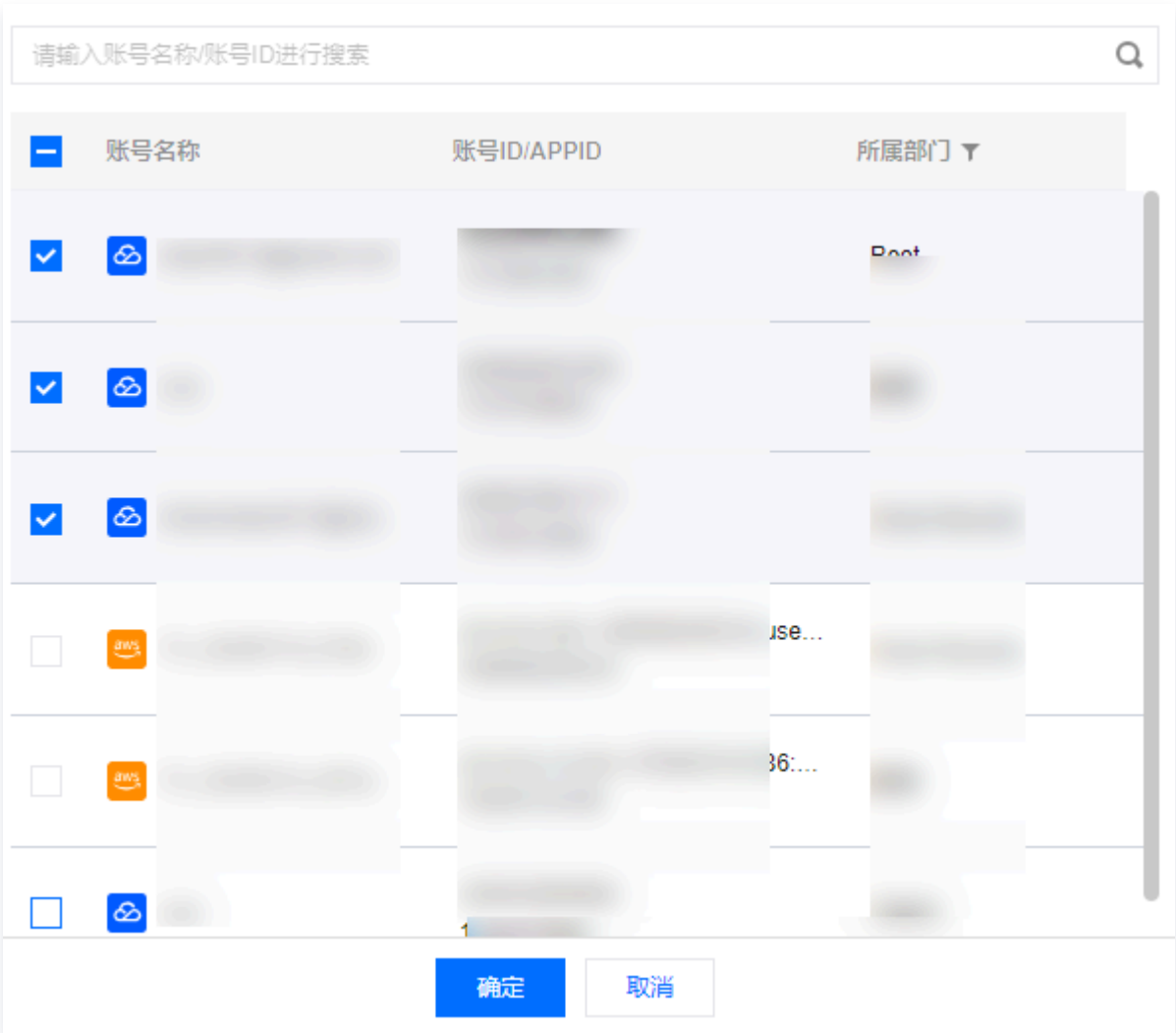
### 多账号管理

- 开通 [多账号管理](#) 功能后，支持多账号多产品日志投递。
1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击右上角的**多账号管理**。





3. 在多账号管理页面，选择所需账号，单击**确定**。



确定

取消

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

|                                              |                                                                                                                      |                                                                   |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 管理员/委派管理员管理其他账号日志，即配置其他账号多产品日志投递。            | 右上角选中其他账号后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取 <b>其他账号</b> 的 Ckafka，可选所需腾讯云消息队列。                       | 展示其他账号的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。            |
| 管理员/委派管理员管理当前账号（管理员/委派管理员）日志，即配置当前账号多产品日志投递。 | 右上角选中当前账号（管理员/委派管理员）后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取 <b>当前账号（管理员/委派管理员）</b> 的 Ckafka，可选所需腾讯云消息队列。 | 展示当前账号（管理员/委派管理员）的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。 |

## 单账号管理

仅支持对当前账号进行多产品日志投递。

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

### ① 注意：

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

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

## 常见问题

### 日志投递如何收费？

日志投递为云安全中心旗舰版专属，可 [前往购买日志投递](#)。

### 公网日志投递出口 IP 白名单

```
106.55.200.0/24
106.55.201.0/24
106.55.202.0/24
81.71.5.0/24
134.175.239.0/24
193.112.130.0/24
193.112.164.0/24
```

```
193.112.221.0/24
111.230.173.0/24
111.230.181.0/24
129.204.232.0/24
193.112.129.0/24
193.112.153.0/24
106.52.11.0/24
106.55.52.0/24
118.89.20.0/24
193.112.32.0/24
193.112.60.0/24
106.52.106.0/24
106.52.67.0/24
106.55.254.0/24
42.194.128.0/24
42.194.133.0/24
106.52.69.0/24
118.89.64.0/24
129.204.249.0/24
182.254.171.0/24
193.112.170.0/24
106.55.207.0/24
119.28.101.0/24
150.109.12.0/24
```

## 日志投递支持哪些产品哪些日志类型？

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

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

# 资产中心

最近更新时间：2024-08-02 10:14:18

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     | 云服务器 CVM           |
|          | 非腾讯云服务器            |
|          | 轻量应用服务器 Lighthouse |
|          | 边缘计算器              |
| 容器资产     | 容器                 |
|          | 本地镜像               |
|          | 仓库镜像               |
|          | 主机节点               |
|          | 集群                 |
|          | Pod                |
| 公网 IP 资产 | IP                 |
|          | 高可用虚拟 IP           |
|          | 弹性公网 IP            |
|          | 非腾讯云 IP            |
|          | 弹性 ipv6            |
|          | anycast 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                    |
| 网络资产-网卡 | 弹性网卡                  |
| 私有网络    | 私有网络 VPC              |
|         | 子网                    |
| 云数据库    | 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          |
| 其他云资源   | 云硬盘 CBS               |
|         | 对象存储 COS              |
|         | 文件存储                  |
|         | 消息队列                  |
|         | Elasticsearch Service |

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。

**① 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](#)。

## 资产中心

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 ⓘ



未防护主机

风险主机

## 公网IP资产



未防护公网IP

风险公网IP

## 域名资产



未防护域名

风险域名

## 容器资产



## 网关资产



## 数据库资产



## 搜索资产

- 在 [资产中心页面](#)，支持按照资产分类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。

三 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 多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

主机资产( ) 容器资产( ) 公网IP资产 域名资产 网络资产( ) 数据库资产(0) 其他云资源( )

开启防护 标记为核心资产 标记为非核心资产 自定义列表字段

| <input type="checkbox"/> | 资产实例ID/名称 | IP地址           | 资源标签 | 资产类型 | 防护状态 | 所属账号 | 操作      |
|--------------------------|-----------|----------------|------|------|------|------|---------|
| <input type="checkbox"/> |           | 公网: 1<br>内网: 1 | 核心资产 | CVM  | 未安装  |      | 开启防护 更多 |
| <input type="checkbox"/> |           | 公网: 1<br>内网: 1 | 核心资产 | CVM  | 已防护  |      | 防护详情 更多 |

- 在 [资产中心页面](#)，支持在网络结构的视角，查询每个地域下，分别有哪些 VPC，每个 VPC 内分别有哪些资产。



## 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 > 标记为核心资产**。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 > 标记为非核心资产**。



- 在 [资产中心页面](#)，可以筛选关注核心/非核心资产。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。

### ① 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**。

编辑标签

编辑须知

- 标签用于从不同维度对资源分类管理。如现有标签不符合您的要求，请前往 [标签管理](#)

已选择 1 个资源

标签键

标签值

×

+ 添加

键值粘贴板

确定

取消

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

1. 如需管理非腾讯云资产，可以在 [资产中心页面](#)，单击左上角**手动添加资产**。

## 资产中心

资产更新



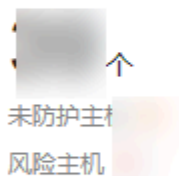
接入多云资产

手动添加资产

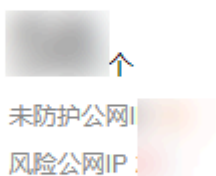
收集外部资产

## 资产统计概况

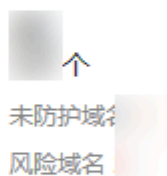
## 主机资产 ⓘ



## 公网IP资产



## 域名资产



## 容器资产



## 网关资产



## 数据库资产



2. 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**。

## ① 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。

手动添加资产



 支持在资产中心添加云外公网IP、域名资产 

添加方式

☒ 手动录入 ☐ 文件导入

地址

1.

请输入公网IP地址、Web网站域名、API域名，手动输入使用回车换行，每行一个；最多支持输入1000行，外部复制粘贴多个地址，请用英文逗号","分隔；不支持CIDR地址，若输入重复IP，后台将自动合并

☐ 承诺添加资产归本账号所属企业所有，如使用他人资产将由本账号归属企业承担法律责任 [查看详情](#)

确定

取消

## 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。

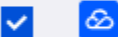
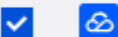
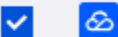
多账号管理

t...等4个账号

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

# 安全体检

## 功能简介

最近更新时间：2023-09-21 17:32:10

### 功能背景

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

### 应用场景

#### 日常安全体检

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

### 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、<br>联动主机安全<br>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、<br>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、<br>联动主机安全<br>和容器安全 |
| 风险服务暴露  | 针对云上向互联网暴露的资产，提供互联网攻击面测绘功能，快速识别云上资产的暴露端口、暴露服务及暴露组件等潜在攻击面。                                                                     | 云安全中心                     |
| 网站内容    | 快速准确识别敏感图片、文字信息等网站风险内容，针对网站进行挂马、                                                                                              | 云安全中心                     |

|    |                        |  |
|----|------------------------|--|
| 风险 | 暗链、垃圾广告、矿池等风险的多维度智能检测。 |  |
|----|------------------------|--|

**说明：**

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

体检资产

| 体检资产                                                                                  | 体检项目             |
|---------------------------------------------------------------------------------------|------------------|
| 云服务器、轻量应用服务器、边缘计算器                                                                    | 漏洞、弱口令、云资源配置风险   |
| 已授权的本地镜像、仓库镜像                                                                         | 漏洞风险             |
| 组件运行正常的集群                                                                             | 漏洞、云资源配置风险       |
| 公网 IP、域名资产                                                                            | 端口、漏洞、弱口令、网站内容风险 |
| 负载均衡、子网、MySQL、Redis、MariaDB、PostgreSQL、MongoDB、云硬盘 CBS、对象存储 COS、Elasticsearch Service | 云资源配置风险          |

**注意：**

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

体检消耗

| 体检资产                                                                            | 体检项目          | 消耗体检配额             |
|---------------------------------------------------------------------------------|---------------|--------------------|
| 公网 IP、域名资产                                                                      | 漏洞、弱口令、网站内容风险 | 1次体检消耗体检配额 = 体检资产数 |
| 云服务器、负载均衡、MySQL、Redis、MariaDB、PostgreSQL、MongoDB、Elasticsearch Service、对象存储 COS | 云资源配置风险       |                    |

云安全中心版本功能对比

| 体检项目    | 免费版 | 高级版        | 企业版         | 旗舰版         |
|---------|-----|------------|-------------|-------------|
| 端口风险    | ✓   | ✓          | ✓           | ✓           |
| 应急漏洞    | ✓   | ✓          | ✓           | ✓           |
| 漏洞风险    | —   | ✓          | ✓           | ✓           |
| 弱口令风险   | —   | ✓          | ✓           | ✓           |
| 云资源配置风险 | —   | ✓          | ✓           | ✓           |
| 风险服务暴露  | —   | —          | ✓           | ✓           |
| 网站内容风险  | —   | —          | ✓           | ✓           |
| 体检配额    | 20次 | 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。

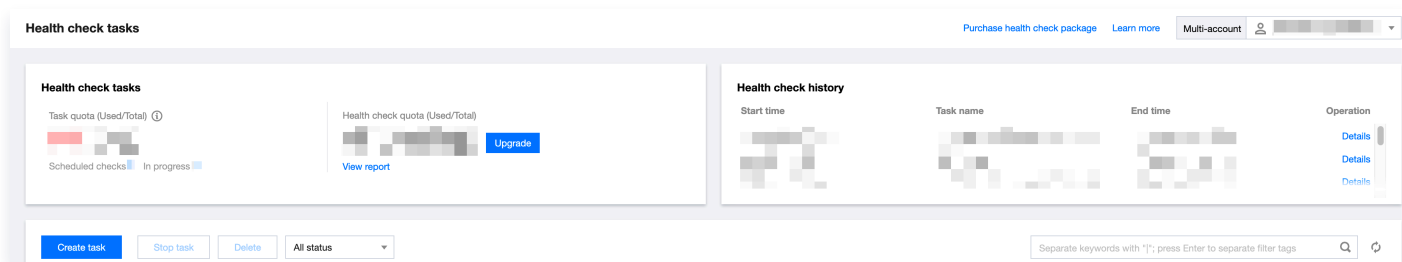
# 操作指引

最近更新时间：2023-09-21 17:32:59

## 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。

### 立体防护-应急漏洞

在 [云立体防护页面](#)，针对公网 IP、域名资产，由云安全中心提供的应急漏洞风险检测，并梳理互联网漏洞暴露面。

#### ① 说明：

单个应急漏洞限免2次扫描。

### 创建任务

1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**体检任务**。
2. 在体检任务页面，单击**创建任务**。
3. 在创建资产体检任务弹窗中，配置相关参数，单击**确定**。



Create task ⓘ

Task name ⓘ

Mode

☐ Basic

☒ Standard

☐ Advanced ⓘ

Plan ⓘ

☐ Immediate

☐ Specified time

☒ Scheduled checks

Daily ▾

Included assets

☒ All assets ⓘ

☐ Select from existing

☐ Manual input

☐ Import

Exclude assets (0)

Check items ⓘ

☒ Port risks ⓘ

☒ Weak passwords ⓘ

☒ Configuration risks ⓘ

☒ Vulnerabilities ⓘ

☒ Content risks ⓘ

☒ Exposed risk services ⓘ

Estimated duration

minutes

Quota usage ⓘ

☐ Agree to Health Check Authorization Agreement. [View details](#)

☐ I hereby acknowledge that the assets to check are owned by current enterprise account. The account owner shall bear the legal responsibility for unauthorized usage of the assets.

OK

Cancel

| 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 | <div><ul style="list-style-type: none"><li>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。</li><li>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种风险进行选择性的扫描。</li><li>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。</li></ul></div> |
| 体检计划 | <div><ul style="list-style-type: none"><li>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。</li></ul></div>                                                                                                                                                |

|      |                                                                                                                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div>● 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。</div><div>● 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。</div></div></div> |
| 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。                                                                                                                                                                                                                                                    |

## 编辑报告

1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**体检任务**。
2. 在体检任务页面，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。

| <input type="checkbox"/> | Task ID/name | Plan | Included... | Check Items | Start time | Estimated dura... | Task status | Reports | Mode | Source | Created | Account | Operation   |
|--------------------------|--------------|------|-------------|-------------|------------|-------------------|-------------|---------|------|--------|---------|---------|-------------|
| <input type="checkbox"/> |              |      |             |             |            |                   |             |         |      |        |         |         | Edit Delete |
| <input type="checkbox"/> |              |      |             |             |            |                   |             |         |      |        |         |         | Edit Delete |

3. 在编辑资产体检任务弹窗中，修改相关参数，单击**确定**。

Edit task ⓘ

Task name ⓘ



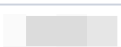
Mode

☐ Basic ☒ Standard ☐ Advanced ⓘ

Plan ⓘ

☐ Immediate ☐ Specified time ☒ Scheduled checks

Daily ▾





Included assets

☐ All assets  ☒ Select from existing ☐ Manual input

☐ Import

Select assets 

All assets 

Check items ⓘ

☒ Port risks ⓘ

☒ Vulnerabilities ⓘ

☒ Weak passwords ⓘ

☐ Content risks ⓘ

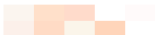
☒ Configuration risks ⓘ

☒ Exposed risk services ⓘ

Estimated duration

 minutes

Quota usage ⓘ



☐ Agree to Health Check Authorization Agreement. [View details](#)

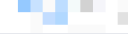
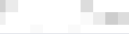
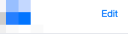
☐ I hereby acknowledge that the assets to check are owned by current enterprise account. The account owner shall bear the legal responsibility for unauthorized usage of the assets.

OK

Cancel

## 删除任务

1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**体检任务**。
2. 在体检任务页面，选择目标任务，单击**删除**。

| <input type="checkbox"/> | Task ID/name                                                                        | Plan ▾                                                                              | Included... ▴                                                                       | Check Items ▾                                                                       | Start time ▴                                                                        | Estimated dura...                                                                    | Task status                                                                           | Reports                                                                               | Mode ▾                                                                                | Source ▾                                                                              | Created                                                                               | Account ▾                                                                             | Operation             |
|--------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------|
| <input type="checkbox"/> |  |  |  |  |  |  |  |  |  |  |  |  | <div>EditDelete</div> |
| <input type="checkbox"/> |  |  |  |  |  |  |  |  |  |  |  |  | <div>EditDelete</div> |

3. 在确认删除弹窗中，单击**确定**，即可删除该任务。

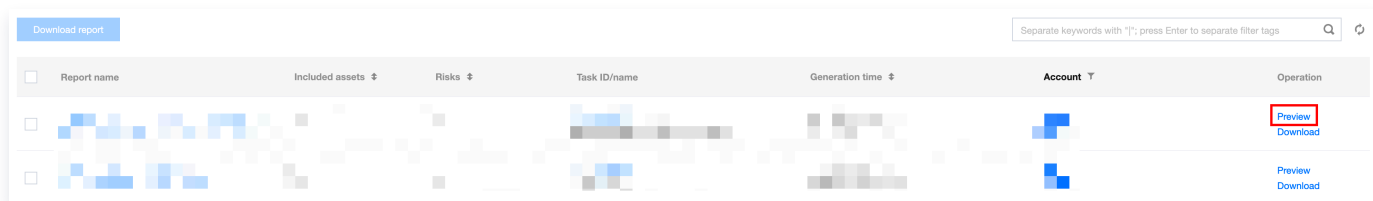
ⓘ 注意：

- 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

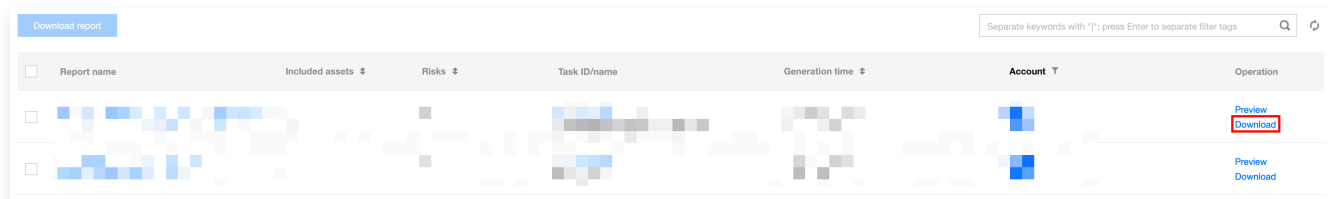
当安全体检任务完成后，云安全中心会自动生成 PDF 格式的安全报告，并提供预览或下载。此外，用户还可以通过关注服务号来随时随地接收报告。

1. 登录 [云安全中心控制台](#)，在左侧导航中，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**下载报告**。



## 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

最近更新時間：2025-04-29 10:30:25

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 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  
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

### ① 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。

### 添加黑白IP

类别 ☐ 黑名单 ☒ 白名单

IP地址

截至时间 

永久生效

备注

添加

取消

#### 5. 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

- 在 IP 白名单页面，单击添加地址，进入添加白名单页面。

黑白名单

IP黑名单 IP白名单 精准白名单 规则白名单

添加地址

删除地址

全部删除

导入数据

导出全部筛选结果

获取鼠标焦点即可选择过滤属性

| <input type="checkbox"/> | 规则ID | IP地址 | 来源 | 截止时间 | 更新时间 | 生效状态 | 备注 | 操作                                          |
|--------------------------|------|------|----|------|------|------|----|---------------------------------------------|
| <input type="checkbox"/> |      |      |    |      |      | 已过期  | 无  | <a href="#">前往编辑</a> <a href="#">复制IP地址</a> |

共 1 项 50 条/页 1 / 1 页

2. 在添加白名单页面，配置相关参数，单击**确定**。

### 添加白名单

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20个

0

截止时间 \*

☐ 永久生效

☒ 限定日期

限定日期 \*

2024-07-30 09:47:40

备注

请输入备注，50个字符以内

#### 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20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。

导入IP名单

×

导入

点击按钮，选择文件。

说明：

1.格式，仅支持.xlsx，.xls，每次只支持单个文件上传。

2.数量，每次最多可导入 条规则，如需导入大量规则，请分多次导入。

3.内容，必须包含类别，IP地址，截止时间三列；具体可参考导出数据excel格式。

4.截止时间，必须在2033/12/31 00:00:00之前，格式YYYY/MM/DD HH:MM:SS。

5.导入的格式严格按照导出格式填写，详情请看[IP黑名单操作指南](#)和[IP白名单操作指南](#)

确定导入

重置

### 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**。
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。

IP查询

W (版)

IP查询

封禁查询

\*类型：ALL

触发策略：策略名称

IP地址：输入IP

记录创建时间：近5分钟 近10分钟 近30分钟 2024-07-23 09:37:00 ~ 2024-07-23 23:59:59

☐ 有效截止时间：2024-07-23 09:42:00 ~ 2024-07-31 09:42:00

查询

# 热点问题

最近更新时间：2024-12-11 17:45:50

## 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。

## 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。

## 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，网络安全等级保护三级技术要求 | 判定 Redis 数据库的服务端口是否对全IP开放访问，正常情况下，数据库服务端口应该只针对可信 IP 或范围开放。 |
| Nosql-Redis 应该位于中国大陆 region          | 基础设施位置 | redis    | 低危 | 网络安全等级保护三级技术要求        | 等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。                           |
| 云数据库 PostgreSQL 数据库不建议对公网开放访问        | 网络访问控制 | postgres | 高危 | 默认安全规范                | 数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。                        |
| 关系型数据库-PostgreSQL 应该启用备份             | 数据安全   | postgres | 中危 | 默认安全规范，网络安全等级保护三级技术要求 | 判定 PostgreSQL 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。             |
| 关系型数据库-PostgreSQL 数据库应该位于中国大陆 region | 基础设施位置 | postgres | 低危 | 网络安全等级保护三级技术要求        | 等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。                           |

|                                      |        |         |    |                       |                                                                                                           |
|--------------------------------------|--------|---------|----|-----------------------|-----------------------------------------------------------------------------------------------------------|
| Nosql-<br>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<br>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<br>MariaDB 数据库不建议对公网开放访问        | 网络访问控制 | mariadb | 高危 | 默认安全规范                | 数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。                                                                       |
| 云数据库<br>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-<br>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-<br>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             | 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                                                                  |



|                     |         |     |    |                       |                                                                                                                                                                          |
|---------------------|---------|-----|----|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 组件不应该开放公网访问         |         |     |    |                       | 据访问与命令控制，如开放公网访问，则可能导致不必要的攻击面暴露，产生数据完整性、机密性、可用性风险。                                                                                                                       |
| 安全组不应放通全部网段任何端口     | 网络访问控制  | cvm | 高危 | 默认安全规范，网络安全等级保护三级技术要求 | 安全组是一种虚拟防火墙，建议根据最小粒度原则，配置防火墙策略。添加服务端口的可信 IP 白名单访问。                                                                                                                       |
| CVM 应该位于中国大陆 region | 基础设施位置  | cvm | 中危 | 网络安全等级保护三级技术要求        | 等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。                                                                                                                                         |
| CVM 应使用密钥对登录        | 身份认证及权限 | cvm | 中危 | 默认安全规范                | 检查 CVM 是否利用 SSH 密钥进行登录，相对于传统的密码登录，SSH 密钥登录方式更为方便，且安全性更高。（仅检查 Linux 系统机器）                                                                                                 |
| CVM 上的主机安全代理应正常运行   | 基础安全防护  | cvm | 高危 | 默认安全规范，网络安全等级保护三级技术要求 | 腾讯云主机安全提供木马查杀、密码破解拦截、登录行为审计、漏洞管理、资产组件识别等多种安全功能。未安装主机安全客户端会面临网络安全，数据泄露的风险。                                                                                                |
| COS 存储桶建议开启存储桶复制    | 数据安全    | cos | 中危 | 默认安全规范，网络安全等级保护三级技术要求 | 跨地域复制是针对存储桶的一项配置，通过配置跨地域复制规则，可以在不同存储区域的存储桶中自动、异步地复制增量对象。启用跨地域复制后，COS 将精确复制源存储桶中的对象内容（如对象元数据和版本 ID 等）到目标存储桶中，复制的对象副本拥有完全一致的属性信息。此外，源存储桶中对于对象的操作，如添加对象、删除对象等操作，也将被复制到目标存储桶 |

|                        |        |     |    |                       |                                                                                                                                     |
|------------------------|--------|-----|----|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                        |        |     |    |                       | 中。建议进行跨区域复制以提升您的数据容灾能力。                                                                                                             |
| COS 存储桶应配置合理的桶策略       | 数据安全   | COS | 高危 | 默认安全规范，网络安全等级保护三级技术要求 | 存储桶策略是指在存储桶中配置的访问策略，允许指定用户对存储桶及桶内的资源进行指定的操作。应依据“最小化权限”原则来配置，不推荐对任意用户开放读取操作权限，有遍历文件名或文件被下载的风险。                                       |
| COS 存储桶应该位于中国大陆 region | 基础设施位置 | COS | 低危 | 网络安全等级保护三级技术要求        | 等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。                                                                                                    |
| COS 存储桶应开启防盗链功能        | 数据安全   | COS | 中危 | 默认安全规范，网络安全等级保护三级技术要求 | 为了避免恶意程序使用资源 URL 盗刷公网流量或使用恶意手法盗用资源，给您带来不必要的损失。建议您通过控制台的防盗链设置配置黑/白名单，对存储对象进行安全防护。                                                    |
| COS 存储桶应开启服务端加密        | 数据安全   | COS | 中危 | 默认安全规范，网络安全等级保护三级技术要求 | 存储桶支持在对象级别上应用数据加密的保护策略，并在访问数据时自动解密。加密和解密这一操作过程都是在服务端完成，这种服务端加密功能可以有效保护静态数据。建议您对敏感数据类型开启此项配置。                                        |
| COS 存储桶应开启日志记录         | 数据安全   | COS | 中危 | 默认安全规范，网络安全等级保护三级技术要求 | 日志管理功能能够记录对于指定源存储桶的详细访问信息，并将这些信息以日志文件的形式保存在指定的存储桶中，以实现存储桶更好的管理。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稳定     | 监控告警   | clb | 低危 | 默认安全规范                | 检测负载均衡 CLB 服务的健康状态，用以判定 CLB 的后端服务是否异常。                                                       |
| CLB 不应转发高危端口               | 网络访问控制 | clb | 高危 | 默认安全规范，网络安全等级保护三级技术要求 | 应依据“最小服务”原则来设定 CLB 转发策略，只对必要的公共服务端口（如：80、443等）做转发，其他端口不应该进行转发。                               |
| CLB 不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             | 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                                                               |

|                                   |        |     |    |        |                                                                                                                                                      |
|-----------------------------------|--------|-----|----|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 型应使用私有网络                          |        |     |    |        | 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。 |

# 云 API 异常监测

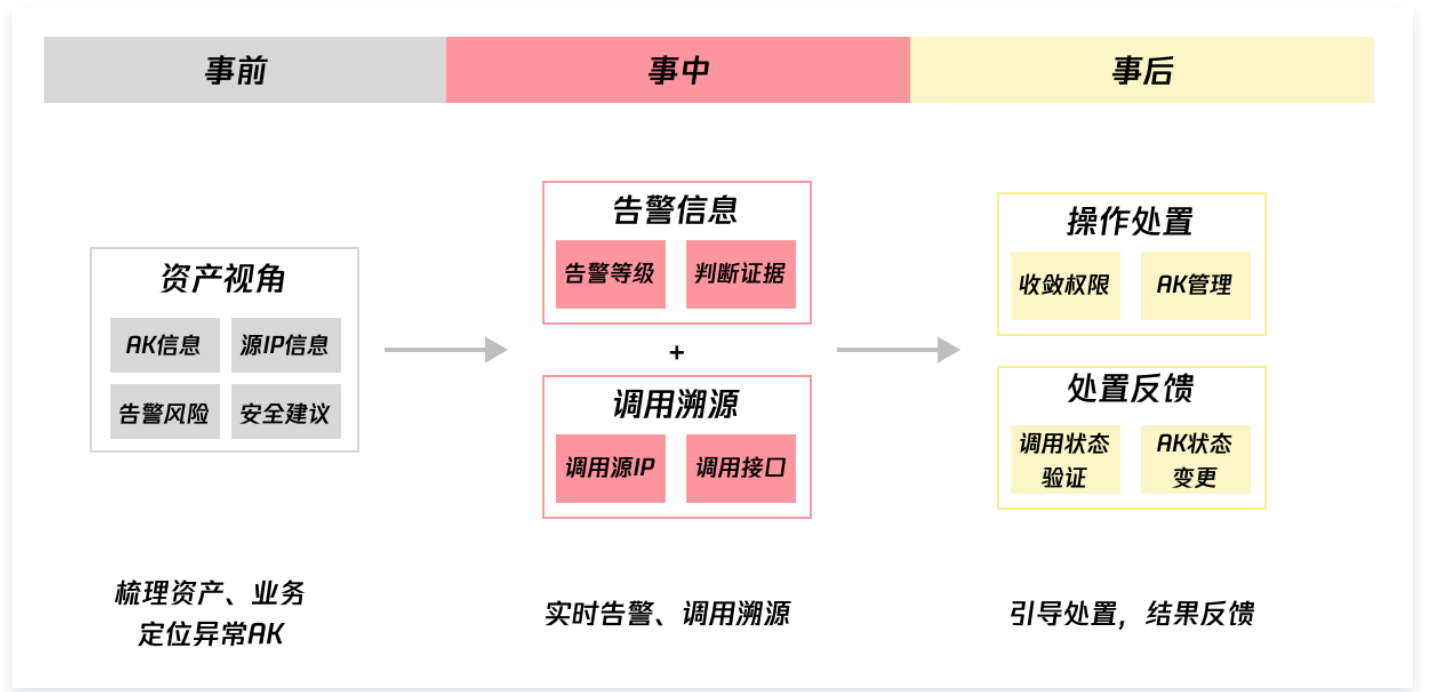
## 功能简介

最近更新时间：2025-09-17 21:28:59

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

**注意：**

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



### 功能点梳理

| 功能版块                | 功能点                                     | 解决问题                                      | 操作指引                 |
|---------------------|-----------------------------------------|-------------------------------------------|----------------------|
| 统计面板<br>资产概览 & 安全概览 | 快速了解 AK 资产情况，定位建议关注的异常 AK、待处理告警、待处理风险等。 | 定位高优问题，了解有多少 AK 需关注，待处理的问题有多少，近期安全运营趋势怎样。 | <a href="#">统计面板</a> |

|        |         |                                                                                                                                                                                                                                       |                                                                                                                                      |      |
|--------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------|
| 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   |         | <p>实时监控 AK 泄露与异常调用：</p> <ul style="list-style-type: none"> <li>● 黑客工具/行云管家/ cos-browser 识别。</li> <li>● GitHub 泄露（GitHub 合作 + IP 检查等）。</li> <li>● 异常 IP 调用敏感接口等。</li> </ul> <p>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。</p> | <ul style="list-style-type: none"> <li>● 实时告警泄露事件，全面分析并溯源异常调用；</li> <li>● 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。</li> </ul> | 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。

# 云 API 密钥安全使用方案

最近更新时间：2025-09-17 21:28:59

云 API 密钥 AccessKey（以下简称“AK”）是构建腾讯云 API 请求的重要凭证。您的 API 密钥代表您的账号身份和所拥有的权限，使用腾讯云 API 可以操作您名下的所有腾讯云资源。

AK 包含 SecretId 和 SecretKey，用于您调用 [腾讯云 API](#) 时生成签名，查看生成签名算法。SecretId 作为用户标识，**SecretKey（必须保密）** 为验证用户身份的密钥。

## ① 注意：

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

## AK 泄露案例

### 1. 代码仓库硬编码暴露风险

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

### 2. 客户端反编译导致的凭证提取

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

### 3. 技术文档与样例代码泄露

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

### 4. 临时密钥滥用

开发者在客户端直接生成临时密钥，攻击者在有效期内劫持并利用其发起恶意请求。

### 5. 日志与监控系统泄露

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

### 6. 服务器内明文配置的 AK 被攻击者获取

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

## AK 安全实践教程

### 避免使用主账号 AK

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

## 请勿在代码中嵌入 AK

嵌入代码中的 AK 凭证容易被人忽视，经验丰富的开发者会将其写入数据库或者独立的文件中，使得其管理起来更方便。

开发者应将 AK 存储在独立加密配置文件或密钥管理系统中（如腾讯云 KMS 白盒密钥），而非直接写入业务代码，降低因代码仓库权限管理疏漏或客户端反编译导致的泄露风险。

## 定期更新 AK

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

## 删除不需要的权限/AK

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

## 遵循最小权限原则申请账户

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限，不要授予更多无关权限。例如，一个用户仅是 COS 服务的使用者，那么不需要将其他服务的资源访问权限（如 CAM 读写权限）授予给该用户。

另外申请用户时，如果只需要 API，仅申请 API 权限用户即可，不要把控制台和 API 的用户混合。

## 事前 AK 请求情况梳理

在云安全中心 > 云 API 异常监测，实时做好 AK 的资产管理和备注。

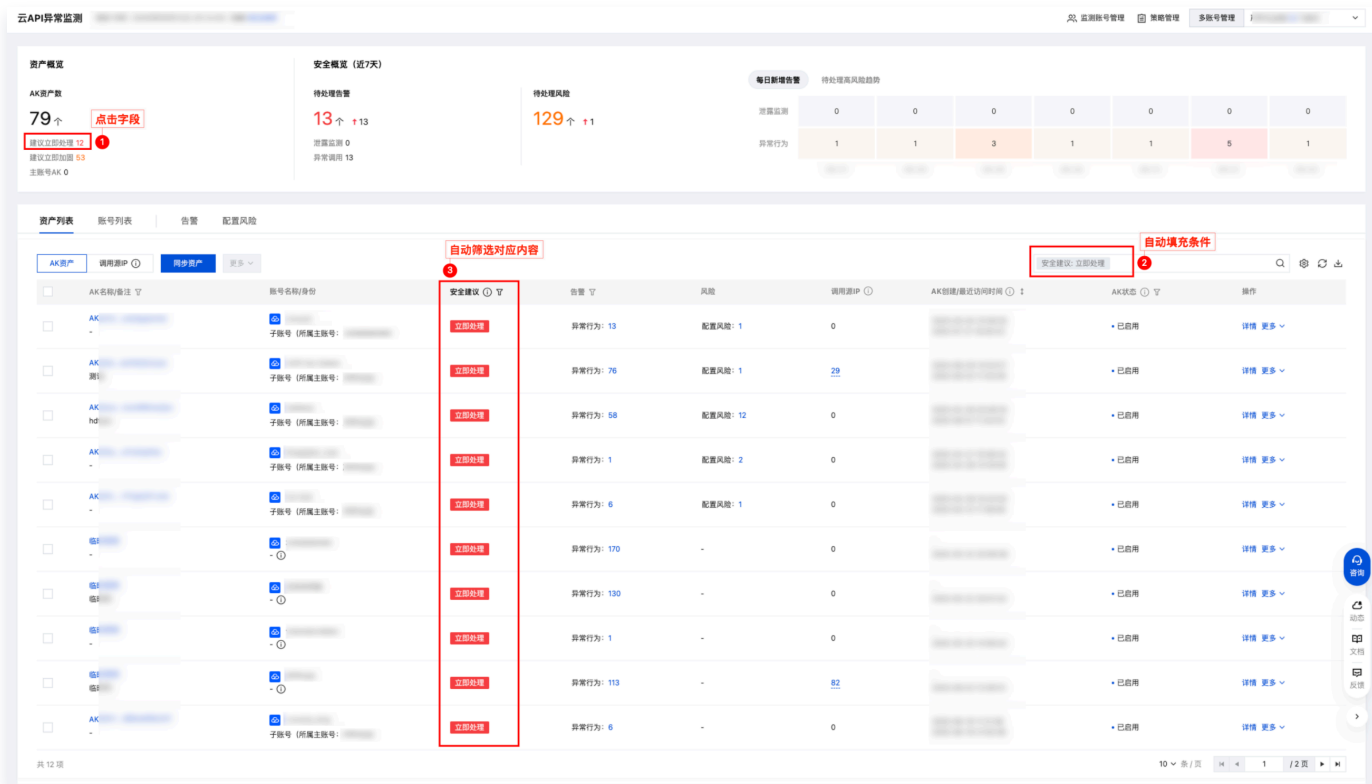
- AK 列表：梳理 AK 资产，了解我有多少把 AK，备注每把 AK 是什么业务在用。
- 调用源 IP：梳理调用源 IP，了解每个调用源 IP 属于哪个业务。
- 风险权限收敛：查看 AK 配置检查结果，梳理是否有不需要的高权限接口。
- 应急响应：当提前掌握好上面的情况后，出现 AK 泄露导致异常调用时，可以快速地完成 AK 替换。

最近更新时间: 2025-09-17 21:28:59

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. **资产概览**：统计当前腾讯云账号下主账号与子账号全部 AK 数量（包含永久密钥与临时密钥）与不同安全建议的 AK 数量。

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

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





# 资产列表

最近更新时间：2026-02-03 15:34:36

## 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”

资产列表

账号列表

告警

配置风险

AK资产

调用源IP

同步资产

更多

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

Q

| <input type="checkbox"/> | AK名称/备注 | 所属账号/AK类型 | 安全建议 | 告警   | 风险    | 调用源IP | AK创建/最近访问时间 | AK状态 | 操作    |
|--------------------------|---------|-----------|------|------|-------|-------|-------------|------|-------|
| <input type="checkbox"/> |         | 子账号       | 立即处理 | -    | 配置风险: | 0     | 2025-2025-  | 已启用  | 详情 更多 |
| <input type="checkbox"/> |         | 子账号       | 立即处理 | -    | 配置风险: | 0     | 2025-2025-  | 已启用  | 详情 更多 |
| <input type="checkbox"/> |         | 子账号       | 立即处理 | 异常行为 | 配置风险: |       | 2025-2025-  | 已启用  | 详情 更多 |

| 字段名        | 示例                                                                             | 说明                                                                                                                                                                                 |
|------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AK 名称/备注   | AKID75XXX<br>部门1AK                                                             | <div>AK 名称与自定义备注。</div> <ul style="list-style-type: none"><li>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。</li><li>备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li><li>支持筛选主账号密钥/子账号密钥/临时密钥。</li></ul> |
| 所属账号/AK 类型 | 账号 A<br>主账号/子账号（所属主账号：主账号 B）                                                   | <ul style="list-style-type: none"><li>AK 所属云厂商与账号，若为子账号展示所属主账号信息。</li><li>鼠标悬浮查看账号名称、账号 ID与 APPID。</li></ul>                                                                       |
| 安全建议       | <ul style="list-style-type: none"><li>立即处理</li><li>建议加固</li><li>暂无异常</li></ul> | <ul style="list-style-type: none"><li>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。</li><li>支持筛选不同建议管理的 AK。</li></ul>                                                              |

|              |                                                                                                 |                                                                                                                        |
|--------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 告警           | <ul style="list-style-type: none"><li>异常行为：x</li><li>泄露监测：x</li></ul>                           | <ul style="list-style-type: none"><li>近期末处理告警，单击拉起 <b>AK 详情</b> 抽屉，定位到<b>告警</b>页签。</li><li>支持筛选泄露监测/异常行为/无告警</li></ul> |
| 风险           | <ul style="list-style-type: none"><li>配置风险：x</li></ul>                                          | 近期末处理风险，单击拉起 <b>AK 详情</b> 抽屉，定位到 <b>配置风险</b> 页签。                                                                       |
| 调用源 IP       | 1                                                                                               | <ul style="list-style-type: none"><li>近七天调用该 AK 的 IP 数量。</li><li>鼠标悬浮查看源 IP、地域、IP 类型以及备注。</li></ul>                    |
| AK 创建/最近访问时间 | <ul style="list-style-type: none"><li>2025-01-01 18:00:00</li><li>2025-01-12 18:00:00</li></ul> | AK 创建与最近访问时间。 <ul style="list-style-type: none"><li>格式：YYYY-MM-DD HH:MM:SS。</li><li>支持排序。</li></ul>                    |
| AK 状态        | <ul style="list-style-type: none"><li>已禁用</li><li>已启用</li><li>已删除</li></ul>                     | 展示 AK 禁用/启用/删除状态。<br>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 <b>确定</b> 。 |
|      | 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。   |

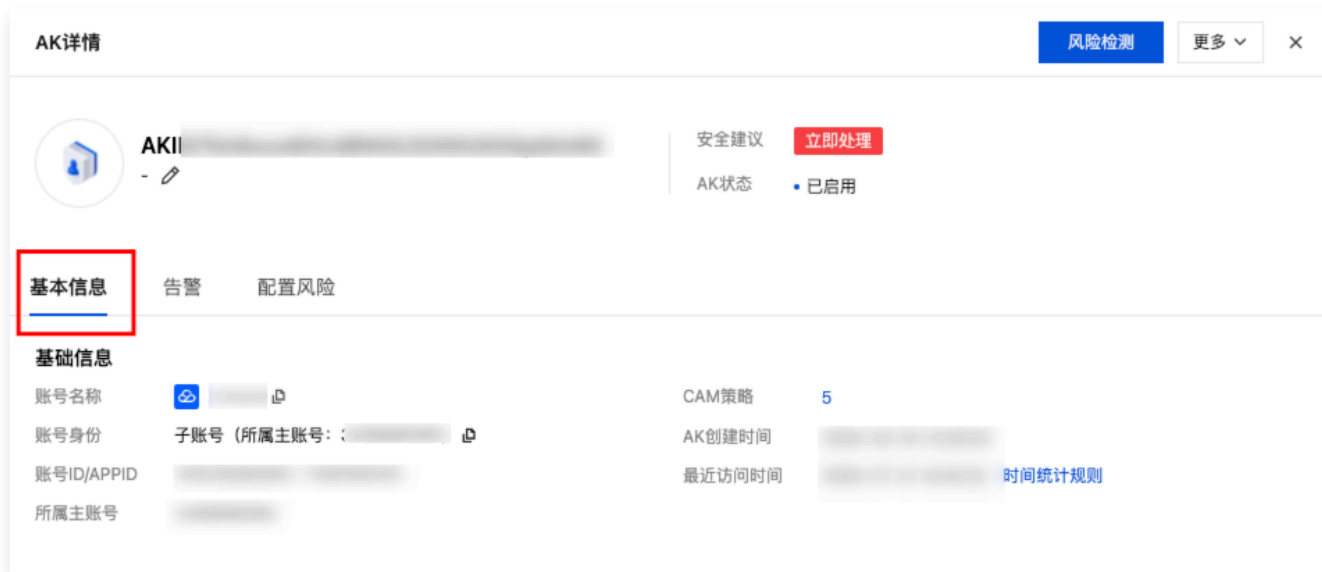
AK 详情

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。



| 资产列表    |         |      |          |         |       |             |      |       |  |
|---------|---------|------|----------|---------|-------|-------------|------|-------|--|
| AK资产    |         |      |          |         |       |             |      |       |  |
| AK名称/备注 | 账号名称/身份 | 安全建议 | 告警       | 风险      | 调用源IP | AK创建/最近访问时间 | AK状态 | 操作    |  |
| AK      | 子账号     | 立即处理 | 异常行为: 13 | 配置风险: 1 | 0     |             | 已启用  | 详情 更多 |  |
| AK      | 子账号     | 立即处理 | 异常行为: 76 | 配置风险: 1 | 29    |             | 已启用  | 详情 更多 |  |

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。



### AK详情

风险检测 更多 X

**AKI**

安全建议 **立即处理**

AK状态 **已启用**

**基本信息**

告警 配置风险

**基本信息**

账号名称 子账号 (所属主账号: )

账号身份 子账号

账号ID/APPID

所属主账号

CAM策略 5

AK创建时间

最近访问时间

时间统计规则

- 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](#)。

AK详情 风险检测 更多 ×

 **AK** - 编辑 安全建议 立即处理 AK状态 已启用

基本信息 **告警** 配置风险

标记处置 更多 全部 处理状态: 未处理 Q ⚙️ 🔄 📄

| <input type="checkbox"/> | 告警名称/类型              | 告警等级 | 告警时间 | 处理状态 | 操作    |
|--------------------------|----------------------|------|------|------|-------|
| <input type="checkbox"/> | 非控制台方式调用高危接口<br>异常行为 | 高危   |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 非控制台方式调用高危接口<br>异常行为 | 高危   |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 非控制台方式调用高危接口<br>异常行为 | 高危   |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 非控制台方式调用高危接口<br>异常行为 | 高危   |      | 未处理  | 详情 更多 |

- 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](#)。

AK详情 风险检测 更多 ×

 **AK** - 编辑 安全建议 立即处理 AK状态 已启用

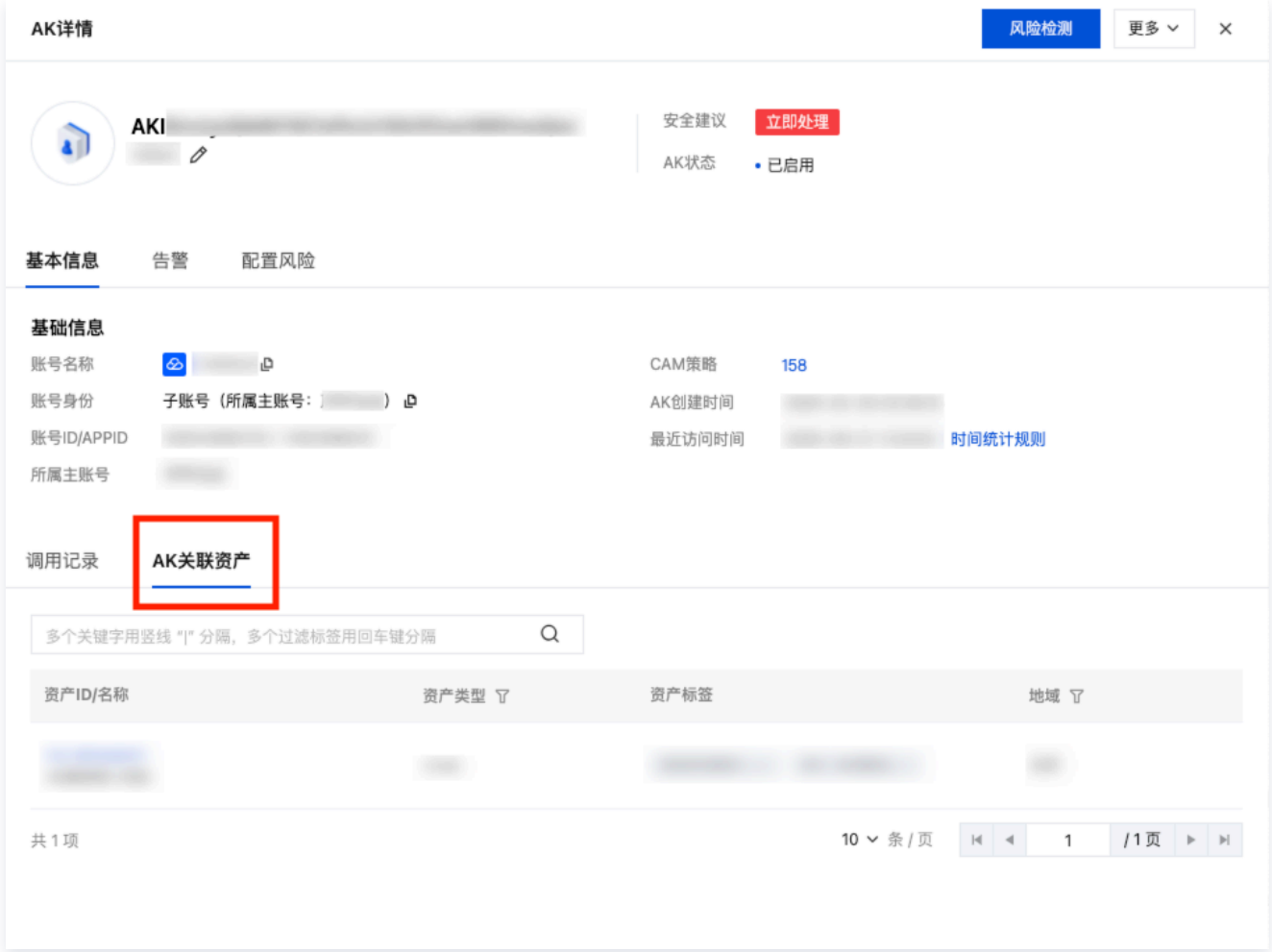
基本信息 告警 **配置风险**

重新检测 更多 全部 处理状态: 未处理 Q ⚙️ 🔄 📄

| <input type="checkbox"/> | 风险名称         | 风险等级 | 风险检出时间 | 处理状态 | 操作      |
|--------------------------|--------------|------|--------|------|---------|
| <input type="checkbox"/> | 不应该拥有高权限预设策略 | 严重   |        | 未处理  | 风险详情 更多 |

共 1 项 10 条 / 页 1 / 1 页

- 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<br>xxx | 该资产在云平台中的唯一标识符及其自定义名称。<br>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。<br>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。<br>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。

AK详情

检测更多

基本信息告警风险

基础信息

账号名称子账号账号ID/APPID所属主账号CAM策略5AK创建时间最近访问时间

调用记录AK关联资产

AK权限策略配置建议

1 确认需要收敛权限的AK

2 禁用或删除 Access Key

3 修改权限策略

4 验证权限回收效果

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

| 调用源IP/地域/备注    | IP类型      | 调用方式 | 调用接口/服务                       | CAM策略 | 操作    |
|----------------|-----------|------|-------------------------------|-------|-------|
| 中国-四川省-成都市   - | 账号外 (未备注) | API  | DescribeAccountPrivileges cdb | 5     | 详情 更多 |
| 中国-四川省-成都市   - | 账号外 (未备注) | API  | DescribeAccounts cdb          | 5     | 详情 更多 |
| 中国-四川省-成都市   - | 账号外 (未备注) | API  | DescribeAsyncRequestInfo cdb  | 5     | 详情 更多 |

| 字段名          | 示例                       | 说明                                                                                                                   |
|--------------|--------------------------|----------------------------------------------------------------------------------------------------------------------|
| 调用源 IP/地域/备注 | 1.x.x.1<br>中国-北京   部门1AK | 调用源 IP、所属地域与自定义备注。 <ul style="list-style-type: none"><li>IP 内容支持一键复制。</li><li>备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li></ul> |
| 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。                                                                                 |

|                         |                                                                                                                                        |                                                                                                                                                                                                                             |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | <ul style="list-style-type: none"><li>• 账号内（未备注）</li><li>• 账号外（已备注）</li><li>• 账号外（未备注）</li><li>• 局域网（已备注）</li><li>• 局域网（未备注）</li></ul> | <ul style="list-style-type: none"><li>• 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。</li><li>• 账号外（已备注）：非账号内 IP 但有备注。</li><li>• 账号外（未备注）：非账号内 IP 且无备注。</li><li>• 局域网（已备注）：局域网 IP 地址，有备注。</li><li>• 局域网（未备注）：局域网 IP 地址，无备注。</li></ul> |
| 调用方式                    | <ul style="list-style-type: none"><li>• API</li><li>• 控制台</li></ul>                                                                    | 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<br>cdb                                                                                                       | 调用的接口与接口所属服务。                                                                                                                                                                                                               |
| CAM 策略<br>用户（角色）/<br>策略 | 1<br>用户：xxx<br>策略：1                                                                                                                    | 该 AK 关联的 CAM 策略个数，单击 <b>数字</b> 打开 CAM 策略详情弹窗。<br>临时密钥由于聚合展示,所以展示用户（角色）。                                                                                                                                                     |
| 调用状态/次数                 | <ul style="list-style-type: none"><li>• 成功<br/>(x次)</li><li>• 失败<br/>(x次)</li></ul>                                                    | 调用该 AK 成功/失败状态及次数。                                                                                                                                                                                                          |
| 首次/最近调用<br>时间           | <ul style="list-style-type: none"><li>• 2025-01-01 18:00:00</li><li>• 2025-01-12 18:00:00</li></ul>                                    | 首次与最近调用时间。 <ul style="list-style-type: none"><li>• 格式：YYYY-MM-DD HH:MM:SS。</li><li>• 支持排序。</li></ul>                                                                                                                        |
| IP 所属资产<br>(ID/名称)      | ins-xxx<br>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。

近7天

多个关键字用竖线 "|" 分隔, 多个过滤标签用回车键分隔

| 调用源IP/地域/备注 | IP类型      | 调用方式 | 调用接口/服务          | CAM策略 | 操作    |
|-------------|-----------|------|------------------|-------|-------|
| 中国-广东省-广州市  | 账号外 (未备注) | API  | SearchLog<br>cwp | 1     | 详情 更多 |
| 中国-广东省-广州市  | 账号外 (未备注) | API  | SearchLog<br>cwp | 1     |       |

添加白名单策略  
管理白名单策略

● 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。

调用记录详情

调用源IP  
调用源IP地域  
调用源IP备注  
IP类型  
IP所属资产ID  
调用AK名称  
调用AK备注

调用方式  
调用接口  
调用服务  
调用次数  
调用状态  
首次调用时间  
最近调用时间

API  
DescribeAccountPrivileges  
cdb  
273  
成功

调用详情 1/273

调用时间  
请求ID  
6dc

```
1 {
2   server: "",
3   assumerUin: "",
4   cliIp: "",
5   ver: "",
6   module: "cdb",
7   language: "zh-CN",
8   reqSrc: "API",
9   httpMethod: "POST",
10  accountArea: "0",
11  assumerOwnerUin: "",
12  ...
13 }
```

调用记录详情

```
17 vpcId: "0",
18 sigMethod: "
19 name: "",
20 action: "Describe
21 uin: "
22 reqHost: "cdb.
23 region: "none",
24 accUin: "
25 timestamp: "
26 }
```

CAM策略详情 (5)

| 策略名称                       | 策略类型  | 操作           |
|----------------------------|-------|--------------|
| AdministratorAccess        | 预设策略  | 策略详情 前往CAM查看 |
|                            | 自定义策略 | 策略详情 前往CAM查看 |
| QcloudFinanceFullAccess    | 预设策略  | 策略详情 前往CAM查看 |
| QcloudWeDataFullAccess     | 预设策略  | 策略详情 前往CAM查看 |
| QcloudWeDataReadOnlyAccess | 预设策略  | 策略详情 前往CAM查看 |

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



调用记录详情

```
17     vpcId: "0",
18     sigMethod: "",
19     name: "",
20     action: "Describe",
21     uin: "",
22     reqHost: "cdb.",
23     region: "none"
```

CAM策略详情

```
1  {
2      statement: [
3          {
4              action: "*",
5              effect: "allow",
6              resource: "*"
7          },
8      ],
9      version: "2.0"
10 }
```

复制

|                            |      |              |
|----------------------------|------|--------------|
| QCloudFinanceFullAccess    | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataFullAccess     | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataReadOnlyAccess | 预设策略 | 策略详情 前往CAM查看 |

- 更多

- 添加白名单策略：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：

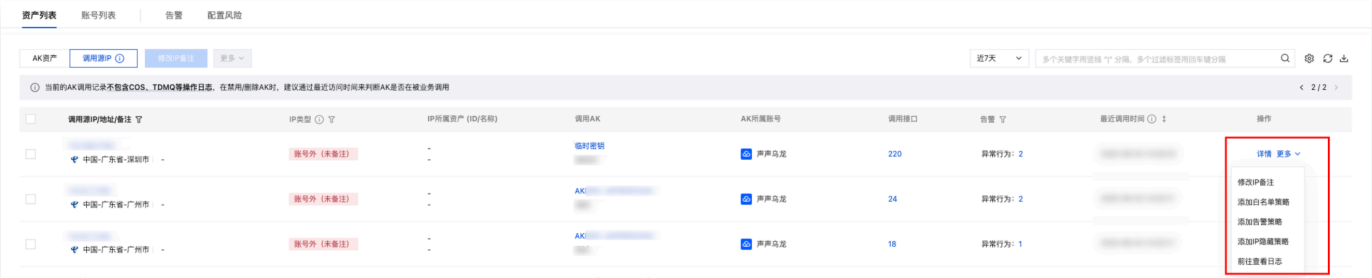
- 列表数据聚合逻辑：一天内同一 IP 调用同一账号下的 AK。
- 仅展示永久密钥的 API 请求。

| 资产列表                                                     |           |                |      |        |      |         |        |    |    |
|----------------------------------------------------------|-----------|----------------|------|--------|------|---------|--------|----|----|
| AK资产                                                     |           |                |      |        |      |         |        |    |    |
| 您可以通过点击隐藏调用源IP，隐藏后将不再显示在列表中。如您需要批量隐藏调用源IP，可点击前往 配置IP隐藏策略 |           |                |      |        |      |         |        |    |    |
| 调用源IP地址/备注                                               | IP类型      | IP所属资产 (ID/名称) | 调用AK | AK所属账号 | 调用接口 | 告警      | 最近调用时间 | 操作 |    |
| 中国-广东省-深圳市                                               | 账号外 (未备注) | -              | 临时密钥 | 25     | 220  | 异常行为: 2 |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AKI  | 25     | 24   | 异常行为: 2 |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AK   | 25     | 18   | 异常行为: 1 |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AKI  | 25     | 26   | -       |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AKI  | 25     | 24   | 异常行为: 1 |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AKI  | 25     | 19   | 异常行为: 2 |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AKI  | 25     | 22   | -       |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AK   | 25     | 21   | 异常行为: 1 |        | 详情 | 更多 |
| 中国-广东省-深圳市                                               | 账号外 (未备注) | -              | 临时密钥 | 25     | 268  | -       |        | 详情 | 更多 |
| 中国-广东省-广州市                                               | 账号外 (未备注) | -              | AKI  | 25     | 24   | 异常行为: 1 |        | 详情 | 更多 |

| 字段名             | 示例                                                                                                                                            | 说明                                                                                                                                                                                                                                                        |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 调用源 IP/地域/备注    | <ul style="list-style-type: none"><li>已隐藏</li><li>未隐藏</li></ul>                                                                               | <p>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。</p> <ul style="list-style-type: none"><li>IP内容支持一键复制。</li><li>备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li></ul>                                                                                                      |
| IP类型            | <ul style="list-style-type: none"><li>账号内（已备注）</li><li>账号内（未备注）</li><li>账号外（已备注）</li><li>账号外（未备注）</li><li>局域网（已备注）</li><li>局域网（未备注）</li></ul> | <ul style="list-style-type: none"><li>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。</li><li>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。</li><li>账号外（已备注）：非账号内 IP 但有备注。</li><li>账号外（未备注）：非账号内 IP 且无备注。</li><li>局域网（已备注）：局域网IP地址，有备注。</li><li>局域网（未备注）：局域网IP地址，无备注。</li></ul> |
| 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 <b>数字</b> 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 <b>数字</b> 打开 <b>数字调用源 IP</b> 详情抽屉。                                                                              |
| 告警      | <ul style="list-style-type: none"><li>异常行为：x</li><li>泄露监测：x</li></ul> | <ul style="list-style-type: none"><li>近期末处理告警，单击拉起<b>调用源 IP</b> 详情抽屉，定位到告警页签。</li><li>支持筛选泄露监测/异常行为/无告警。</li></ul> |
| 最近调用时间  | 2025-01-01 18:00:00                                                   | 最近调用时间。 <ul style="list-style-type: none"><li>格式：YYYY-MM-DD HH:MM:SS。</li><li>支持排序。</li></ul>                      |

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 <b>确定</b> 。   |
|      | 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。

调用源IP详情

修改IP备注更多

AK权限策略配置建议收起建议

1 检查AK是否有需要收敛的权限

根据调用记录与相关告警、风险，定位使用相关接口的CAM策略。

当前页面未包含COS的调用记录，COS的调用记录可根据最后访问时间和COS开通的CLS日志进行判断。

2 收敛权限策略或禁用/删除api 密钥

收敛权限

同步使用该api 密钥的相关业务方后，在权限策略中移除与接口相关的权限。[查看示意](#)

禁用/删除

登录 访问管理 管理控制台，并进入 访问密钥-API密钥管理 /用户列表-API密钥。[前往登录](#)

确保api 密钥最近访问时间一段时间没有更新后，禁用对应的 api 密钥。

保留禁用的api 密钥一段时间（紧急情况下可以恢复密钥），根据情况选择是否删除AK。

其他使用建议详见 [云API密钥安全使用方案](#)

调用记录

近7天

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

| AK名称/备注 | 调用方式 | 调用接口/服务                      | CAM策略 | 调用状态/次数     | 操作                                    |
|---------|------|------------------------------|-------|-------------|---------------------------------------|
| AK      | API  | SearchLog<br>cwp             | 1     | 成功<br>(17次) | <a href="#">详情</a> <a href="#">更多</a> |
| AKI     | API  | DescribeHostLoginList<br>cwp | 1     | 成功<br>(8次)  | <a href="#">详情</a> <a href="#">更多</a> |
| AKII    | API  | DescribeLogType<br>cwp       | 1     | 成功<br>(1次)  | <a href="#">详情</a> <a href="#">更多</a> |

| 字段名      | 示例                                                              | 说明                                                                                                                                               |
|----------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| AK 名称/备注 | AKID75XXX<br>部门1AK                                              | AK 名称与自定义备注。 <ul style="list-style-type: none"><li>AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 <b>AK 详情</b> 抽屉。</li><li>备注可自定义编辑，不超过20字符，若备注为空显示“-”</li></ul> |
| 调用方式     | <ul style="list-style-type: none"><li>API</li><li>控制台</li></ul> | 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  | DescribeAccountP<br>rivileges<br>cdb                            | 调用的接口与接口所属服务。                                                                                                                                    |
| CAM 策略   | 1<br>用户：xxx                                                     | 该 AK 关联的 CAM 策略个数，单击 <b>数字</b> 打开 CAM 策略详情弹窗。                                                                                                    |

|                 |                                                                         |                                                                                               |
|-----------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| 用户（角色） / 策略     | 策略：1                                                                    | 临时密钥由于聚合展示,所以展示用户（角色）。                                                                        |
| 调用状态/次数         | <ul style="list-style-type: none"><li>成功 (x次)</li><li>失败 (x次)</li></ul> | 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。 <ul style="list-style-type: none"><li>格式：YYYY-MM-DD HH:MM:SS。</li><li>支持排序。</li></ul> |
| 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。

调用记录

近7天

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

| AK名称/备注 | 调用方式 | 调用接口/服务                   | CAM策略 | 调用状态/次数  | 操作                 |
|---------|------|---------------------------|-------|----------|--------------------|
| AK      | API  | SearchLog cwp             | 1     | 成功 (17次) | 详情 更多              |
| AKI     | API  | DescribeHostLoginList cwp | 1     | 成功 (8次)  | 添加白名单策略<br>管理白名单策略 |

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



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

调用记录详情

```
17    vpcId: "0",
18    sigMethod: "
19    name: "",
20    action: "Describ
21    uin: "
22    reqHost: "cdb.
23    region: "none"
```

CAM策略详情

```
1    {
2      statement: [
3        {
4          action: "*",
5          effect: "allow",
6          resource: "*"
7        },
8      ],
9      version: "2.0"
10   }
```

复制

|                            |      |              |
|----------------------------|------|--------------|
| QCloudFinanceFullAccess    | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataFullAccess     | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataReadOnlyAccess | 预设策略 | 策略详情 前往CAM查看 |

- 更多

- 添加白名单策略：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：2025-09-17 21:28:59

## 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。

资产列表

账号列表

告警

配置风险

风险标签

多个关键字用空格“ ”分隔，多个过滤标签用回车键分隔

账号名称/类型

访问方式

安全建议

告警

风险

最近登录IP/时间

账号保护

操作

子账号 (所属主账号: )

API

立即处理

-

配置风险: 2

登录保护: 未开启

操作保护: 未开启

详情 更多

子账号 (所属主账号: )

控制台与API

立即处理

异常行为: 4

配置风险: 12

登录保护: 开启

操作保护: 开启

详情 更多

子账号 (所属主账号: )

API

立即处理

异常行为: 7

配置风险: 1

登录保护: 开启

操作保护: 开启

详情 更多

子账号 (所属主账号: )

控制台与API

立即处理

-

配置风险: 1

登录保护: 未开启

操作保护: 未开启

详情 更多

子账号 (所属主账号: )

控制台与API

立即处理

-

配置风险: 13

登录保护: 未开启

操作保护: 未开启

详情 更多

子账号 (所属主账号: )

控制台与API

立即处理

-

-

登录保护: 未开启

操作保护: 未开启

详情 更多

子账号 (所属主账号: )

控制台与API

立即处理

-

-

登录保护: 未开启

操作保护: 开启

详情 更多

子账号 (所属主账号: )

控制台与API

建议加固

-

配置风险: 11

登录保护: 未开启

操作保护: 未开启

详情 更多

子账号 (所属主账号: )

控制台与API

建议加固

-

-

登录保护: 开启

操作保护: 开启

详情 更多

子账号 (所属主账号: )

控制台与API

建议加固

-

配置风险: 11

登录保护: 未开启

操作保护: 未开启

详情 更多

共 120 项

10 / 页1 / 12 页

新增

刷新

文档

反馈

| 字段名     | 示例                                                                                | 说明                                                                                                                    |
|---------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 账号名称/身份 | <ul style="list-style-type: none"><li>账号 A</li><li>主账号/子账号（所属主账号：主账号 B）</li></ul> | <ul style="list-style-type: none"><li>AK 所属云厂商与账号，若为子账号展示所属主账号信息。</li><li>鼠标悬浮查看账号名称、账号 ID与 APPID。</li></ul>          |
| 访问方式    | <ul style="list-style-type: none"><li>API</li><li>控制台与 API</li></ul>              | <ul style="list-style-type: none"><li>该账号的访问途径。</li><li>支持筛选 API/控制台与 API。</li></ul>                                  |
| 安全建议    | <ul style="list-style-type: none"><li>立即处理</li><li>建议加固</li><li>暂无异常</li></ul>    | <ul style="list-style-type: none"><li>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。</li><li>支持筛选不同建议管理的 AK。</li></ul> |
| 告警      | <ul style="list-style-type: none"><li>异常行为: x</li><li>泄露监测: x</li></ul>           | <ul style="list-style-type: none"><li>近期末处理告警，单击拉起 <b>AK 详情</b> 抽屉，定位到告警页签。</li><li>支持筛选泄露监测/异常行为/无告警。</li></ul>      |
| 风险      | 配置风险: x                                                                           | 近期末处理风险，单击拉起 <b>AK 详情</b> 抽屉，定位到风险页签。                                                                                 |

|           |                                                                                                 |                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 最近登录IP/时间 | <ul style="list-style-type: none"><li>1.x.x.1（中国-广东省-深圳市）</li><li>2025-01-12 18:00:00</li></ul> | <ul style="list-style-type: none"><li>最近一次登录的IP地址（含地理位置）及登录时间。</li><li>时间格式：YYYY-MM-DD HH:MM:SS。</li><li>支持按时间排序。</li></ul> |
| 账号保护      | <ul style="list-style-type: none"><li>登录保护：开启</li><li>操作保护：开启</li></ul>                         | <ul style="list-style-type: none"><li>展示账号的登录保护与操作保护等安全状态的开启情况。</li><li>支持筛选全部开启/部分开启/未开启。</li></ul>                        |

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

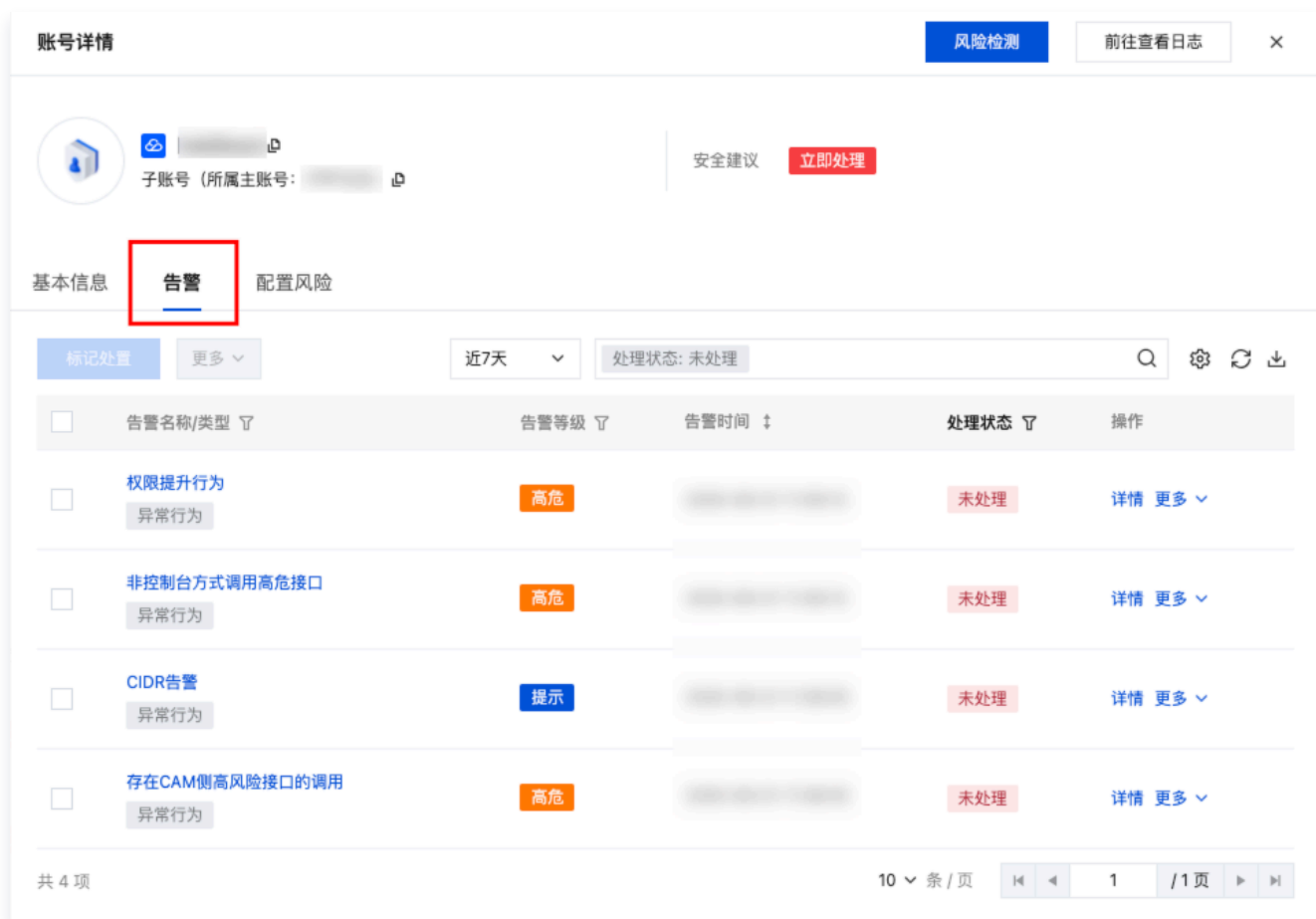
1. 登录 云安全中心控制台，在左侧导览中，单击云 API 异常监测。
2. 在账号列表中，选择所需账号，单击详情。



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](#)。

账号详情 风险检测 前往查看日志 ×

  子账号 (所属主账号: ) 安全建议 立即处理

基本信息 告警 **配置风险**

重新检测 更多 近7天 处理状态: 未处理 Q ⚙️ 🔄 📄

| <input type="checkbox"/> | 风险名称                  | 风险等级 | 风险检出时间 | 处理状态 | 操作      |
|--------------------------|-----------------------|------|--------|------|---------|
| <input type="checkbox"/> | 不应该拥有高权限预设策略          | 严重   |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> | 应该对访问管理(CAM)的操作权限进行收敛 | 高危   |        | 未处理  | 风险详情 更多 |

- 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。

账号详情 风险检测 前往查看日志 ×

 **AK权限策略配置建议** 收起建议

1

**检查AK是否有需要收敛的权限**

- 根据调用记录与相关告警、风险，定位使用相关接口的CAM策略。
- 当前页面未包含COS的调用记录，COS的调用记录可根据最后访问时间和COS开通的CLS日志进行判断。

2

**收敛权限策略或禁用/删除api 密钥**

收敛权限

- 同步使用该api 密钥的相关业务方后，在权限策略中移除与接口相关的权限。[查看示意](#)

禁用/删除

- 登录 访问管理 管理控制台，并进入 访问密钥-API密钥管理 / 用户列表-API密钥。[前往登录](#)
- 确保api 密钥最近访问时间一段时间没有更新后，禁用对应的 api 密钥。
- 保留禁用的api 密钥一段时间（紧急情况下可以恢复密钥），根据情况选择是否删除AK。

其他使用建议详见 [云API密钥安全使用方案](#)

**调用记录**

近7天 多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔 Q 📄

| 调用源IP/地域/备注                                                                                        | IP类型      | 调用方式 | 调用接口/服务                              | CAM策略 | 操作    |
|----------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|-------|-------|
|  中国-湖北省-武汉市   - | 账号外 (未备注) | 控制台  | DescribeOrganizationUserInfo<br>csip | 6     | 详情 更多 |
|  中国-湖北省-武汉市   - | 账号外 (未备注) | 控制台  | DescribeOrganizationUserInfo<br>csip | 6     | 详情 更多 |
|  中国-湖北省-武汉市   - | 账号外 (未备注) | 控制台  | DescribeOrganizationInfo<br>csip     | 6     | 详情 更多 |

| 字段名             | 示例                                                                                                                                                   | 说明                                                                                                                                                                                                                                                                   |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 调用源 IP/地域/备注    | <ul style="list-style-type: none"> <li>1.x.x.1</li> <li>中国-北京   部门 1AK</li> </ul>                                                                    | 调用源 IP、所属地域与自定义备注。 <ul style="list-style-type: none"> <li>IP 内容支持一键复制。</li> <li>备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li> </ul>                                                                                                                                              |
| IP 类型           | <ul style="list-style-type: none"> <li>账号内（已备注）</li> <li>账号内（未备注）</li> <li>账号外（已备注）</li> <li>账号外（未备注）</li> <li>局域网（已备注）</li> <li>局域网（未备注）</li> </ul> | <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>账号外（已备注）：非账号内 IP 但有备注。</li> <li>账号外（未备注）：非账号内 IP 且无备注。</li> <li>局域网（已备注）：局域网 IP 地址，有备注。</li> <li>局域网（未备注）：局域网 IP 地址，无备注。</li> </ul> |
| 调用方式            | <ul style="list-style-type: none"> <li>API</li> <li>控制台</li> </ul>                                                                                   | 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         | <ul style="list-style-type: none"> <li>DescribeAccountPrivileges</li> <li>cdb</li> </ul>                                                             | 调用的接口与接口所属服务。                                                                                                                                                                                                                                                        |
| CAM 策略用户（角色）/策略 | 1<br>用户：xxx<br>策略：1                                                                                                                                  | 该 AK 关联的 CAM 策略个数，单击 <b>数字</b> 打开 CAM 策略详情弹窗。<br>临时密钥由于聚合展示,所以展示用户（角色）。                                                                                                                                                                                              |
| 调用状态/次数         | <ul style="list-style-type: none"> <li>成功 (x次)</li> <li>失败 (x次)</li> </ul>                                                                           | 调用该 AK 成功/失败状态及次数。                                                                                                                                                                                                                                                   |
| 首次/最近调用时间       | <ul style="list-style-type: none"> <li>2025-01-01 18:00:00</li> <li>2025-01-12 18:00:00</li> </ul>                                                   | 首次与最近调用时间。 <ul style="list-style-type: none"> <li>格式：YYYY-MM-DD HH:MM:SS。</li> <li>支持排序。</li> </ul>                                                                                                                                                                  |
| IP 所属资产 (ID/名称) | <ul style="list-style-type: none"> <li>ins-xxx</li> <li>机器1号</li> </ul>                                                                              | 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。

调用记录详情

```
17    vpcId: "0",
18    sigMethod: "[REDACTED]",
19    name: "",
20    action: "Describe",
21    uin: "[REDACTED]",
22    reqHost: "cdb.[REDACTED]",
23    region: "none"
```

CAM策略详情

```
1  {
2      statement: [
3          {
4              action: "*",
5              effect: "allow",
6              resource: "*"
7          },
8      ],
9      version: "2.0"
10 }
```

复制

|                            |      |              |
|----------------------------|------|--------------|
| QCloudFinanceFullAccess    | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataFullAccess     | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataReadOnlyAccess | 预设策略 | 策略详情 前往CAM查看 |

- 更多

- 添加白名单策略：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：2025-09-17 21:28:59

## 告警列表

1. 登录 [云安全中心控制台](#)，在左侧导览中，单击云 API 异常监测。

2. 在告警列表中，基于告警规则视角，查看告警内容（泄露、异常调用）， 关联 AK 与异常调用记录，并提供权限策略配置建议。

资产列表

账号列表

告警

配置风险

标记位置

更多

近7天

处理状态: 未处理

| <input type="checkbox"/> | 告警名称/类型                  | 告警等级 | AK名称/备注 | 账号名称/身份       | 告警时间 | 处理状态 | 操作    |
|--------------------------|--------------------------|------|---------|---------------|------|------|-------|
| <input type="checkbox"/> | 通过API调用安全产品的敏感接口<br>异常行为 | 中危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 通过API调用安全产品的敏感接口<br>异常行为 | 中危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 非控制台方式调用高危接口<br>异常行为     | 高危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 权限提升行为<br>异常行为           | 高危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 存在CAM侧高风险接口的调用<br>异常行为   | 高危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | CIDR告警<br>异常行为           | 提示   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 通过API调用安全产品的敏感接口<br>异常行为 | 中危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 通过API调用安全产品的敏感接口<br>异常行为 | 中危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 通过API调用安全产品的敏感接口<br>异常行为 | 中危   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |
| <input type="checkbox"/> | 控制台创建密钥操作<br>异常行为        | 提示   |         | 子账号 (所属主账号: ) |      | 未处理  | 详情 更多 |

共 13 项

10 条 / 页

1 / 2 页

咨询

动态

文档

反馈

| 字段名         | 示例                                                                                                        | 说明               |
|-------------|-----------------------------------------------------------------------------------------------------------|------------------|
| 告警名称/<br>类型 | <ul style="list-style-type: none"><li>异常行为</li><li>泄露监测</li></ul>                                         | 单击拉起告警详情抽屉。      |
| 告警等级        | <ul style="list-style-type: none"><li>严重</li><li>高危</li><li>中危</li><li>低危</li><li>提示</li><li>无效</li></ul> | 基于腾讯云安全实践评定告警等级。 |



|              |                                                                             |                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| AK 名称/<br>备注 | AKID75XXX<br>部门1AK                                                          | AK 名称与自定义备注。 <ul style="list-style-type: none"><li>AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 <b>AK 详情</b> 抽屉。</li><li>备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li></ul> |
| 账号名称/<br>身份  | 账号 A<br>主账号/子账号（所属主账号：主账号 B）                                                | <ul style="list-style-type: none"><li>AK 所属云厂商与账号，若为子账号展示所属主账号信息。</li><li>鼠标悬浮查看账号 ID 与 APPID；支持筛选主账号/子账号。</li></ul>                              |
| 告警时间         | 2025-01-12 18:00:00                                                         | 告警发生时间。 <ul style="list-style-type: none"><li>格式：YYYY-MM-DD HH:MM:SS。</li><li>支持排序。</li></ul>                                                     |
| 处理状态         | <ul style="list-style-type: none"><li>未处理</li><li>已处置</li><li>已忽略</li></ul> | 展示告警处理状态，手动完成标记，处理状态支持筛选。                                                                                                                         |

3. 在告警列表中，选择所需告警，单击**详情/更多**。



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

## 规则说明

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

| 规则名称                | 规则说明                                                                                                                |
|---------------------|---------------------------------------------------------------------------------------------------------------------|
| 根密钥调用高危接口           | 主账号访问密钥调用高危接口。<br>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：<br>cam.ListAccessKeys、cam.DeleteUser... |
| 非控制台方式调用高危接口        | 使用非控制台方式(主要是通过 SDK 调用云 API)，调用高危接口。                                                                                 |
| 未授权的服务调用            | 通过 API 调用未授权的服务，需要收敛该账号/角色的权限。                                                                                      |
| 创建密钥操作              | 有新的密钥被创建。                                                                                                           |
| 权限提升行为              | 通过调用 sts、cam 的部分接口，该用户权限得到提升。                                                                                       |
| 非正常时间段敏感行为          | 在晚上10点至凌晨6点时间段内，通过控制台或者 API 执行一些敏感操作，例如删除资源等操作。                                                                     |
| 新增用户调用高危接口          | 1天内创建的用户调用了高危 API，需要注意。                                                                                             |
| GitHub密钥确认请求        | 检查请求是否来源于 GitHubAK 回调的出口 IP。<br>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。<br>行云管家是一个多云管理平台,可以可视化的管理云上 CVM、网络、镜像等，部分攻击者也会使用。需要梳理运维人员是否使用行云管家。                            |
| 自动化助手高危操作           | 通过调用 tat 的部分接口，直接对机器执行命令。                                                                                           |

# 告警详情

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

查看告警信息，告警信息包括：告警策略、策略描述、AK 名称、AK 备注、AK 关联风险、CAM 策略、账号名称以及账号身份。

告警详情

未处理

标记处置

更多

×

通过API调用安全产品的敏感接口

异常行为

告警等级

中危

告警时间

告警策略

通过API调用安全产品的敏感接口

策略描述

通过API调用安全产品(waf、cwp、csip等)的一些敏感接口

AK名称

AK备注

AK关联风险

1

CAM策略

1

账号名称

账号身份

子账号 (所属主账号: )

- 查看异常调用记录，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。

告警详情

未处理

标记处置

更多

AK权限策略配置建议

收起建议

1 检查AK是否有需要收敛的权限

根据调用记录与相关告警、风险，定位使用相关接口的CAM策略。

当前页面未包含COS的调用记录，COS的调用记录可根据最后访问时间和COS开通的CLS日志进行判断。

2 收敛权限策略或禁用/删除api 密钥

收敛权限

同步使用该api 密钥的相关业务方后，在权限策略中移除与接口相关的权限。[查看示意](#)

禁用/删除

登录 访问管理 管理控制台，并进入 访问密钥-API密钥管理 /用户列表-API密钥。[前往登录](#)

确保api 密钥最近访问时间一段时间没有更新后，禁用对应的 api 密钥。

保留禁用的api 密钥一段时间（紧急情况下可以恢复密钥），根据情况选择是否删除AK。

其他使用建议详见 [云API密钥安全使用方案](#)

异常调用记录

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

| 调用源IP/地域/备注           | IP类型      | 调用方式 | 调用接口/服务                       | CAM策略 | 操作                                    |
|-----------------------|-----------|------|-------------------------------|-------|---------------------------------------|
| <div>中国-广东省-广州市</div> | 账号外 (未备注) | API  | ModifyBruteAttackRules<br>cwp | 1     | <a href="#">详情</a> <a href="#">更多</a> |
| <div>中国-广东省-广州市</div> | 账号外 (未备注) | API  | ModifyBruteAttackRules<br>cwp | 1     | <a href="#">详情</a> <a href="#">更多</a> |

| 字段名          | 示例                                                                                                                           | 说明                                                                                                                                                                                                                                                        |
|--------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 调用源 IP/地域/备注 | 1.1.1.1<br>中国-北京   部门<br>1AK                                                                                                 | 调用源 IP、所属地域与自定义备注。 <ul style="list-style-type: none"><li>IP 内容支持一键复制。</li><li>备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li></ul>                                                                                                                                      |
| IP类型         | <ul style="list-style-type: none"><li>账号内（已备注）</li><li>账号内（未备注）</li><li>账号外（已备注）</li><li>账号外（未备注）</li><li>局域网（已备注）</li></ul> | <ul style="list-style-type: none"><li>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。</li><li>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。</li><li>账号外（已备注）：非账号内 IP 但有备注。</li><li>账号外（未备注）：非账号内 IP 且无备注。</li><li>局域网（已备注）：局域网IP地址，有备注。</li><li>局域网（未备注）：局域网IP地址，无备注。</li></ul> |

©2013-2026 腾讯云版权所有

第128 共160页

|                 |                                                                                                     |                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <ul style="list-style-type: none"><li>● 局域网（未备注）</li></ul>                                          |                                                                                                                                                       |
| AK 名称/备注        | AKID75XXX<br>部门1AK                                                                                  | AK 名称与自定义备注。 <ul style="list-style-type: none"><li>● AK 保留前6位与后11位，中间省略，支持一键复制；单击拉起 <b>AK 详情</b> 抽屉。</li><li>● 备注可自定义编辑，不超过20字符，若备注为空显示“-”。</li></ul> |
| 调用方式            | <ul style="list-style-type: none"><li>● API</li><li>● 控制台</li></ul>                                 | 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<br>cdb                                                                    | 调用的接口与接口所属服务。                                                                                                                                         |
| CAM 策略用户（角色）/策略 | 1<br>用户：xxx<br>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。<br>临时密钥由于聚合展示,所以展示用户（角色）。                                                                                        |
| 调用状态/次数         | <ul style="list-style-type: none"><li>● 成功（x次）</li><li>● 失败（x次）</li></ul>                           | 调用该 AK 成功/失败状态及次数。                                                                                                                                    |
| 首次/最近调用时间       | <ul style="list-style-type: none"><li>● 2025-01-01 18:00:00</li><li>● 2025-01-12 18:00:00</li></ul> | 首次与最近调用时间。 <ul style="list-style-type: none"><li>● 格式：YYYY-MM-DD HH:MM:SS。</li><li>● 支持排序。</li></ul>                                                  |
| IP 所属资产（ID/名称）  | ins-xxx<br>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**。

异常调用记录

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

Q

📄

| 调用源IP/地域/备注                                                                                        | IP类型 ⓘ   | 调用方式 | 调用接口/服务                       | CAM策略 | 操作                 |
|----------------------------------------------------------------------------------------------------|----------|------|-------------------------------|-------|--------------------|
|  中国-广东省-广州市   - | 账号外（未备注） | API  | ModifyBruteAttackRules<br>cwp | 1     | 详情 更多 ▾            |
|  中国-广东省-广州市   - | 账号外（未备注） | API  | ModifyBruteAttackRules<br>cwp | 1     | 添加白名单策略<br>管理白名单策略 |

● 详情

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



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

调用记录详情

```
17    vpcId: "0",
18    sigMethod: "[REDACTED]",
19    name: "",
20    action: "Describe",
21    uin: "[REDACTED]",
22    reqHost: "cdb.[REDACTED]",
23    region: "none"
```

CAM策略详情

```
1  {
2      statement: [
3          {
4              action: "*",
5              effect: "allow",
6              resource: "*"
7          },
8      ],
9      version: "2.0"
10 }
```

复制

|                            |      |              |
|----------------------------|------|--------------|
| QCloudFinanceFullAccess    | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataFullAccess     | 预设策略 | 策略详情 前往CAM查看 |
| QcloudWeDataReadOnlyAccess | 预设策略 | 策略详情 前往CAM查看 |

- 更多

- 添加白名单策略：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：2025-09-17 21:29:00

## 风险项视角

### 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 > 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。

资产列表

账号列表

告警

配置风险

风险项视角

资产视角

最新检测

近7天

多个关键字用竖线“|”分隔，多个过滤标适用回车键分隔

| <input type="checkbox"/> | 风险名称                      | 风险等级 | 受影响账号 | 最近检出时间 | 操作      |
|--------------------------|---------------------------|------|-------|--------|---------|
| <input type="checkbox"/> | 不应该拥有高权限预设策略              | 严重   | 11    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对访问管理(CAM)的操作权限进行收敛     | 高危   | 11    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对集团账号管理的操作权限进行收敛        | 高危   | 10    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对云服务器(CVM)的操作权限进行收敛     | 高危   | 10    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对腾讯云自动化助手(TAT)的操作权限进行收敛 | 高危   | 10    |        | 详情 重新检测 |
| <input type="checkbox"/> | 存在超过90天未使用的已启用密钥          | 高危   | 8     |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对容器安全服务(TCSS)的操作权限进行收敛  | 中危   | 10    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对容器服务的操作权限进行收敛          | 中危   | 10    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对对象存储(COS)的操作权限进行收敛     | 中危   | 10    |        | 详情 重新检测 |
| <input type="checkbox"/> | 应该对云数据库(MySQL)的操作权限进行收敛   | 中危   | 10    |        | 详情 重新检测 |

共 13 项

10 条 / 页

1

/ 2 页

咨询

动态

文档

反馈

| 字段名    | 示例                                                                           | 说明                                          |
|--------|------------------------------------------------------------------------------|---------------------------------------------|
| 风险名称   | 不应该拥有高权限预设策略                                                                 | 单击拉起风险项详情抽屉。                                |
| 风险等级   | <div><div>严重</div><div>高危</div><div>中危</div><div>低危</div><div>提示</div></div> | 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。<br>格式：YYYY-MM-DD HH:MM:SS。<br>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   | 单击拉起风险项详情抽屉，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。

风险项详情

重新检测

收起建议

1 检查账号是否有需要治理的配置风险

根据风险内容检查是否有高权限的预设策略、长期未使用AK或拥有某服务的相关敏感接口权限。  
(当前页面未包含COS的调用记录，COS的调用记录可根据最后访问时间和COS开通的CLS日志进行判断)

2 收敛权限策略或禁用/删除api 密钥

收敛权限

同步使用该api 密钥的相关业务方后，在权限策略中移除与接口相关的权限。[查看示意](#)

若存在某服务的相关敏感接口权限，检查相关接口调用情况，无调用则为冗余配置，可根据实际需要考虑收敛。[查看示意](#)

禁用/删除

登录 访问管理 管理控制台，并进入 访问密钥-API密钥管理 /用户列表-API密钥。[前往登录](#)

确保api 密钥最近访问时间一段时间没有更新后，禁用对应的 api 密钥。

保留禁用的api 密钥一段时间（紧急情况下可以恢复密钥），根据情况选择是否删除AK。

其他使用建议详见 [云API密钥安全使用方案](#)

受影响账号

重新检测

更多

近7天

处理状态: 未处理

Q

↓

| <input type="checkbox"/> | 账号名称/身份                                           | 账号保护                 | 风险检出时间 | 处理状态 | 操作      |
|--------------------------|---------------------------------------------------|----------------------|--------|------|---------|
| <input type="checkbox"/> | <div><div></div><div>子账号（所属主账号：主账号 B）</div></div> | 登录保护：未开启<br>操作保护：未开启 |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> | <div><div></div><div>子账号（所属主账号：主账号 B）</div></div> | 登录保护：未开启<br>操作保护：未开启 |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> | <div><div></div><div>子账号（所属主账号：主账号 B）</div></div> | 登录保护：未开启<br>操作保护：未开启 |        | 未处理  | 风险详情 更多 |

| 字段名     | 示例                                                         | 说明                                                                                   |
|---------|------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 账号名称/身份 | <div><div>账号 A</div><div>主账号/子账号 (所属主账号：主账号 B)</div></div> | <div><div>AK 所属云厂商与账号，若为子账号展示所属主账号信息。</div><div>鼠标悬浮查看账号名称、账号 ID与 APPID。</div></div> |
| 账号保护    | <div><div>登录保护：开启</div><div>操作保护：开启</div></div>            | <div><div>展示账号的登录保护与操作保护等安全状态的开启情况。</div><div>支持筛选全部开启/部分开启/未开启。</div></div>         |
| 风险检出时间  | 2025-01-12 18:00:00                                        | <div><div>风险检出时间。</div><div>格式：YYYY-MM-DD HH:MM:SS。</div><div>支持排序。</div></div>      |

©2013-2026 腾讯云版权所有

第134 共160页

|      |                                                                               |                           |
|------|-------------------------------------------------------------------------------|---------------------------|
| 处理状态 | <div><div></div>未处理</div> <div><div></div>已收敛</div> <div><div></div>已忽略</div> | 展示风险处理状态，手动完成标记，处理状态支持筛选。 |
|------|-------------------------------------------------------------------------------|---------------------------|

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。

受影响账号

重新检测

更多

近7天

处理状态: 未处理

账号名称/身份

账号保护

风险检出时间

处理状态

操作

子账号 (所属主账号: )

登录保护: 未开启

操作保护: 未开启

未处理

风险详情 更多

子账号 (所属主账号: )

登录保护: 未开启

操作保护: 未开启

未处理

重新检测

标记忽略

API密钥管理

子账号 (所属主账号: )

登录保护: 未开启

操作保护: 未开启

未处理

风险详情 更多

| 操作类型 |          | 说明                           |
|------|----------|------------------------------|
| 风险详情 |          | 单击拉起风险详情抽屉，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。

受影响账号

重新检测

更多

近7天

处理状态: 未处理

账号名称/身份

账号保护

风险检出时间

处理状态

操作

子账号 (所属主账号: )

登录保护: 未开启

操作保护: 未开启

未处理

风险详情 更多

子账号 (所属主账号: )

登录保护: 未开启

操作保护: 未开启

未处理

风险详情 更多

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。

风险详情

未处理

重新检测

更多

×

应该对访问管理(CAM)的操作权限进行收敛

配置风险

风险等级

高危

风险检出时间

2025-09-02 18:09:37

所属账号

账号身份

子账号 (所属主账号: )

访问方式

控制台与API

账号保护

登录保护: 未开启

操作保护: 未开启

相关CAM策略

5

关联账号告警

0

相关AK与关联告警

0

- 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。

风险证据&描述

风险描述

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

证据

共1个

| 策略名称 | 操作 | 资源 | 请求条件 |
|------|----|----|------|
|      |    | 全部 | 无    |

- 查看风险相关接口调用情况以及配置建议。

账号权限策略配置建议

收起建议 ▲

1

检查账号是否有需要治理的配置风险

- 根据风险内容检查是否有高权限的预设策略、长期未使用AK或拥有某服务的相关敏感接口权限。  
(当前页面未包含COS的调用记录，COS的调用记录可根据最后访问时间和COS开通的CLS日志进行判断)

2

收敛权限策略或禁用/删除api 密钥

收敛权限

- 同步使用该api 密钥的相关业务方后，在权限策略中移除与接口相关的权限。[查看示意](#)
- 若存在某服务的相关敏感接口权限，检查相关接口调用情况，无调用则为冗余配置，可根据实际需要考虑收敛。[查看示意](#)

禁用/删除

- 登录 访问管理 管理控制台，并进入 访问密钥-API密钥管理 /用户列表-API密钥。[前往登录](#)
- 确保api 密钥最近访问时间一段时间没有更新后，禁用对应的 api 密钥。
- 保留禁用的api 密钥一段时间（紧急情况下可以恢复密钥），根据情况选择是否删除AK。

其他使用建议详见 [云API密钥安全使用方案](#)

风险相关接口调用情况

① 当前的AK调用记录 不包含COS、TDMQ等操作日志，在禁用/删除AK时，建议通过最近访问时间来判断AK是否在被业务调用

近7天

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

Q

↓

| 接口名称                                            | 所属服务      | 调用次数 |
|-------------------------------------------------|-----------|------|
| CreateCollApiKey ①<br>通过云API创建密钥，常见的攻击路径，需要注意风险 | 访问管理（cam） | 0    |

共 1 项

10 条 / 页

1

/ 1 页

| 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。

©2013-2026 腾讯云版权所有

第137 共160页

资产列表账号列表告警配置风险

风险项视角资产视角最新检测更多

近7天处理状态: 未处理

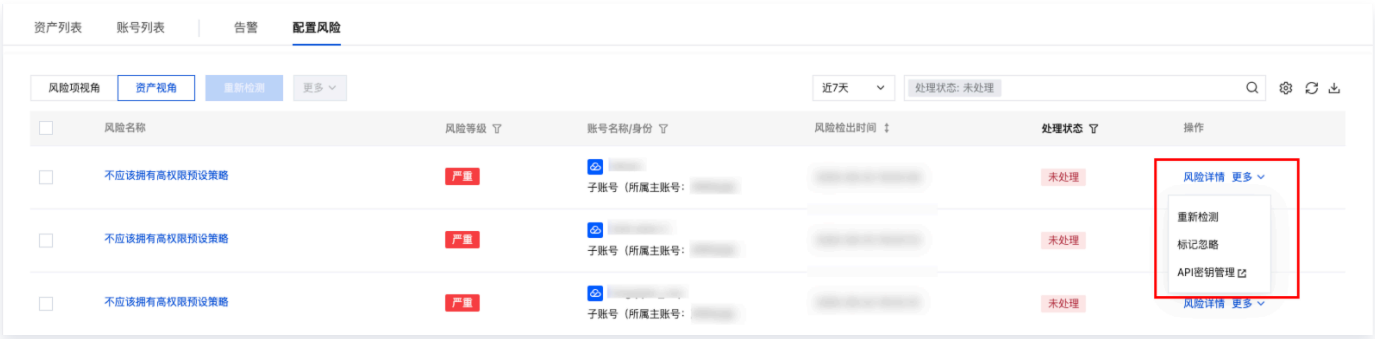
| 风险名称                                  | 风险等级 | 账号名称/身份                                                                                         | 风险检出时间 | 处理状态 | 操作      |
|---------------------------------------|------|-------------------------------------------------------------------------------------------------|--------|------|---------|
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |
| <input type="checkbox"/> 不应该拥有高权限预设策略 | 严重   |  子账号 (所属主账号: ) |        | 未处理  | 风险详情 更多 |

共 130 项10 条 / 页1 / 13 页

查询动态文档反馈

| 字段名     | 示例                                                                           | 说明                                                                                           |
|---------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 风险名称    | 不应该拥有高权限预设策略                                                                 | 单击拉起风险详情抽屉。                                                                                  |
| 风险等级    | <div><div>严重</div><div>高危</div><div>中危</div><div>低危</div><div>提示</div></div> | 基于腾讯云安全实践评定风险等级。                                                                             |
| 账号名称/身份 | <div><div>账号 A</div><div>主账号/子账号（所属主账号：主账号 B）</div></div>                    | <div><div>AK 所属云厂商与账号，若为子账号展示所属主账号信息。</div><div>鼠标悬浮查看账号 ID 与 APPID；支持筛选主账号/子账号。</div></div> |
| 风险检出时间  | 2025-01-12 18:00:00                                                          | <div><div>风险检出时间。</div><div>格式：YYYY-MM-DD HH:MM:SS。</div><div>支持排序。</div></div>              |
| 处理状态    | <div><div>未处理</div><div>已收敛</div><div>已忽略</div></div>                        | 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 |          | 单击拉起 <b>风险详情</b> 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。

风险详情

未处理

重新检测

更多

X

应该对访问管理(CAM)的操作权限进行收敛

配置风险

风险等级

高危

风险检出时间

2025-09-02 18:09:37

所属账号

子账号 (所属主账号: )

访问方式

控制台与API

账号保护

登录保护: 未开启

操作保护: 未开启

相关CAM策略

5

关联账号告警

0

相关AK与关联告警

0

- 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。

风险证据&描述

风险描述

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

证据

共1个

| 策略名称 | 操作 | 资源 | 请求条件 |
|------|----|----|------|
|      |    | 全部 | 无    |

- 查看风险相关接口调用情况以及配置建议。



账号权限策略配置建议

收起建议 ▲

1 检查账号是否有需要治理的配置风险

- 根据风险内容检查是否有高权限的预设策略、长期未使用AK或拥有某服务的相关敏感接口权限。  
(当前页面未包含COS的调用记录, COS的调用记录可根据最后访问时间和COS开通的CLS日志进行判断)

2 收敛权限策略或禁用/删除api 密钥

收敛权限

- 同步使用该api 密钥的相关业务方后, 在权限策略中移除与接口相关的权限。[查看示意](#)
- 若存在某服务的相关敏感接口权限, 检查相关接口调用情况, 无调用则为冗余配置, 可根据实际需要考虑收敛。[查看示意](#)

禁用/删除

- 登录 访问管理 管理控制台, 并进入 访问密钥-API密钥管理 /用户列表-API密钥。[前往登录](#)
- 确保api 密钥最近访问时间一段时间没有更新后, 禁用对应的 api 密钥。
- 保留禁用的api 密钥一段时间 (紧急情况下可以恢复密钥), 根据情况选择是否删除AK。

其他使用建议详见 [云API密钥安全使用方案](#)

风险相关接口调用情况

① 当前的AK调用记录 不包含COS、TDMQ等操作日志 , 在禁用/删除AK时, 建议通过最近访问时间来判断AK是否在被业务调用

近7天

多个关键字用竖线 "|" 分隔, 多个过滤标签用回车键分隔

Q

↓

| 接口名称                                              | 所属服务       | 调用次数 |
|---------------------------------------------------|------------|------|
| CreateCollApiKey ①<br>通过云API创建密钥, 常见的攻击路径, 需要注意风险 | 访问管理 (cam) | 0    |

共 1 项

10 条 / 页

1

/ 1 页

| 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, |

©2013-2026 腾讯云版权所有

第141 共160页

|                              |                                                                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | CreateSecurityGroup, CreateSecurityGroupWithPolicies, CreateVpcEndPoint, CreateVpcPeeringConnection                                                                               |
| 应该对向量数据库的操作权限进行收敛            | 应该向量数据库的操作权限进行收敛，不应拥有如下敏感接口权限：ModifyAccessKey                                                                                                                                     |
| 应该对容器服务的操作权限进行收敛             | 应该容器服务的操作权限进行收敛，不应拥有如下敏感接口权限：CreateClusterEndpoint, DeleteEKSCluster, DeleteEKSClusterInstances, DescribeClusterKubeconfig, DescribeClusterSecurity, DescribeEKSClusterCredential |
| 应该对高性能计算平台的操作权限进行收敛          | 应该高性能计算平台的操作权限进行收敛，不应拥有如下敏感接口权限：ModifyInitNodeScripts                                                                                                                             |
| 应该对云开发服务的操作权限进行收敛            | 应该对云开发服务的操作权限进行收敛，不应拥有如下敏感接口权限：CreateCloudUser, DescribeEnvs                                                                                                                      |
| 应该对腾讯云自动化助手的操作权限进行收敛         | 应该对腾讯云自动化助手的操作权限进行收敛，不应拥有如下敏感接口权限：CreateCommand, CreateInvoker, EnableInvoker, InvokeCommand, RunCommand                                                                          |
| 应该对安全凭证服务的操作权限进行收敛           | 应该对安全凭证服务的操作权限进行收敛，不应拥有如下敏感接口权限：AssumeRole, GetFederationToken                                                                                                                    |
| 应该对云函数的操作权限进行收敛              | 应该对云函数的操作权限进行收敛，不应拥有如下敏感接口权限：CreateFunction, Invoke                                                                                                                               |
| 应该对云数据库(Redis)的操作权限进行收敛      | 应该对云数据库(Redis)的操作权限进行收敛，不应拥有如下敏感接口权限：ClearInstance, KillMasterGroup, ModifyInstanceAccount, ResetPassword                                                                         |
| 应该对云数据库(PostgreSQL)的操作权限进行收敛 | 应该对云数据库(PostgreSQL)的操作权限进行收敛，不应拥有如下敏感接口权限：ResetAccountPassword                                                                                                                    |
| 应该对集团账号管理的操作权限进行收敛           | 应该对集团账号管理的操作权限进行收敛，不应拥有如下敏感接口权限：AddUserToGroup, CreateUserSyncProvisioning                                                                                                        |
| 应该对轻量应用服务器的操作权限进行收敛          | 应该对轻量应用服务器的操作权限进行收敛，不应拥有如下敏感接口权限：CreateKeyPair, ImportKeyPair, ResetInstancesPassword                                                                                             |
| 应该对域名注册的操作权限进行收敛             | 应该对域名注册的操作权限进行收敛，不应拥有如下敏感接口权限：CreateDomainBatch, RegisterDomain, RenewAgentPay                                                                                                    |
| 应该对云解析(DNS)的操作权限进行收敛         | 应该对云解析(DNS)的操作权限进行收敛，不应拥有如下敏感接口权限：CreateDomainBatch, CreateShareDomains                                                                                                           |
| 应该对容器安全服务(TCSS)的操作权限进行收敛     | 应该对容器安全服务(TCSS)的操作权限进行收敛，不应拥有如下敏感接口权限：DeleteMachine                                                                                                                               |

|                              |                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 应该对主机安全(CWP)的操作权限进行收敛        | 应该对主机安全(CWP)的操作权限进行收敛，不应拥有如下敏感接口权限：DeleteMachine                                                                                                                                                                                                                                                                                                                                |
| 应该对操作审计(CloudAudit)的操作权限进行收敛 | 应该对操作审计(CloudAudit)的操作权限进行收敛，不应拥有如下敏感接口权限：DeleteAudit, DeleteAuditTrack                                                                                                                                                                                                                                                                                                         |
| 应该对云数据库(MySQL)的操作权限进行收敛      | 应该对云数据库(MySQL)的操作权限进行收敛，不应拥有如下敏感接口权限：CloseWanService, CreateAccounts, CreateRoInstancecp, 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, AddUsererr, UpdateUser                                                                                                                     |
| 应该删除长期未使用AK密钥                | 应该删除长期未使用AK密钥，即使AK被禁用了也应该删除                                                                                                                                                                                                                                                                                                                                                     |
| 不应该拥有高权限预设策略                 | AK不应该有AdministratorAccess、QCloudResourceFullAccess、QCloudCAMFullAccess、QCloudFinanceFullAccess高权限预设策略                                                                                                                                                                                                                                                                           |

# 策略管理

最近更新时间：2025-09-17 21:28:59

## 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。

策略管理

多账号管理

告警策略

白名单策略

IP隐藏策略

添加策略

删除

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

|                          | 策略名称/类型          | 策略来源  | 策略内容                                  | 关联账号 | 开关                               |
|--------------------------|------------------|-------|---------------------------------------|------|----------------------------------|
| <input type="checkbox"/> | 存在新的IP调用API异常行为  | 系统策略  | 该IP在过去3个月内未曾调用过API，需要确认下是否为...        | 12   | <div><div></div>已开启: 10/12</div> |
| <input type="checkbox"/> | 存在新的IP调用高危接口异常行为 | 系统策略  | 该IP在过去3个月内未曾调用过API，首次调用了高危接...        | 12   | <div><div></div>已开启: 12/12</div> |
| <input type="checkbox"/> | github密钥确认请求泄露监测 | 系统策略  | 该请求源IP来自于GitGuardian(github官方密钥泄露判... | 12   | <div><div></div>已开启: 12/12</div> |
| <input type="checkbox"/> | 内网异常调用异常行为       | 系统策略  | 存在局域网或者腾讯云内网跨vpc调用，该调用对应vpc...        | 12   | <div><div></div>已开启: 11/12</div> |
| <input type="checkbox"/> |                  | 自定义策略 |                                       | 1    | <div><div></div>已开启: 1/1</div>   |
| <input type="checkbox"/> |                  | 自定义策略 |                                       | 1    | <div><div></div>已开启: 1/1</div>   |
| <input type="checkbox"/> | 可疑列举服务器行为异常行为    | 系统策略  | 通过同一个密钥，短时间内多次列举服务器列表                 | 12   | <div><div></div>已开启: 12/12</div> |
| <input type="checkbox"/> | 可疑子用户存在调用异常行为    | 系统策略  | 可疑的子用户存在调用，这些用户的名称与部分AK利用...          | 12   | <div><div></div>已开启: 12/12</div> |
| <input type="checkbox"/> | 访问密钥存在泄露泄露监测     | 系统策略  | 该访问密钥已经泄露，存在严重风险，请及时禁用/更换...          | 12   | <div><div></div>已开启: 12/12</div> |
| <input type="checkbox"/> | 行云管家行为异常行为       | 系统策略  | 这部分调用来源于行云管家，需要关注                     | 12   | <div><div></div>已开启: 12/12</div> |

共 29 项

10 条 / 页

1

3 页

3. 单击添加策略，配置相关参数，单击保存。

← 添加告警策略

×

基本信息

1

填写告警策略基本信息

策略名称 \*

请输入规则名称，不超过20个字符

告警等级 \*

☒ 严重

☐ 高危

☐ 中危

☐ 低危

☐ 提示

生效账号 \*



▼

告警策略内容

策略生效预览

3

查看告警策略生效预览

当

全部源IP

使用

-

通过

全部调用方式

调用

全部接口

，返回码为

成功等2个返回码

时，产生告警。

2

填写告警策略内容

生效调用源IP

☐ 全部源IP

☐ 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）

☒ 自定义输入

IP示例：1.1.1.1；IP范围示例：1.1.1.1-1.1.1.10；IP段示例：172.168.34.1/24  
输入示例：  
1.1.1.1  
1.1.1.1-1.1.1.10  
172.168.34.1/24  
(多个IP/类型换行隔开，每行一个/一种)  
  
最多支持输入1000行，若输入重复IP，后台将自动合并

调用方式

☒ 全部调用方式

☐ 控制台

☐ API

生效AK

☐ 全部AK(25)

☐ 从现有AK中选择

☐ 长期密钥

☐ 临时密钥

☒ 自定义输入

请输入需要生效的AK，示例：  
AK1  
AK2  
(多个AK换行隔开，每行一个)  
  
最多支持输入 1000 行；若输入重复AK，后台将自动合并

生效接口

☒ 全部接口

☐ 自选接口

返回码

☒ 全部

☒ 成功☒ 失败

保存

取消

调用源IP

IPIPIP...

调用方式

AK

返回码

接口接口接口...

| 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<br>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<br>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。

策略管理

多账号管理

告警策略白名单策略IP隐藏策略

添加策略删除

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

| <input type="checkbox"/> | 策略名称 | 加白内容                   | 备注 | 更新时间                | 所属账号 | 操作    |
|--------------------------|------|------------------------|----|---------------------|------|-------|
| <input type="checkbox"/> |      | 生效策略<br>IP<br>AK<br>接口 | -  | 2025-07-17 21:47:28 |      | 编辑 删除 |
| <input type="checkbox"/> |      | 生效策略<br>IP<br>AK<br>接口 | -  | 2025-07-17 21:12:34 |      | 编辑 删除 |
| <input type="checkbox"/> |      | 生效策略<br>IP<br>AK<br>接口 | -  | 2025-07-17 10:16:06 |      | 编辑 删除 |
| <input type="checkbox"/> |      | 生效策略<br>IP<br>AK<br>接口 | -  | 2025-04-14 16:11:10 |      | 编辑 删除 |

共 4 项

10 条 / 页

1 / 1 页

3. 单击添加策略，配置相关参数，单击保存。

← 添加白名单策略

1 填写白名单策略基本信息

策略名称 \*  
请输入规则名称，不超过20个字符

备注  
请输入文本，不超过100个字符

生效范围 ☒ 修改历史告警的处理状态为“已忽略”

告警策略内容

策略生效预览 3 查看白名单策略生效预览

在 全部 策略中，当 全部源IP 使用 - 通过 全部调用方式 调用 全部接口，返回码为 成功等2个返回码 时，均不进行告警监测，且 存量告警的处理状态修改为“已忽略”。

2 填写白名单策略内容

生效策略  
请选择生效告警策略，若不选择则对全部策略生效

生效调用源IP

☐ 全部源IP

☐ 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）

☒ 自定义输入

IP示例：1.1.1.1；IP范围示例：1.1.1.1-1.1.1.10；IP段示例：172.168.34.1/24  
输入示例：  
1.1.1.1  
1.1.1.1-1.1.1.10  
172.168.34.1/24  
(多个IP/类型换行隔开，每行一个/一种)  
  
最多支持输入1000行，若输入重复IP，后台将自动合并

调用方式 ☒ 全部调用方式 ☐ 控制台 ☐ API

生效AK

☐ 全部AK(25) ☐ 从现有AK中选择 ☐ 长期密钥 ☐ 临时密钥 ☒ 自定义输入

请输入需要加白的AK，示例：  
AK1  
AK2  
(多个AK换行隔开，每行一个)  
  
最多支持输入 1000 行；若输入重复AK，后台将自动合并

生效接口 ☒ 全部接口 ☐ 自选接口

返回码

☒ 全部

☒ 成功 ☒ 失败

保存

取消

>> 隐藏说明

调用源IP

IP IP IP ...

调用方式

AK AK

返回码

调用接口

接口 接口 接口 ...

| 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<br>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<br>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。

策略管理

多账号管理

告警策略

白名单策略

**IP隐藏策略**

①

- 您可配置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。

添加策略

删除

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

| <input type="checkbox"/> | 策略名称 | 策略内容                        | 备注 | 更新时间 ↓              | 所属账号 | 操作                                    |
|--------------------------|------|-----------------------------|----|---------------------|------|---------------------------------------|
| <input type="checkbox"/> |      | <div>IP</div> <div>AK</div> | -  | 2025-08-14 10:54:02 |      | <a href="#">编辑</a> <a href="#">删除</a> |

共 1 项

10 条 / 页

1

/ 1 页

3. 单击添加策略，配置相关参数，单击保存。



← 添加IP隐藏策略

×

①

• 您可配置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。

基本信息

1

填写 IP 隐藏策略基本信息

策略名称 \*

请输入规则名称，不超过20个字符

备注

请输入文本，不超过100个字符

2

填写 IP 隐藏策略内容

生效调用源IP

☐ 全部源IP

☐ 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）

☒ 自定义输入

IP示例：1.1.1.1；IP范围示例：1.1.1.1-1.1.1.10；IP段示例：172.168.34.1/24

输入示例：

1.1.1.1

1.1.1.1-1.1.1.10

172.168.34.1/24

（多个IP/类型换行隔开，每行一个/一种）

最多支持输入1000行，若输入重复IP，后台将自动合并

生效AK

☐ 全部AK(25)

☐ 从现有AK中选择

☐ 长期密钥

☐ 临时密钥

☒ 自定义输入

请输入需要加白的AK，示例：

AK1

AK2

（多个AK换行隔开，每行一个）

最多支持输入 1000 行；若输入重复AK，后台将自动合并

保存

取消

| 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<br>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<br>AK2            |

# 用户行为分析（UEBA）

最近更新时间：2024-08-02 10:14:18

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。

## 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](#)，在左侧导航中，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。

### ① 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。

自定义用户

日志类型

选择一个日志类型

还没有接入日志，前往 [接入日志](#)

用户ID

选择一个代表用户ID的字段

用户名称

选择一个代表用户名称的字段（可不选）

操作对象 ?

请选择

操作方式 ?

请选择

确定

取消

| 参数名称  | 说明                                                                                                                                                                                                                             |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 日志类型  | 在完成 <a href="#">配置日志接入</a> 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。<br>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。<br>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**。

行为概况



暂无行为数据，请先接入云审计日志

云安全中心还没有接入云审计日志，无法提供用户行为概览数据，请前往日志分析页面完成云审计日志接入，或 [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。

**① 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。

接入日志源



日志来源

自定义日志来源

日志来源名称

请输入日志来源名称

存储时长

7天

30天

60天

90天

180天

接入方式

通过自有COS桶接入

COS存储桶

请选择需要接入的COS存储桶



将需要接入的日志写入选择的COS存储桶，并配置权限为允许云安全中心服务角色读取，云安全中心会自动定时读取日志文件，你也可以选择 [提交工单](#) 定制读取方式或 [前往创建一个新的存储桶](#)

存储目录

请选择文件存储目录

请选择压缩格式

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

请输入目标解析文件的其他字段信息

样例解析

我们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

请先输入日志样例

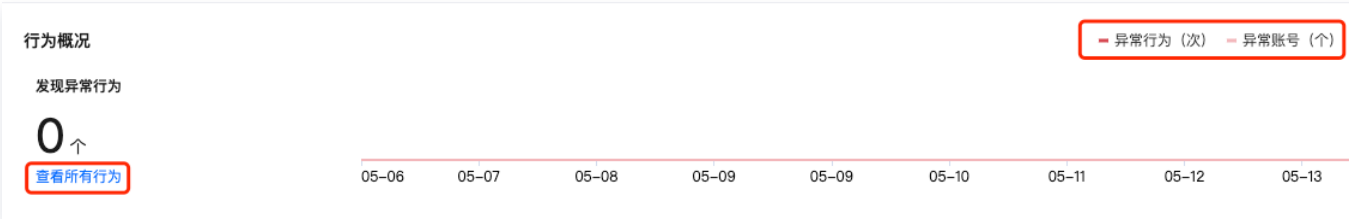
请选择时间戳格式

确定

取消

| 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 <a href="#">提交工单</a> 来定制读取方式，或前往 COS 产品页面创建一个新的存储桶。 |
|         | 存储目录    | 为提升读取性能，建议在选定的目录下，进一步按照 yyyy/mm/dd 的格式组织日志文件路径，我们会根据日历自动读取对应自然日的文件；日志格式支持 J 格式，用‘/n’分割行，支持 gzip 压缩。                    |
|         | 日志样例    | 建议您输入日志样例供系统参考。系统会根据输入的样例进行字段解析，您可以进一步查看并选择指定字段及排序操作，这将提升日志的读取性能及解析的正确性。                                               |
|         | 时间戳     | 选择日志样例及其对应的时间戳格式。                                                                                                      |

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



查看策略

1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**用户行为分析（UEBA）**。

2. 在用户行为分析（UEBA）列表中，提供系统策略来检测异常行为和异常账号，可针对 AKSK 异常调用、高危接口调用、用户高危操作、未授权服务使用、权限提升等风险行为进行检测告警。

添加策略

删除策略

多个关键字用竖线"|"分隔，多个过滤标签用回车键分隔

Q

🔄

| <input type="checkbox"/> | 策略ID/名称        | 策略类型 ▾ | 告警等级 ▾ | 策略内容                                    | 开关 ▾                                | 命中次数 | 操作    |
|--------------------------|----------------|--------|--------|-----------------------------------------|-------------------------------------|------|-------|
| <input type="checkbox"/> | 可疑IP调用高危接口     | 系统策略   | 严重     | 过去6个月未曾出现过的IP，调用了高危接口                   | <input checked="" type="checkbox"/> | 0次   | 编辑 删除 |
| <input type="checkbox"/> | root账号进行aksk调用 | 系统策略   | 高危     | 根账号使用aksk进行接口调用                         | <input checked="" type="checkbox"/> | 0次   | 编辑 删除 |
| <input type="checkbox"/> | 长期未使用aksk突发调用  | 系统策略   | 高危     | 长期未使用指一个月内未曾出现过的aksk                    | <input checked="" type="checkbox"/> | 0次   | 编辑 删除 |
| <input type="checkbox"/> | 新用户高危操作        | 系统策略   | 高危     | 新用户指创建时间在最近一天内的用户，高危操作指调用敏感/存在安全隐患的接口列表 | <input checked="" type="checkbox"/> | 0次   | 编辑 删除 |
| <input type="checkbox"/> | 非常用接口突发高频调用    | 系统策略   | 中危     | 指在单位时间内某接口调用次数较高，但是其在过去七天内调用较少          | <input checked="" type="checkbox"/> | 0次   | 编辑 删除 |

| 参数名称  | 说明                                              |
|-------|-------------------------------------------------|
| 策略 ID | 系统默认生成。                                         |
| 策略名称  | 系统策略由产品后台定义；用户自定义策略由用户定义。                       |
| 策略类型  | 包括系统策略和自定义策略。                                   |
| 告警等级  | 包括严重、高危、中危、低危和提示。                               |
| 策略内容  | 解释策略的检测内容。                                      |
| 开关    | 用户可自定义开启或关闭此条策略。                                |
| 命中次数  | 统计近7天的策略命中纪录。单击可跳转告警中心查看告警详情，告警来源为用户行为分析（UEBA）。 |
| 操作    | 系统策略不允许编辑和删除。用户自定义策略可编辑或删除策略。                   |

## 添加策略

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

自定义策略

×

策略名称

请输入策略名，不超过20个字符

用户类型

选择用户类型

选择该类型对应的日志类型

发生时间

☒ 每10分钟 ☐ 每小时 ☐ 每天 ☐ 每周 ☐ 每月

发生事件

☒ 语句检索 ☐ 过滤检索

请输入检索语句，支持SQL语句

告警名称

选择告警名称

告警等级

☒ 严重 ☐ 高危 ☐ 中危 ☐ 低危 ☐ 提示

操作者 ⓘ

请选择

操作对象 ⓘ

请选择

操作方式 ⓘ

请选择

| 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。 <ul style="list-style-type: none"><li>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。</li><li>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。</li></ul> |
| 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                                                                                               |



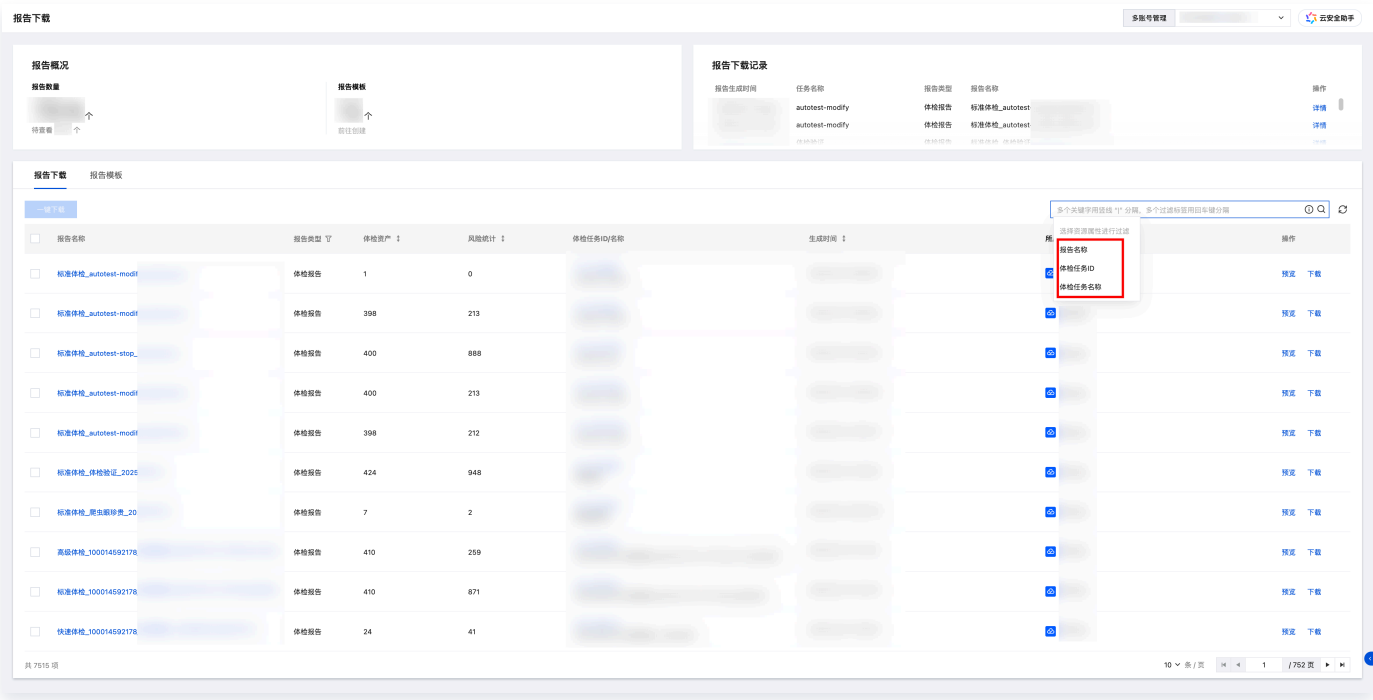
|      |                                                        |
|------|--------------------------------------------------------|
|      | 品、资源、实例、接口等信息，允许为空。                                    |
| 操作方式 | 请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的方式，建议选择密钥、AKSK 等信息，允许为空。 |

# 报告下载

最近更新时间：2025-09-17 21:48:26

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。

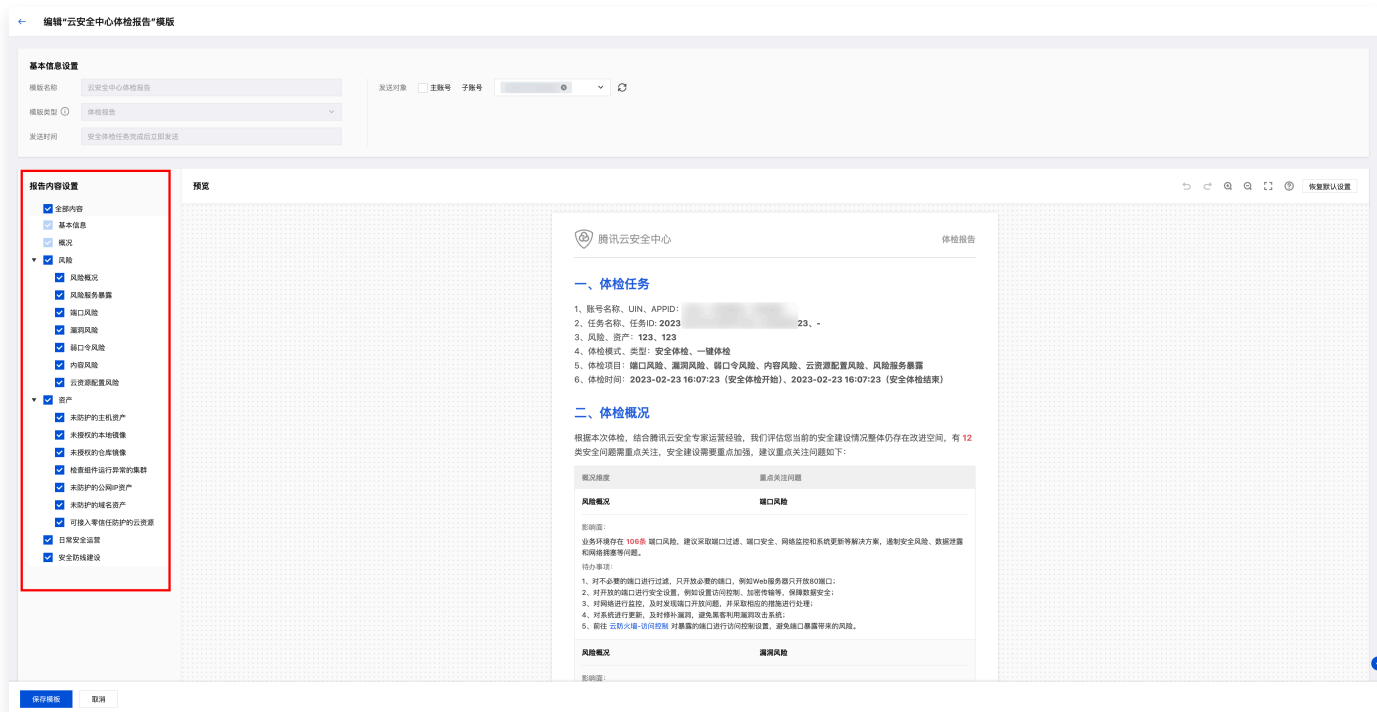
1. 登录 [云安全中心控制台](#)，在左侧导览中，单击**报告下载**。
2. 在报告下载页面，您可以根据体检任务筛选报告。支持通过**体检任务 ID** 或 **体检任务名称**进行模糊搜索，快速定位目标报告。



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。

