云安全中心

目录

产品介绍 6
产品定义 6
产品优势 7
安全数据全面采集 7
安全威胁深度检测 7
安全态势集中监测 7
安全告警快速处置 7
功能特性 7
云态势感知 7
风险管理 7
威胁运营 8
编排响应 8
应用场景 8
场景一：云上合规风险治理 8
方案优势 8
场景示意图 9
场景二：安全事件自动化运营 10
方案优势 10
场景示意图 11
场景三：安全态势可视化 11
方案优势 11
场景示意图 12
产品规格 13
云安全中心规格说明 13
计费说明 14
计费模式 14
标准资费 14
扩展资源规格说明 14
升级扩容 14
前提条件 15
规格限制 15
约束条件 15
系统影响 15
购买扩展资源 15
续订 16
到期说明 16
续订说明 16
手动续订 16
自动续订 17
退订 17
退订说明 18
操作步骤 18
查看账单 19
账单说明 19
操作步骤 19

快速入门 22
使用流程 22
购买云安全中心实例 24
前提条件 24
规格限制 24
约束条件 24
适用场景 24
操作步骤 24
接入日志、告警 26
前提条件 26
操作步骤 26
查看安全概览 27
前提条件 28
操作步骤 28
日志、告警外发设置 28
为日志类型添加转发目标 28
配置转发目标 30
用户指南 31
安全态势 31
安全概览 31
综合安全态势 33
安全成果展示 34
威胁攻击态势 35
资产中心 37
资产概览 37
资产管理 39
风险管理 41
云安全态势管理 41
漏洞管理 45
弱口令管理 49
威胁运营 51
告警概览 51
AI智能分析告警 51
告警管理 53
通知管理 57
威胁检测 64
安全体检 67
使用安全体检 67
编排响应 68
剧本管理 68
规则配置 69
报表中心 70
报表任务 70
报表模板 72
设置 73
集成配置 73
数据源监控 76
规则标签配置 77

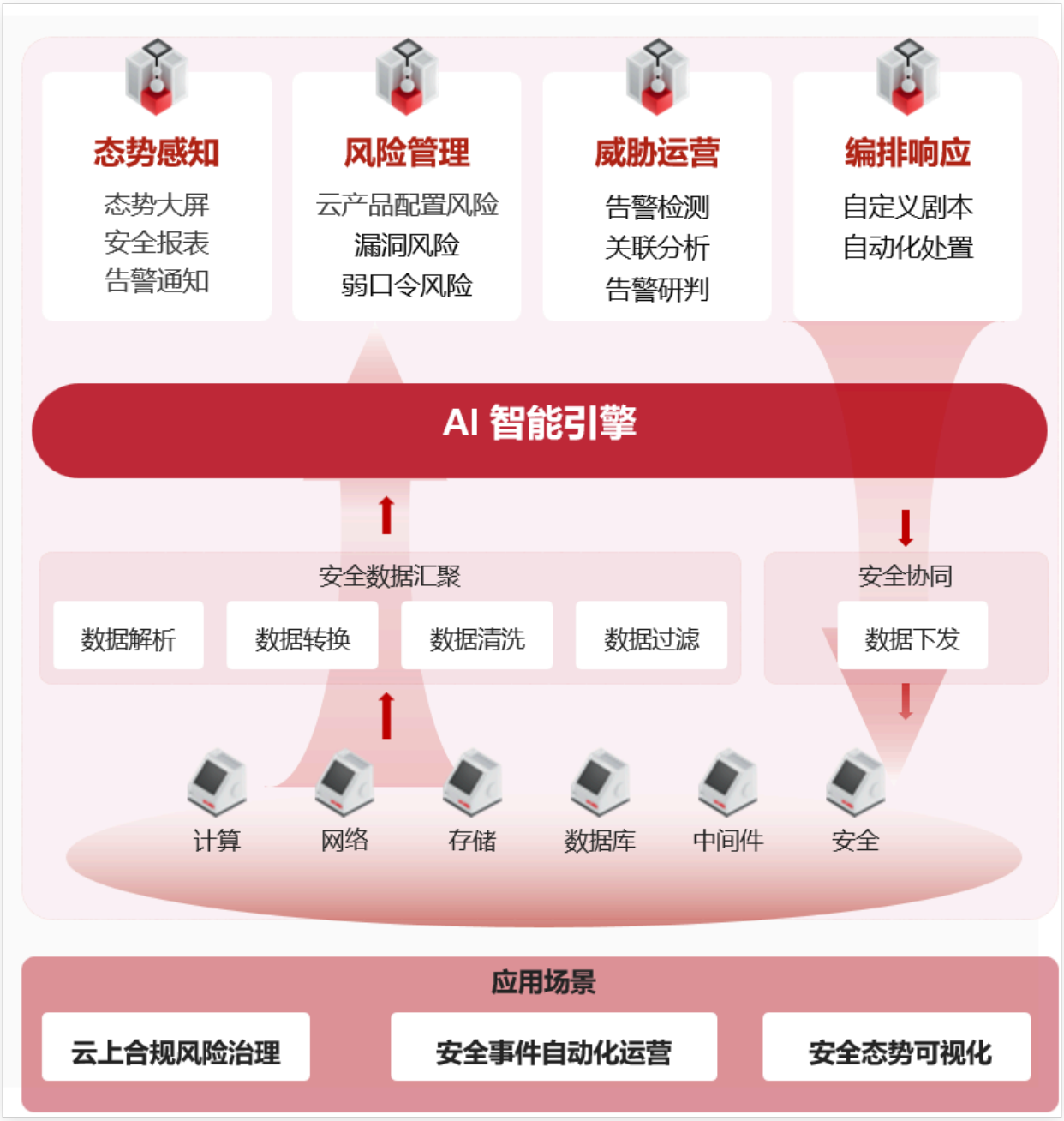
查看审计事件.....80
支持审计的操作列表.....80
查看云审计事件.....81
最佳实践.....83
如何进行剧本管理.....83
新建剧本.....83
新增剧本节点.....84
新增脚本任务节点.....86
剧本线条设置.....88
如何进行漏洞管理.....89
如何对资产进行查看管理.....92
如何进行威胁建模.....97
等级保护测评解读.....99
如何接入产品日志.....102
基于云安全中心进行风险治理.....104
应用场景.....104
典型案例.....104
操作步骤.....104
云资产统一纳管与全景盘点.....104
合规基线策略配置与批量检测.....105
风险分级核查与闭环处置.....105
整改验证与常态化运营.....106
常见问题.....108
产品咨询类.....108
云安全中心是否只是对其他云安全产品日志进行采集分析?.....108
云安全中心如何帮助客户满足等保合规要求?.....108
云安全中心支持采集云上哪些安全日志?.....108
短信使用余量是否会进行提醒?.....108
云安全中心没有收到告警，可能的原因是什么?.....108
计费购买类.....109
同一个账号可以购买多个云安全中心实例吗?.....109
云安全中心实例到期后，数据还会保留吗?.....109
云安全中心实例可以降低规格吗?.....109
云安全中心是否支持自动续订?.....109
云安全中心存在规格差异吗?.....109
云安全中心有哪些扩展服务可以购买?.....109
续费时是否可同时变更云安全中心版本或规格?.....110
扩展资源购买上限是什么?.....110
云安全中心是否支持按需计费?.....110
云安全中心有促销折扣吗?.....110
在使用期间购买了扩展资源，资源到期时间是何时?.....110
购买的扩展资源，支持单独退订吗?.....110
退订重购后，原实例的配置数据可以保留吗?.....110
如何选择日志分析量扩展资源?.....110
日志分析量扩展资源会过期吗?.....110
如何查看当前购买产品的产品规格?.....111
配置类.....111
数据接入相关.....111

告警通知相关.....112

产品介绍

产品定义

天翼云统一安全运营平台，联动协同云原生自研产品提供具备云安全态势管理（CSPM）、安全信息与事件管理（SIEM），安全编排与自动响应（SOAR）能力的一体化AI智能安全运营平台。



云安全中心系统主要包含态势感知、风险管理、威胁运营以及编排响应四大模块。

- 态势感知：全方位捕捉云上威胁，多维度实时可视化呈现安全态势。
- 风险管理：云环境风险集中管控，实现 “识别 - 评估 - 处置” 闭环管理。
- 威胁运营：依托 AI 智能体，精准检测未知威胁，提升研判效率。
- 编排响应：安全编排，自动响应。

产品优势

云安全中心作为用户侧的安全中心，产品优势如下：

安全数据全面采集

进行内部（资产、脆弱性、云产品配置）、外部（告警日志）以及云端威胁情报接入等相关安全数据的全面采集，汇聚、分析。

安全威胁深度检测

对多源安全告警进行关联分析、规则分析、情报分析等，发现潜伏的高级持续性威胁，提升告警检出率和准确率。

安全态势集中监测

从多安全告警、攻击方向、攻击趋势、影响范围等多维度多视角进行态势呈现。

安全告警快速处置

对接联动云安全防护产品，实现安全编排。在安全告警发生时自动下发阻断策略，并在必要时下发通知预警，及时完成安全闭环。

功能特性

云态势感知

全方位捕捉云上威胁，多维度实时可视化呈现安全态势。

风险管理

云环境风险集中管控，实现 “识别 - 评估 - 处置” 闭环管理。

威胁运营

依托 AI 智能体，精准检测未知威胁，提升研判效率。

编排响应

一键对接云上安全能力，应对安全事件实现安全编排，自动化响应。

应用场景

场景一：云上合规风险治理

深度适配国家网络安全等级保护（等保 2.0）、ISO 27001/27017/27018、金融JR/T 0071-2020 等国家及行业合规标准，覆盖政务、金融、工业、医疗等多领域监管要求。助力企业明确安全目标与主体责任，系统化构建符合监管规范的信息系统安全体系，有效收敛安全漏洞、降低 AI 自动化攻击与勒索云化等新型威胁风险，通过合规能力可视化呈现，向客户及利益相关方传递坚实安全承诺，强化合作信任与市场竞争力。

方案优势

- 全域数据智析：汇聚多维度安全数据，AI 引擎深度挖掘，精准定位合规短板。
- 多云统一管控：云上资产统管，全链路合规状态可视、可管、可控。
- 闭环合规服务：弹性订阅套餐，覆盖 “事前加固 - 事中拦截- 事后溯源 “。

场景示意图


安全运营人员
定期/自定义扫描
云服务配置基线
身份认证
访问控制
日志审计
系统漏洞
数据安全
访问控制
日志审计
系统漏洞
修复指导
检测失败
检测正常
云安全态势

场景二：安全事件自动化运营

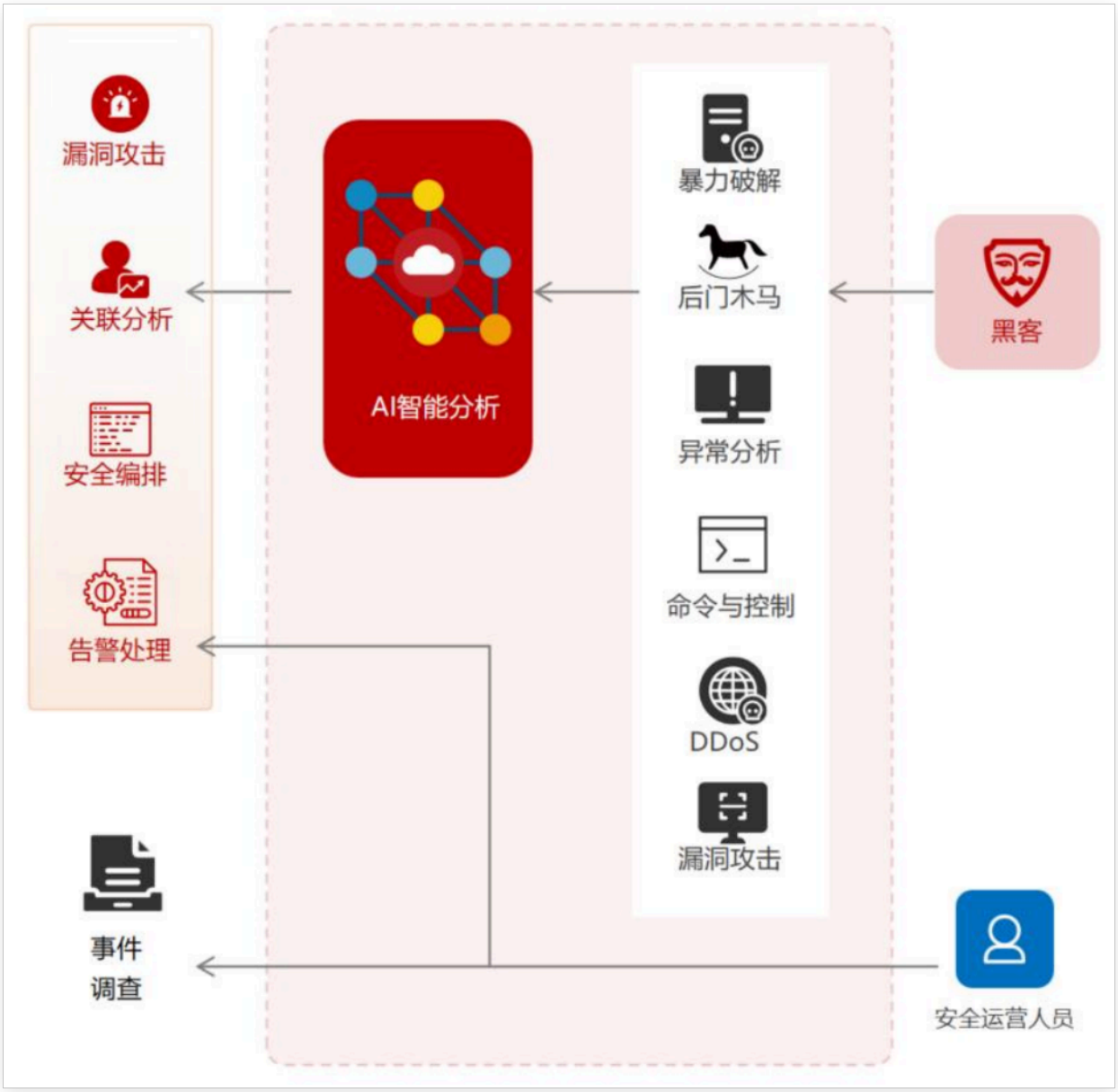
针对企业普遍存在风险、告警、处置三大分散的安全运营痛点，天翼云云安全中心打造云原生一体化安全运营平台。

平台支持全局风险统一可视、多源告警一键接入、智能汇聚降噪、事件一键闭环处置，可大幅提升攻防演练、安全对抗等场景下的应急响应效率。同时平台持续迭代优化安全告警规则，有效帮助中小企业降低安全运营人力与运维成本。

方案优势

- 智能精准告警：跨产品数据关联，减少无效告警，提升告警精准度。
- 统一运营平台：整合分散安全工具，实现高效集中化运营。
- 安全编排响应：一键处置下发 ，快速响。

场景示意图



场景三：安全态势可视化

聚焦 CSO/CIO/CISO 日常管理与上级汇报核心需求，通过安全威胁态势大屏直观呈现安全投资价值，全景展示云上资产风险分布与管控成效，帮助高管实时掌握全栈安全状态，为安全决策、资源调配及汇报沟通提供数据支撑，满足高层对云上业务风险“可视化、可量化、可管控” 的核心诉求。

方案优势

- 全栈服务联动：打通网络 / 主机 / 应用 / 数据等安全服务，实现风险全域覆盖。
- 海量数据实时处理：分布式大数据引擎，支撑海量安全数据实时流分析。
- 可视化决策大屏：全栈安全态势集中呈现，适配管理决策与汇报场景。

场景示意图


CSO/CIO/CSIO
安全看板
资产状况
安全评分
攻击排名
漏洞管理
基线核查
威胁告警
网络安全
主机安全
应用安全
数据安全
安全报表
安全日报
安全周报
安全体检报告
安全态势大屏

产品规格

云安全中心为所有用户提供的主功能是一致的，产品实例主资源目前有标准版一个版本。

另外，在标准版主资源基础上，支持购买扩展资源，用户可以通过购买额外的扩展资源，以满足更多日志分析量以及安全态势大屏等服务的需求。

云安全中心规格说明

云安全中心版本规格说明：

规格名称	可选版本	规格说明	计费模式
（必选）云安全中心实例版本	标准版	具备云安全态势管理（CSPM）、安全信息与事件管理（SIEM），安全编排与自动响应（SOAR）能力的一体化AI智能安全运营平台。	包周期
（必选）日志分析量	-	存储云安全中心日志各项日志信息，500GB起购。 说明 • 日志分析量的额外起购单位为50GB，即每次购买的日志分析量为50GB的整数倍。 • 云安全中心额外免费为您提供50GB的日志分析额度。	包周期
（可选）态势大屏	-	提供态势大屏直观展示用户当前的告警态势以及安全成果态势。	一次性计费

说明

扩展资源与主资源绑定，到期时间与主资源一致。

计费说明

计费模式

云安全中心支持包年包月付费模式。

标准资费

云安全中心根据开通实例时选购的主资源版本、扩展资源数量、购买时长生成预付费账单。

计费项		标准价格
主资源（标准版）		1600元/月
扩展资源	日志分析量	0.45元/GB/月
	态势大屏	4500元/月

说明

- 针对一次性付费客户，享受一年及以上8.5折优惠。
- 一个账号仅可购买一个主资源版本和态势大屏，日志分析量可以重复购买。
- 日志分析量是对采集的安全日志原始数据进行存储，多维度分析的使用总量，一般情况下可按照日志采集量的4倍来进行估算。

扩展资源规格说明

- 云安全中心日志分析量：日志分析量的起购单位为50G，即每次购买的日志分析量为50G的整数倍。
- 云安全中心态势大屏：购买后，失效日期和主产品保持一致。

说明

- 扩展资源不支持独立购买，必须在购买主资源的基础上进行叠加购买。
- 扩展资源购买后与主资源绑定，资源到期时间与主资源一致，不支持单独退订或单独续订。

升级扩容

开通了云安全中心实例后，可根据实际使用需求购买日志分析量扩展资源和态势大屏扩展资源。

前提条件

已购买云安全中心实例。

规格限制

- 态势大屏扩展资源只可购买一次。
- 日志分析量扩展资源的购买资源最小单位为50G，即扩展资源需要购买50G的整数倍。

约束条件

- 云安全中心实例生效期间，支持扩增扩展资源数量。
- 扩展资源与主资源绑定，到期时间与主资源一致，不支持单独续订、退订。

系统影响

购买扩展资源时，原已启用的服务不会暂停，对业务无任何影响。

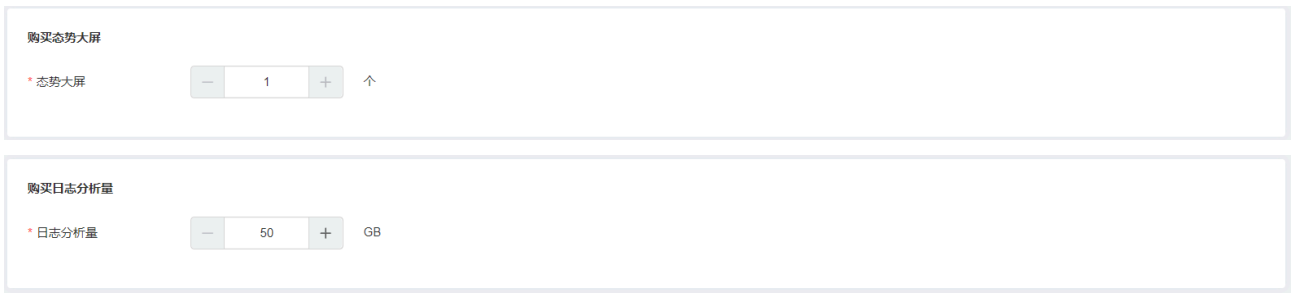
购买扩展资源

若当前实例还未购买某类扩展资源，则需单独购买。

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全 > 云安全中心”，进入产品服务页面。
3. 在左侧导航栏，选择“已购资源”。



4. 选择需要购买的扩展资源，“态势大屏”扩展资源、“日志分析量”扩展资源。



说明

- “日志分析量扩展资源”可以设置购买数量，固定为50G的整数倍。
- “态势大屏扩展资源”为固定1个。

5. 设置扩展资源数量。
6. 在页面下方确认配置费用，阅读《云安全中心服务协议》并勾选“我已阅读，理解并接受《云安全中心服务协议》“，单击“立即购买”。
7. 在订单页完成订单确认并支付，付费成功后，购买扩展资源规格生效。

续订

为避免云安全中心实例到期后，服务自动停止，需要在实例到期前进行手动续费，或设置到期自动续费。

到期说明

服务到期后，如果没有按时续费，平台会冻结服务，但用户配置信息会提供15天的保留期。

- 保留期内，平台会冻结云安全中心的服务，用户配置的各类数据会继续生效，但用户无法访问云安全中心。
- 保留期满，用户若仍未续费，平台会清除实例资源，用户原有的配置信息将会被删除，同时云安全中心将不再获取第三方日志、用户云上资产等信息。

续订说明

订单到期后，若没有续订，将不能继续使用订单中的服务，建议您提前进行续订。更多详情请阅读天翼云 续订规则说明 。

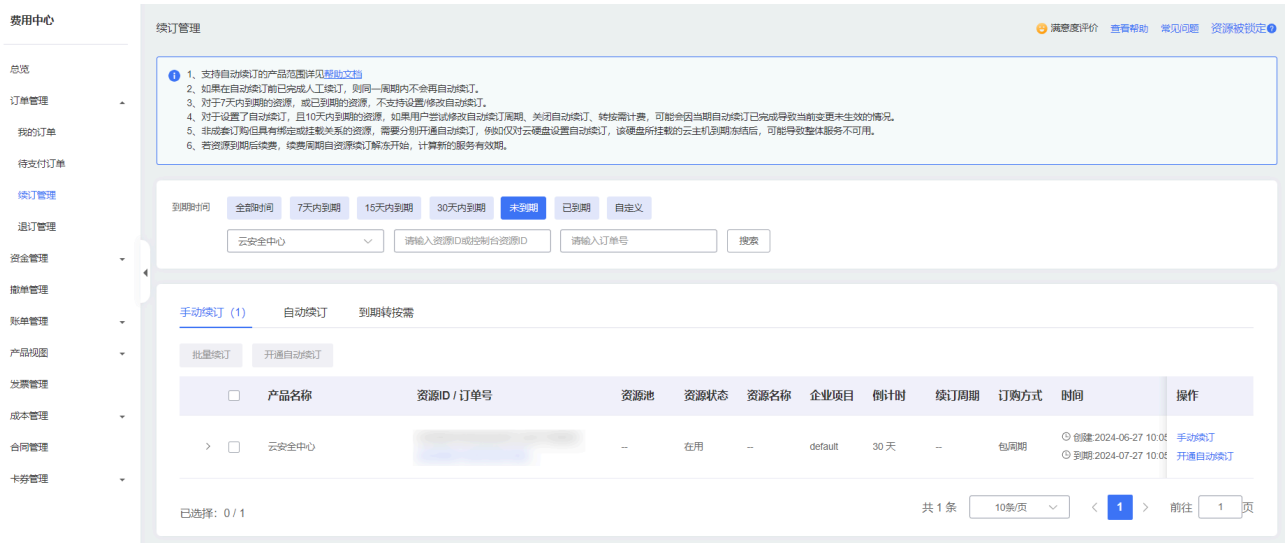
手动续订

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全 > 云安全中心”。
3. 在左侧导航栏，选择“已购资源”。

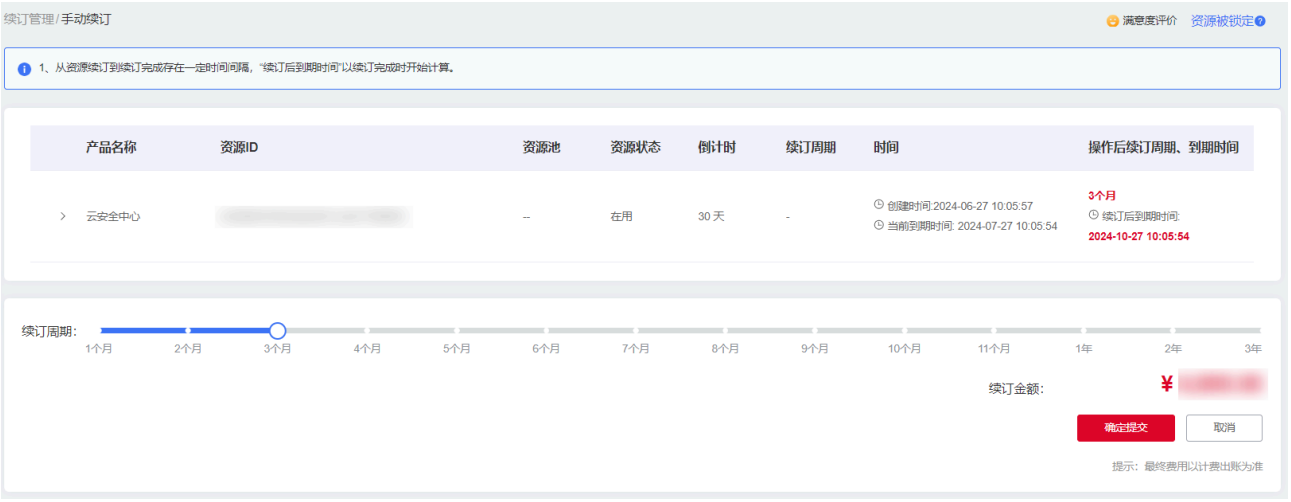


4. 在当前实例信息展示界面，点击“续订”。

5. 在“续订管理”操作界面，可以根据需要进行“手动续订”或者“开通自动续订”。



6. 点击“手动续订”后，进入手动续订页面。
7. 选择续订时长，确认续订时长、续订金额后，单击“确定提交”提交续订订单。



8. 在订单页完成订单确认并支付，付费成功后，续订生效。

自动续订

方法一：云安全中心支持在购买实例时，同步开通“自动续订”。详细操作请参见 购买云安全中心 。

方法二：若开通实例时未开启自动续订，用户也可在开通后，通过天翼云“费用中心 > 订单管理 > 续订管理”页面，开通自动续订。详细操作请参见 开通自动续订 。

退订

云安全中心支持退订，可通过云安全中心控制台界面、天翼云管理中心发起并完成退订操作。

退订说明

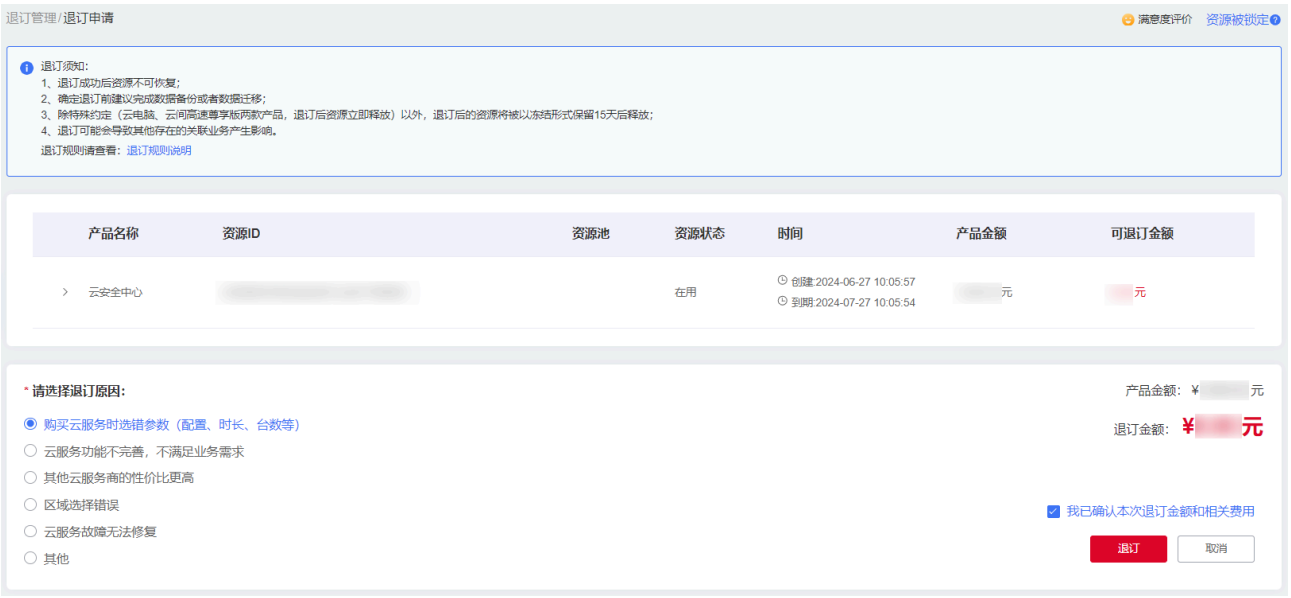
- 云安全中心退订后，主资源及扩展资源将一同退订；扩展资源不支持单独退订。
- 成功发起退订后，实例资源将转入冻结状态，冻结期15天。冻结期间，用户配置数据会保留15天， 用户配置的各类数据会继续生效，但用户无法访问云安全中心，15天后资源被释放，释放后无法恢复。

操作步骤

1. 进入天翼云“费用中心 > 订单管理 > 退订管理”页面，找到相应订单，点击“退订”。



2. 进入退订申请页面，确认退订信息，选择退订原因，信息确认无误后勾选“我已确认本次退订金额和相关费用”，点击“退订。



3. 系统提示退订申请提交成功，可前往“订单管理 > 我的订单”，在订单详情页面查看退订进度。



4. 当状态变为退订完成时，订单完成退订。



查看账单

用户可以在费用中心按月查看在天翼云的消费概况，详情请参见 账单概览 。

账单说明

云安全中心产品为包年包月计费产品，包年包月产品采用预付费模式，即先付费再使用，支付成功后，云资源将被系统分配给用户使用，直到超过保留期后被系统回收。

说明

- 当月最终账单将在次月3日生成，在次月4日10点后可查看和导出。
- 云安全中心属于按月结算的产品，当月消费可在次月3日查看账单。

操作步骤

1. 登录天翼云控制中心。
2. 在页面右上角用户名称处，选择“费用中心”。

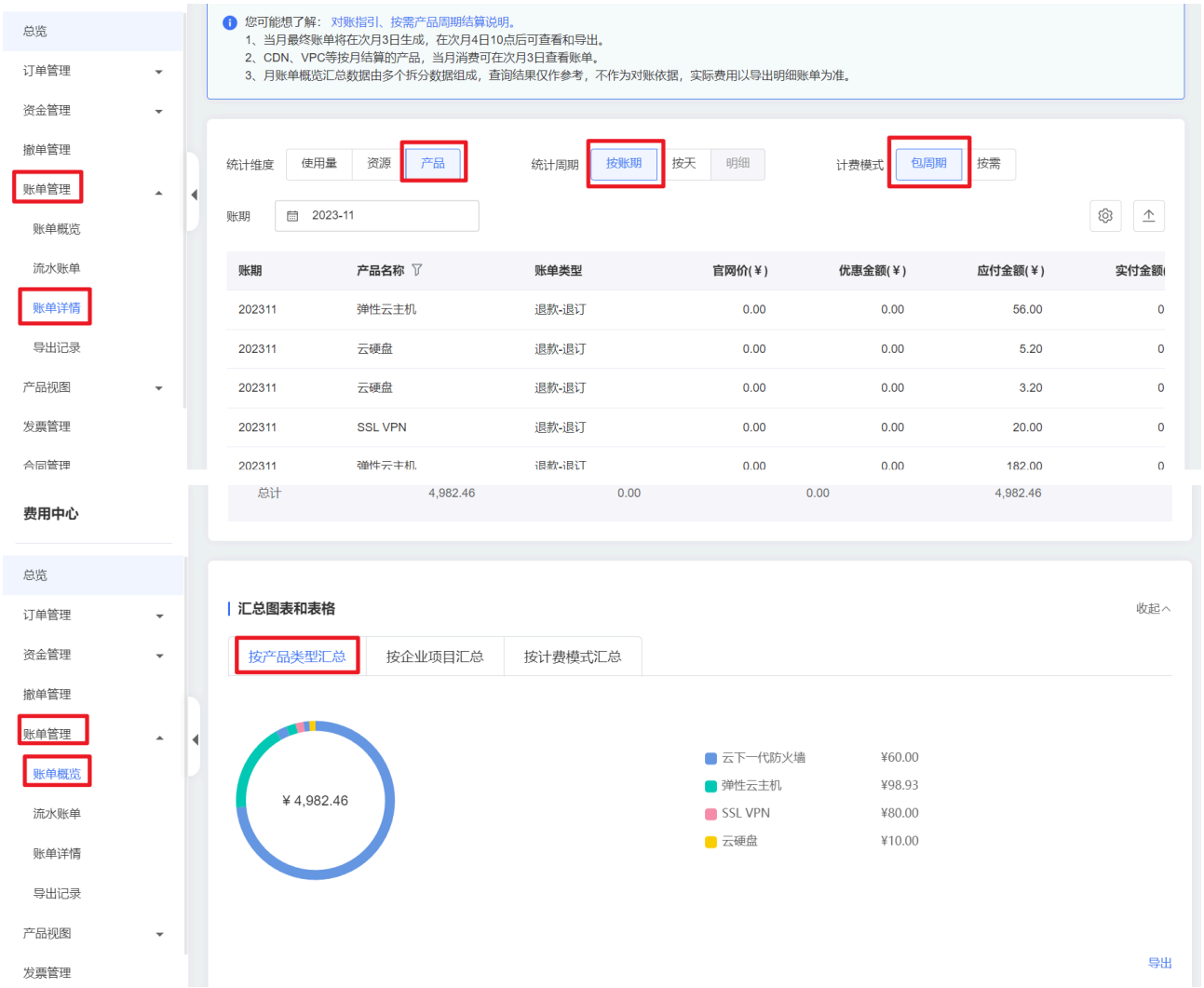


3. 在左侧菜单栏选择“账单管理”，进入“账单概览”页面，可按产品类型汇总查看产品账单。



4. 在左侧菜单栏选择“账单详情”，进入账单详情页面。

   统计维度选择“产品”，统计周期选择“按账期”，计费模式选择“包周期”，账期选择需要查看的账单时间，即可查看到产品的账单详情。

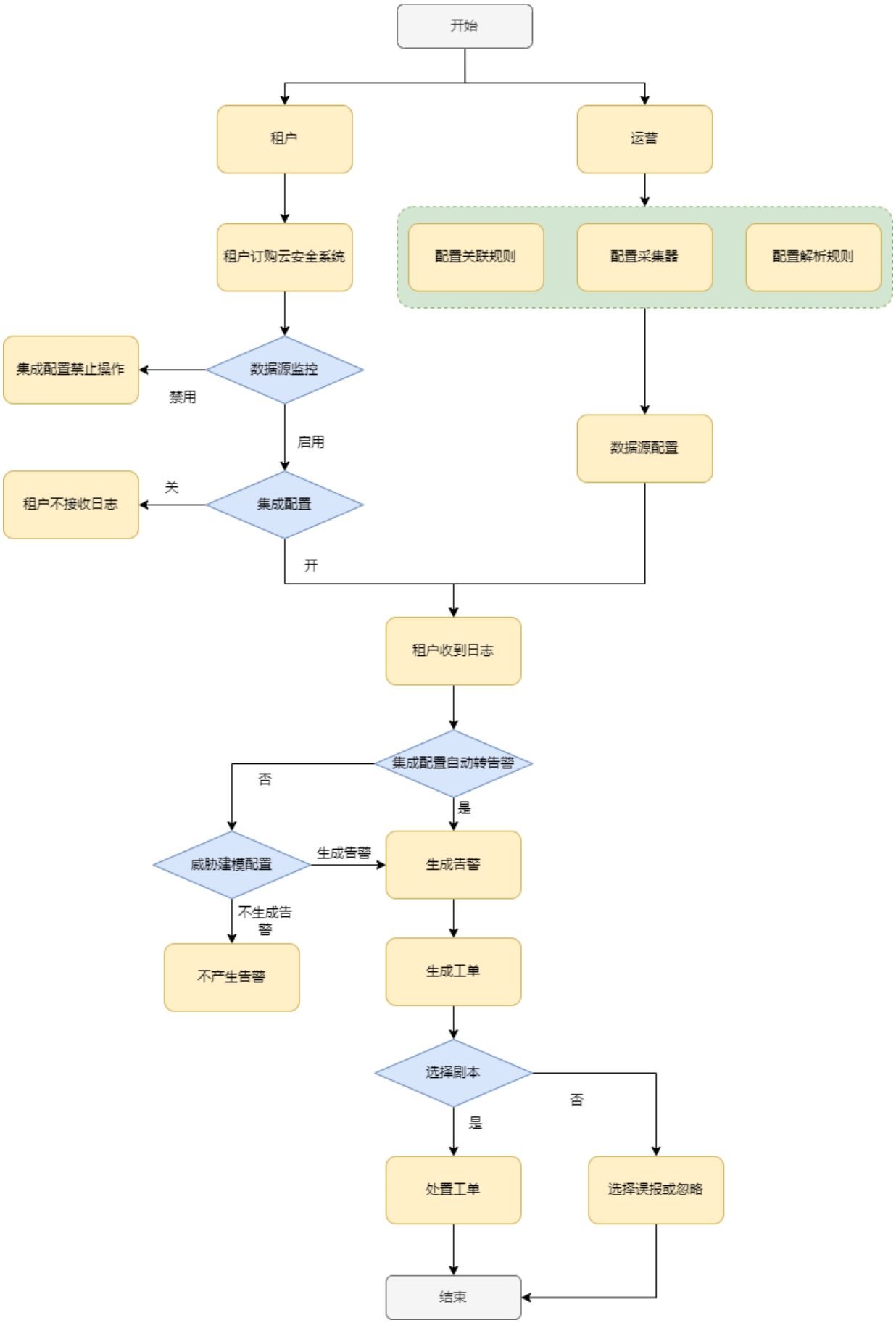


快速入门

使用流程

为全面帮助您进行安全运营，您需要购买云安全中心实例并接入安全产品日志。云安全中心获取到各类日志后，能通过日志的内容进行威胁建模，完成各类安全告警的生成，辅助您进行安全处置，实现安全运营。

云安全中心使用流程如下：


开始
租户
运营
租户订购云安全系统
配置关联规则
配置采集器
配置解析规则
集成配置禁止操作
数据源监控
禁用
启用
数据源配置
租户不接收日志
关
集成配置
开
租户收到日志
集成配置自动转告警
否
是
威胁建模配置
生成告警
生成告警
不生成告警
不产生告警
生成工单
选择副本
否
是
处置工单
选择误报或忽略
结束

购买云安全中心实例

云安全中心支持包年/包月计费方式，目前提供标准版的主资源，两种扩展资源：日志分析量、态势大屏。您可以根据业务规模选择云安全中心规格。

前提条件

已 注册天翼云账号 并完成 实名认证 。

规格限制

- 态势大屏只可购买一次。
- 日志分析量扩展资源的购买资源最小单位为50G，即购买时只能选择50G的整数倍。

约束条件

- 同一账号在同一个区域只能开通一个云安全中心实例，对应一个服务版本。
- 开通云安全中心实例，必须购买主资源，主资源生效期间，支持叠加购买扩展资源，扩展资源与主资源绑定，到期时间与主资源一致，不支持单独续订、退订。

适用场景

用户购买了天翼云上的安全服务“Web应用防火墙（原生版）、服务器安全卫士（原生版）、云等保专区、数据库审计、云堡垒机（原生版）企业版、云防火墙（原生版）”并部署在天翼云上。

操作步骤

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全 > 云安全中心”，进入云安全中心控制台。



3. 单击“立即购买”，进入购买页面。
4. 选择版本信息、扩展资源、购买时长。

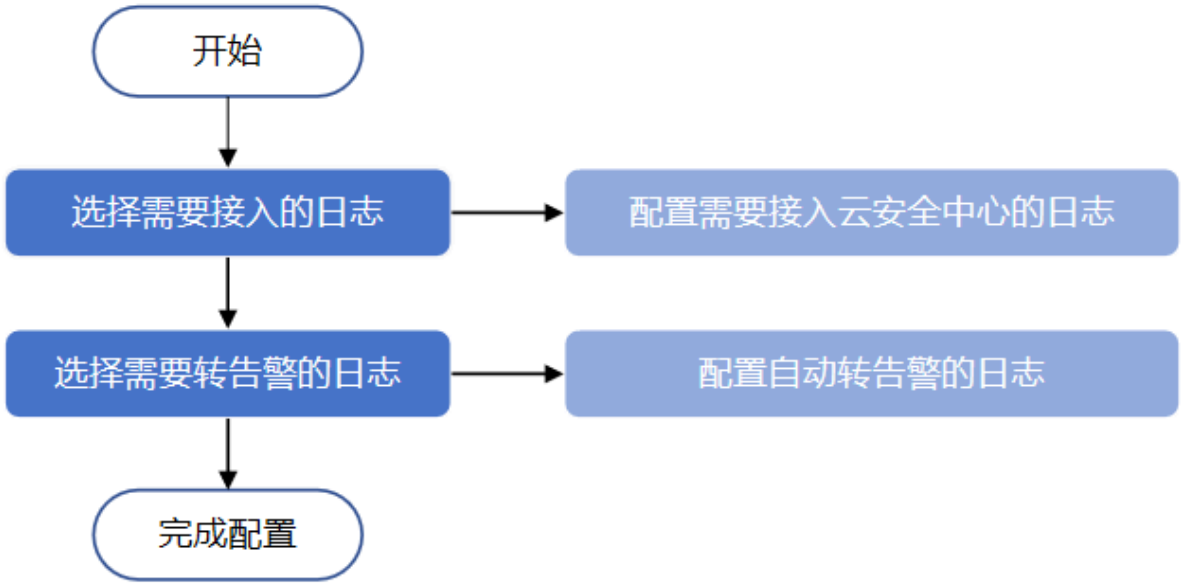
参数		说明
基本信息	版本选择	支持“标准版”。规格详情请参见 产品规格 。
	计费模式	支持“包年包月”。
扩展配置	购买态势大屏	默认为“现在购买”，也可以选择“暂不购买”。 说明 态势大屏只可购买一次。
	购买日志分析量	默认为“现在购买”，也可以选择“暂不购买”。 说明 • 云安全中心标准版免费提供50G的日志分析额度，如果您需要额外的额度，请另外购买。 • 日志分析量扩展资源的购买资源最小单位为50G，即购买时只能选择50G的整数倍。
订购	购买时长	拖动时间轴设置购买时长。
	自动续订	开启“自动续订”后，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。 • 按月购买，自动续费周期默认为3个月。 • 按年购买，自动续费周期默认为1年。 如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。

5. 确认配置参数和配置费用，阅读《云安全中心服务协议》并勾选“我已阅读，理解并接受《云安全中心服务协议》”，单击“立即购买”。
6. 进入“付款”页面，完成付款。

接入日志、告警

开通云安全中心实例后，系统默认会接入部分日志数据并对用户进行初始化配置。您可以根据自己的业务特性修改初始化配置。

在云安全中心的集成配置页面，选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。



前提条件

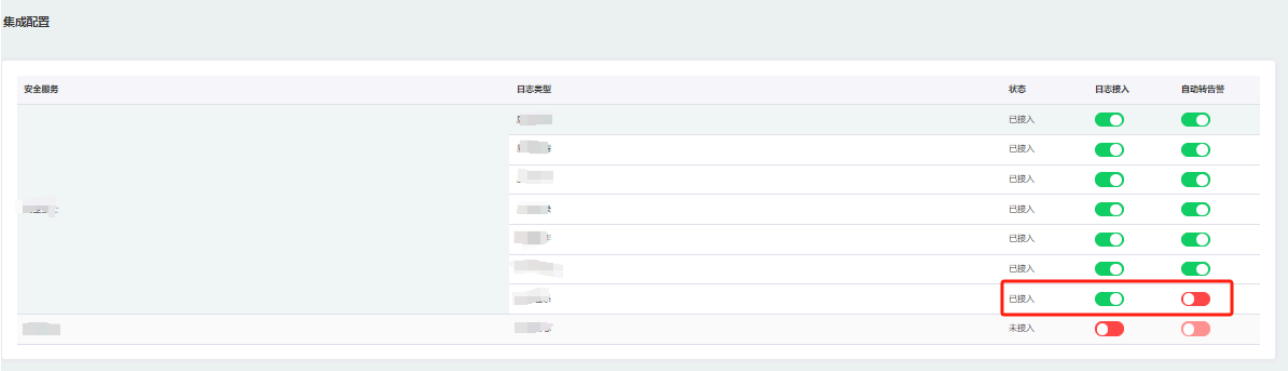
- 已购买云安全中心实例，具体操作请参见 购买云安全中心实例 。
- 已购买天翼云上的安全服务“Web应用防火墙（原生版）、服务器安全卫士（原生版）、云等保专区、数据库审计、云堡垒机（原生版）企业版、云防火墙（原生版）”并部署在天翼云上。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“设置 > 数据源监控”，打开数据源监控页面。
3. 在操作列点击“启用”，确保数据源监控处于启用状态。



4. 在左侧导航栏，选择“设置 > 集成配置”，打开数据集成配置页面。
5. 选择需要接入的日志，并打开日志接入开关。



6. 选择需要转告警的日志，并打开自动转告警的开关。



说明

- 系统默认会接入部分日志，用户如有需要，可以自行关闭。
- 需要先在数据源监控页面启用开关后，才可以在集成配置页面中开启日志和告警配置。
- 选择需要接入的日志时，只能针对您已经购买的云产品。
- 选择需要转告警的日志，只能针对已经选择接入的日志进行。

查看安全概览

安全概览会通过大屏的方式展示安全评分、资产总数、告警总数、威胁动态、日志分布TOP5、风险资产TOP5、告警处置概览、近七天趋势图、攻击链统计图。

前提条件

安全概览的数据来源于接入系统的数据量，需要确保已完成数据接入。具体操作请参见 接入日志、告警 。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“安全态势 > 安全概览”，进入安全概览页面，查看安全评分和风险数据统计。

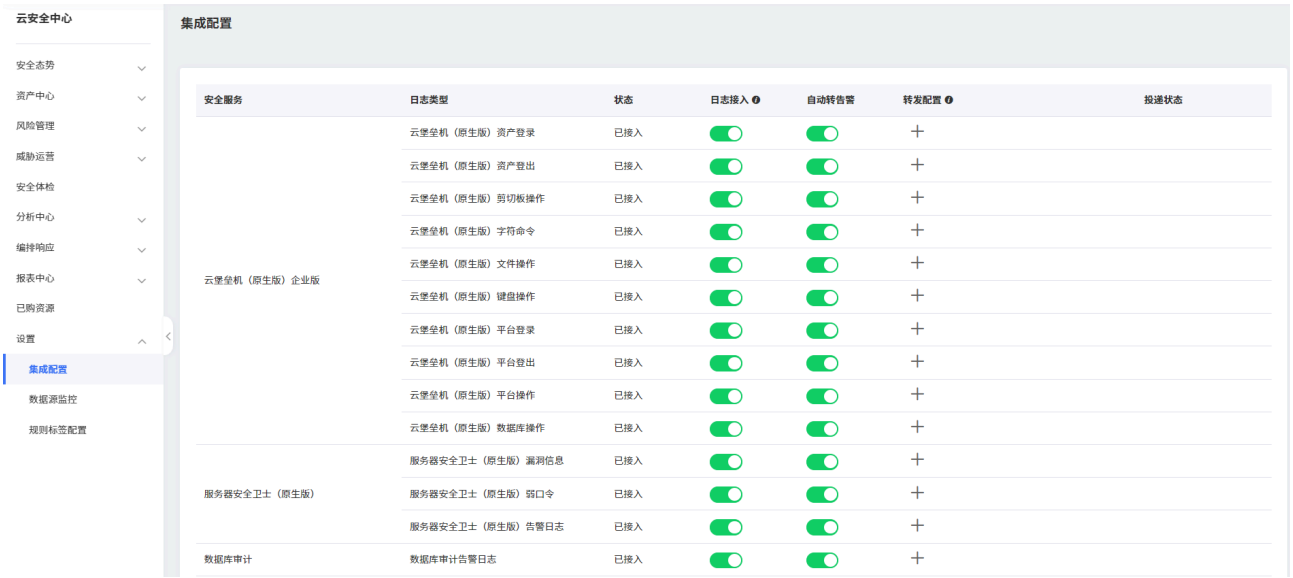
> 说明
>
> - 日志、告警等维度数据展示均支持下钻点击，通过详情进行展示。
> - 概览数据只展示当前情况，最新实时数据需要手动刷新页面获取。

日志、告警外发设置

日志外发功能为公测功能，新购用户可以限时免费体验。

为日志类型添加转发目标

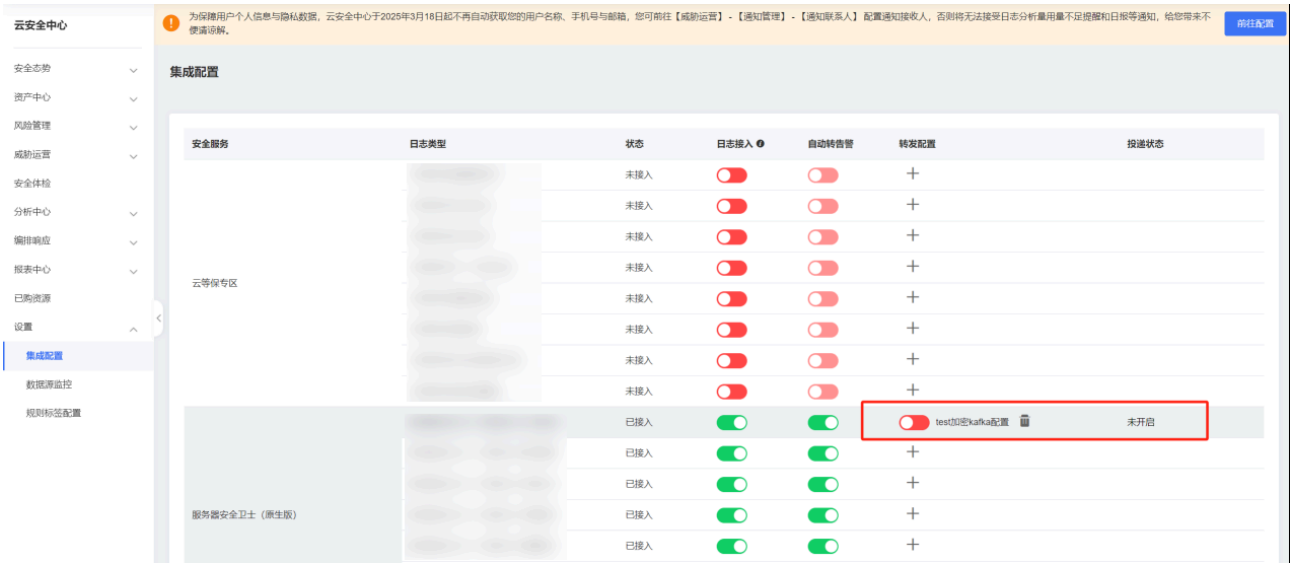
1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“设置 > 集成配置”，进入集成配置页面。



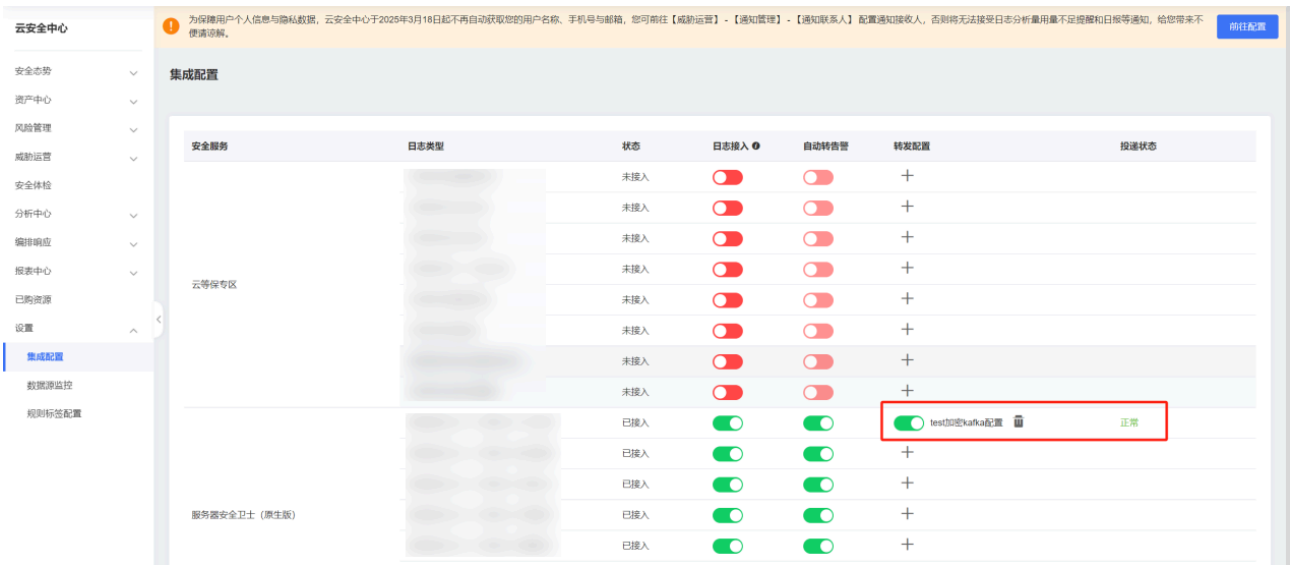
3. 选择日志类型，点击“转发配置”列的【+】按钮，弹出“新增转发配置”窗口。



4. 选择“转发目标”，单击“保存”，自动返回集成配置页面。此时转发配置开关为“关闭”，投递状态为“未开启”。

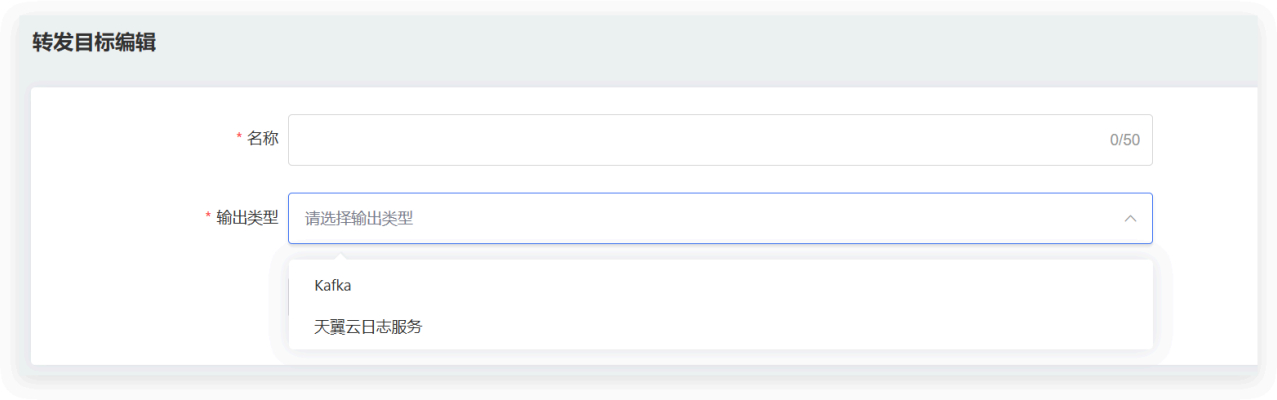


5. 单击“转发配置”开关，打开“转发配置”。



配置转发目标

1. 在新增转发配置页面，单击“转发目标配置”进入转发目标配置页面，单击“新增”，进入“转发目标编辑”页面。



2. 输入相关信息，单击“检测”。

说明

- 当输出类型选择Kafka时，“加密类型”选择“不加密”时，会自动在目标Kafka创建相应的“队列名（topic）”。
- 当输出类型选择Kafka时“加密类型”选择“SASL加密”时，需要先手动在目标Kafka创建相应的“队列名（topic）”。
- 当输出类型选择天翼云日志服务时，资源池仅支持选择”华东1“、”西南1“、”华北2“、”华南2“。

3. 检测通过后，单击“保存”。

保存成功，返回转发目标配置页面，可以看到已新增的转发目标。



用户指南

安全态势

安全概览

安全概览：展示安全评分、资产总数、风险资产数、已处置漏洞数量、已处置漏洞告警数量、威胁动态、安全运营、待处理告警数量。



安全评分

评分系统根据弱口令、漏洞和告警扣分，各占40%、30%、30%。

扣分规则：【弱口令】10分/项；【漏洞】高危5分/项，中危2分/项；【告警】致命5分/项，严重3分/项，警告1分/项。

风险等级实时更新，低风险（80-100分）、中风险（60-80分）、高风险（0-60分）。

> 说明
>
> 安全评分是依据用户的弱口令、漏洞、告警进行综合计算，不同项目其分数配额相互独立。

资产总数

统计已经接入云安全中心的资产总数，单击对应按钮即可跳转至 资产概览 页面。

风险资产数

统计所有风险资产总数，单击对应按钮即可跳转至 资产概览 页面。

已处置漏洞

统计所有云安全中心中已处理的漏洞总数量，单击对应按钮即可跳转至 漏洞管理 页面。

已处置告警

统计所有云安全中心中已处理的告警总数量。

告警总数

统计您当前产生的所有有效告警数量，同时展示最近七日的新增数量以及待处置的有效告警数量。

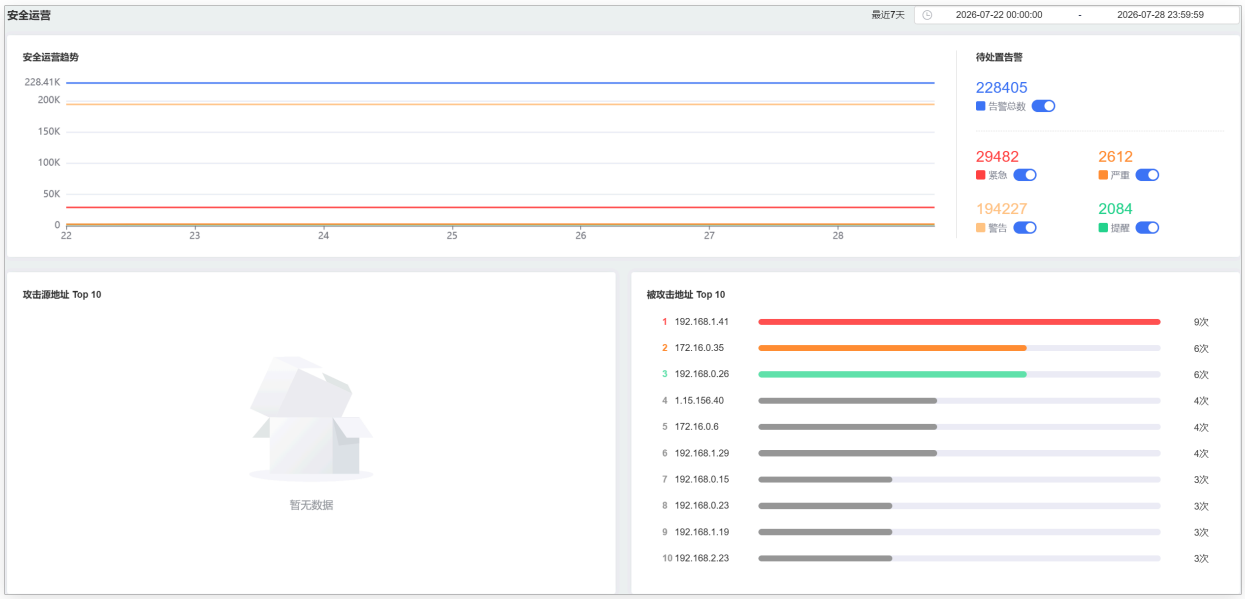
- 近7日新增，点击数量可以跳转至告警管理页面，并查询近7天的数据。
- 待处置数量，点击数量可以跳转至告警管理页面，并查询“处置状态 = 待处置”的数据。

威胁动态

提供有效告警滚动展示，快速定位高风险事件，提升响应效率。

- 点击“查看更多”，可以跳转至告警管理页面，并查询“处置状态 = 待处置”的数据。

安全运营



展示最近七天告警总数、紧急告警数量、严重告警数量、警告告警数量、提醒告警数量、攻击源地址TOP10、被攻击地址TOP10，进行轮播。

安全合规

安全合规模块展示云安全中心基线检查项总数、已通过检查项、通过率、未通过基线TOP10。



综合安全态势

用户可以查看攻击源地址TOP10、攻击目标地址TOP10和全国、全球地图上的攻击态势。

前提条件

综合安全态势需要购买态势大屏扩展资源，具体操作请参见 升级扩容 。

查看综合安全态势大屏

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全 > 云安全中心”，进入产品服务页面。
3. 在左侧导航栏，选择“安全态势 > 综合安全态势”，进入综合安全态势大屏页面。
   - 在右上角支持选择时间范围，也可以设置定时刷新时间。
   - 单击右上角的  图标，进入全屏模式。
   - 单击左上角的  图标，返回“安全概览”页面。



设置定时刷新时间

综合安全态势大屏支持定时刷新大屏数据，定时刷新时间最小为5分钟刷新一次，最大为720分钟刷新一次，进入大屏默认为30分钟刷新一次。

您可以执行以下步骤修改定时刷新时间：

1. 在综合安全态势大屏页面，单击右上角时间范围。
2. 单击“停止”，间隔时间变为可配置。配置完时间后，再单击“开始”，即可完成修改。

安全成果展示

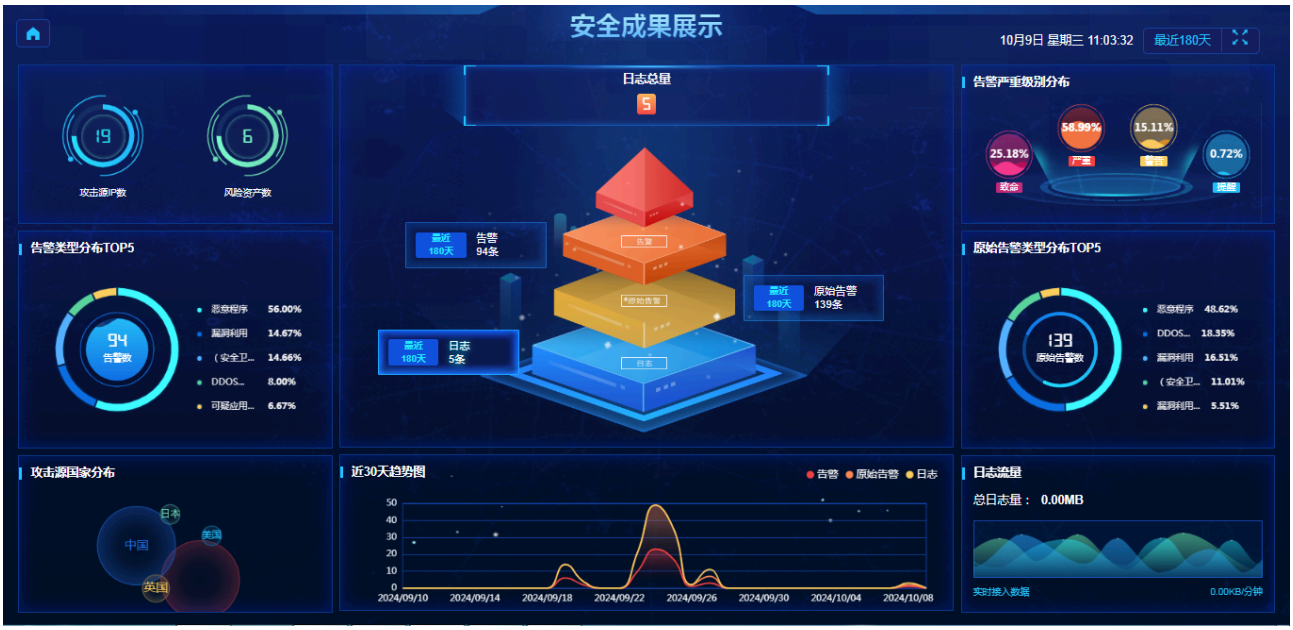
用户从日志接收解析到最终形成告警过程全流程的过程重要的数据统计。

前提条件

安全成果展示需要购买态势大屏扩展资源，具体操作请参见 购买扩展资源 。

查看安全成果展示大屏

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全 > 云安全中心”，进入产品服务页面。
3. 在左侧导航栏，选择“安全态势 > 安全成果展示”，进入安全成果展示大屏页面。
   - 在右上角支持选择时间范围，也可以设置定时刷新时间。
   - 单击右上角的  图标，进入全屏模式。
   - 单击左上角的  图标，返回“安全概览”页面。

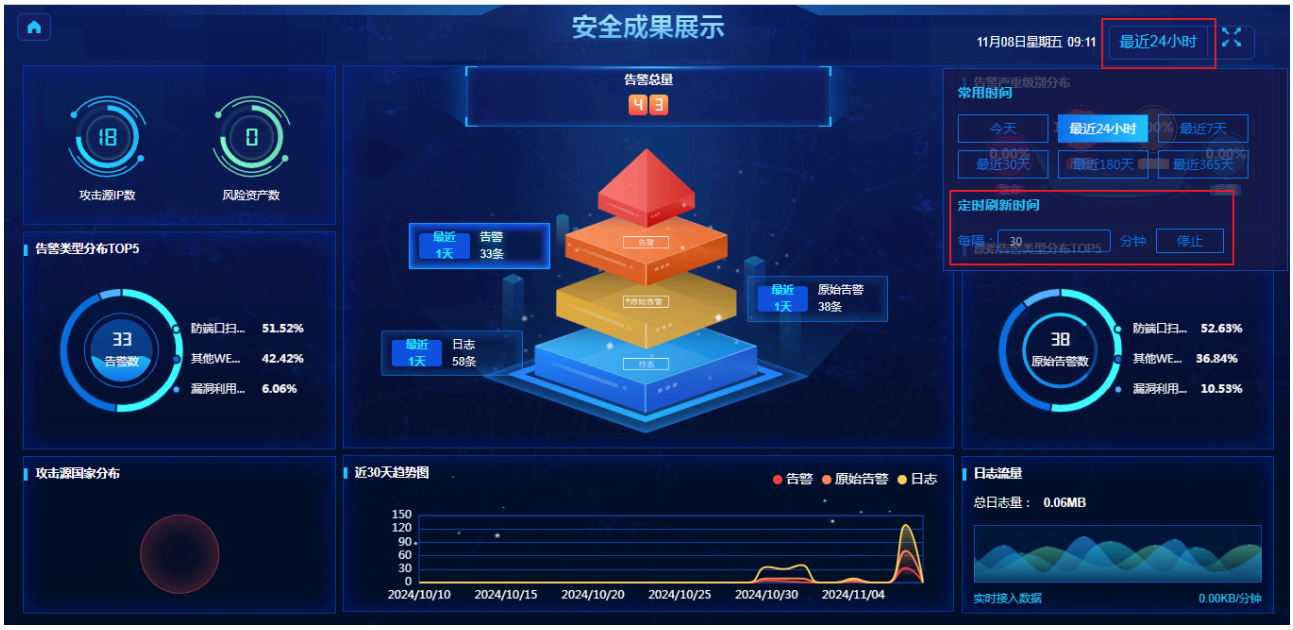


设置定时刷新时间

安全成果展示大屏支持定时刷新大屏数据，定时刷新时间最小为5分钟刷新一次，最大为720分钟刷新一次，进入大屏默认为30分钟刷新一次。

您可以执行以下步骤修改定时刷新时间：

1. 在威胁攻击态势大屏页面，单击右上角时间范围。
2. 单击“停止”，间隔时间变为可配置。配置完时间后，再单击“开始”，即可完成修改。



威胁攻击态势

用户可以查看不同级别的告警的数量统计、异常资产、高危待处理等态势。

前提条件

威胁攻击态势需要购买态势大屏扩展资源，具体操作请参见 购买扩展资源 。

查看威胁攻击态势大屏

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全 > 云安全中心”，进入产品服务页面。
3. 在左侧导航栏，选择“安全态势 > 威胁攻击态势”，进入威胁攻击态势大屏页面。
   - 在右上角支持选择时间范围，也可以设置定时刷新时间。
   - 单击右上角的  图标，进入全屏模式。
   - 单击左上角的  图标，返回“安全概览”页面。



设置定时刷新时间

威胁攻击态势大屏支持定时刷新大屏数据，定时刷新时间最小为5分钟刷新一次，最大为720分钟刷新一次，进入大屏默认为30分钟刷新一次。

您可以执行以下步骤修改定时刷新时间：

1. 在威胁攻击态势大屏页面，单击右上角时间范围。
2. 单击“停止”，间隔时间变为可配置。配置完时间后，再单击“开始”，即可完成修改。



资产中心

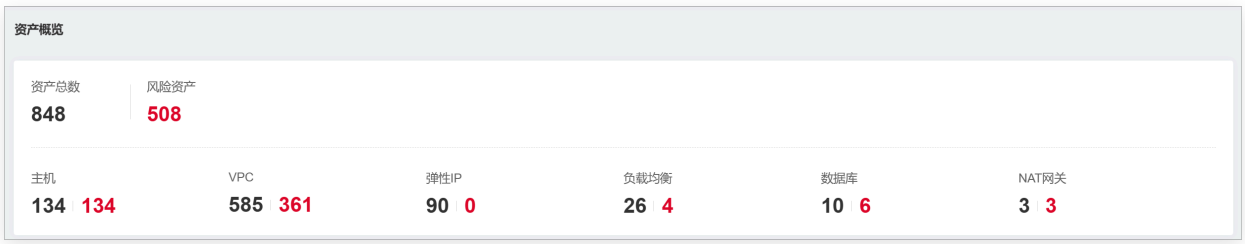
资产概览

资产总数

资产概览显示资产总数、风险资产数、主机数量、VPC数量，弹性IP，负载均衡，数据库和NAT网关数量。

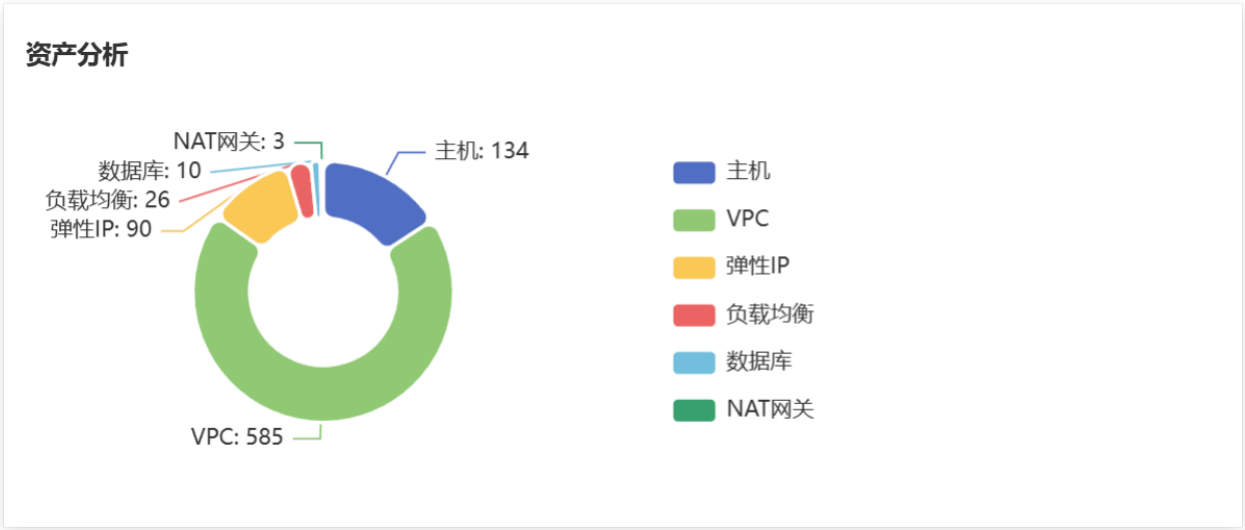
单击资产黑色数字，会跳转至对应资产的全量列表。

单击资产红色数字，会跳转至有风险资产的列表。



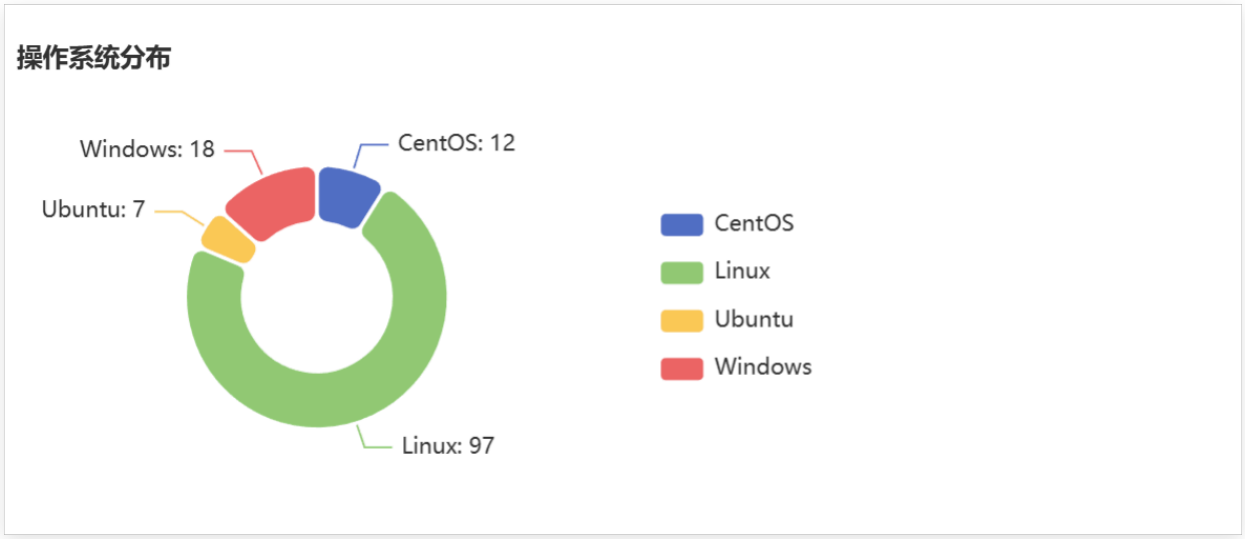
资产分析

资产分析模块使用饼状图展示所有资产数量。



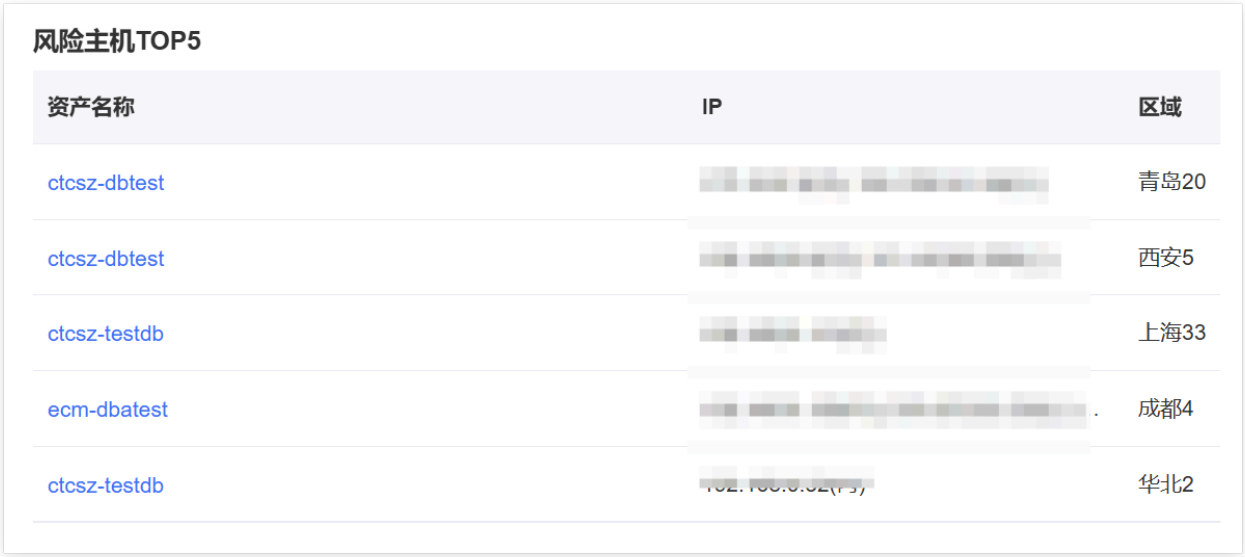
操作系统分布

操作系统分布使用饼状图展示所有资产的操作系统分布情况。



风险主机TOP5

风险主机TOP5展示风险总数量最多的5个资产，可单击资产名称跳转至对应资产。



风险主机TOP5

资产名称	IP	区域
ctcsz-dbtest	[redacted]	青岛20
ctcsz-dbtest	[redacted]	西安5
ctcsz-testdb	[redacted]	上海33
ecm-dbatest	[redacted]	成都4
ctcsz-testdb	[redacted]	华北2

风险组件TOP5

风险组件TOP5展示风险总数量最多的5个组件，可单击组件名称跳转至对应组件。



风险云组件TOP5

资产名称	资产类型	区域	风险数量
mysql-dba-rds	MySQL	长沙42	4个
vpc-39ed	VPC	[redacted]	3个
vpc-yy-20250526	VPC	[redacted]	3个
vpc-c946	VPC	[redacted]	3个
vpc-20250115-yy	VPC	[redacted]	3个

资产管理

为了便于租户对平台资产数据进行整理分析与管理，资产中心提供资产管理功能。为租户提供主机资产、网络资产、数据库资产及资产属性的查询、资产导入导出以及导入资产的删除功能。

用户可以根据自身需求，选择主机、VPC、弹性IP、负载均衡、数据库、NAT网关页签查询。



查询资产

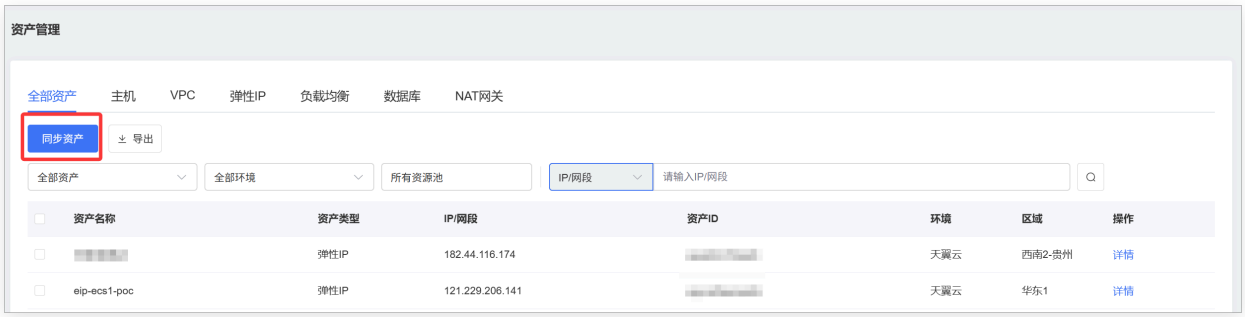
为租户提供资产及资产属性的查询功能。

可以根据资产类型、资产环境、所属资源池、资产IP、资产名称和资产ID查询资产。



更新资产信息

单击“同步资产”，获取最新资产状态。



查看资产详情

在资产详情页面可以查看资产的基础信息，以及该资产上存在的风险。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“资产中心 > 资产管理”，进入资产管理页面。
3. 在资产管理页面，单击资产操作列的“详情”，即可跳转至对应资产的资产详情页面。



资产导入

1. 选择需要导入的资产类型。
2. 在资产列表上方，单击“导入”。
3. 在弹出的“资产导入”窗口中，单击“资产导入模板下载”，下载导入模板。
4. 按照导入模板字段说明，完成模板填写。
5. 单击“选择文件”，上传模板文件。
6. 单击“导入”，完成导入。



资产导出

1. 在页签最上方选择需要导出的资产类型。
2. 在资产列表上方，单击“导出”。
3. 在弹出的提示框中，单击“确定”，完成资产导出。



风险管理

云安全态势管理

云安全态势感知页面默认为每天进行扫描并展示最新的扫描结果，其中包括通过率、全部检查项、已通过检查项、已加白项。

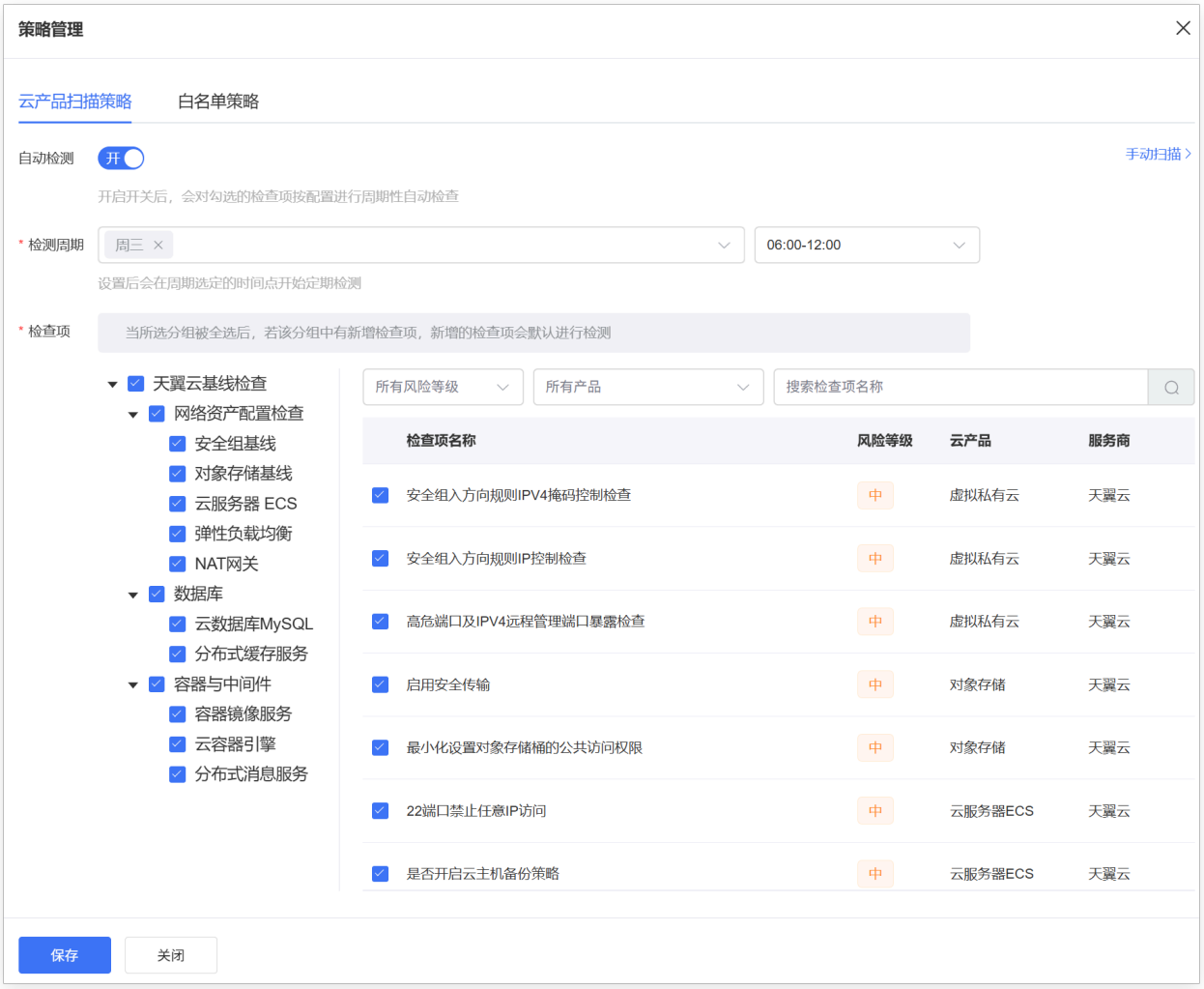


策略管理

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“风险管理 > 云安全态势管理”。
3. 在页面右上角中，选择“策略管理”。



4. 在页面右侧弹出的对话框中，根据业务需求选择策略管理内容。



5. 策略配置完成后，单击“保存”即可完成策略配置。

新增白名单策略

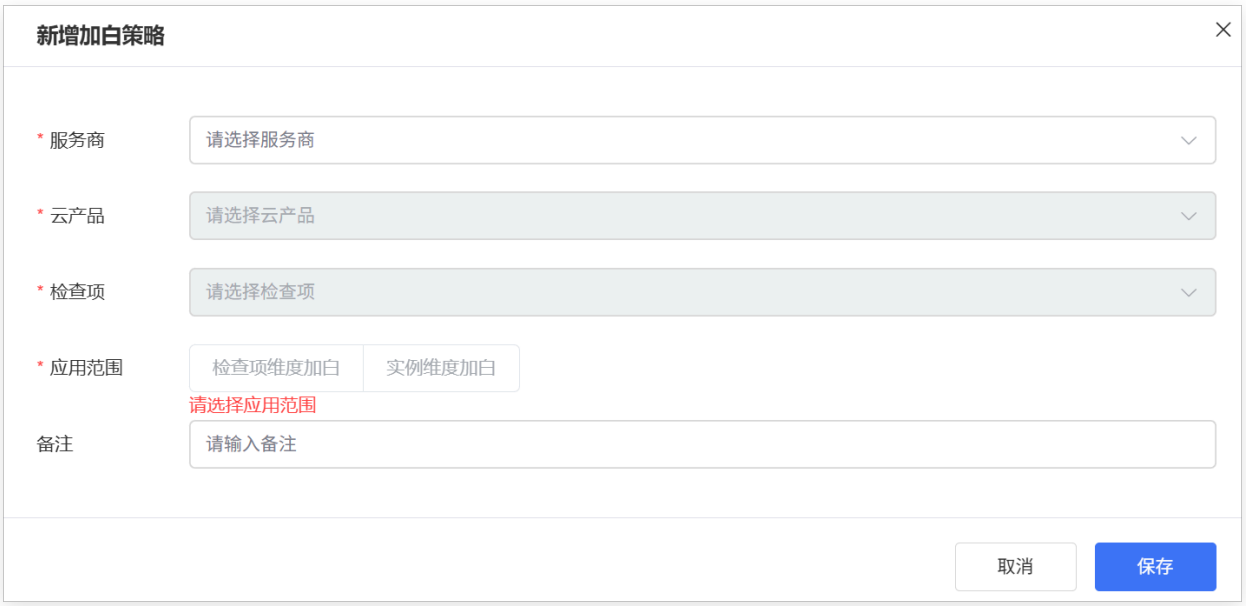
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“风险管理 > 云安全态势管理”。
3. 在页面右上角中，选择“策略管理”。



4. 在页面右侧弹出的对话框中，选择白名单策略。



5. 单击“新增加白策略”，在弹出的对话框中填写加白信息。



6. 填写完成后，单击“保存”即可完成白名单策略新增。

检查项验证

您可以通过人工方式定期执行安全检查项，对云端资产进行全面安全验证。

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“风险管理 > 云安全态势管理”。

3. 选择需要执行的检查项，单击“操作”列的“验证”按钮，在弹出的对话框中，单击“确定”即可开始扫描。

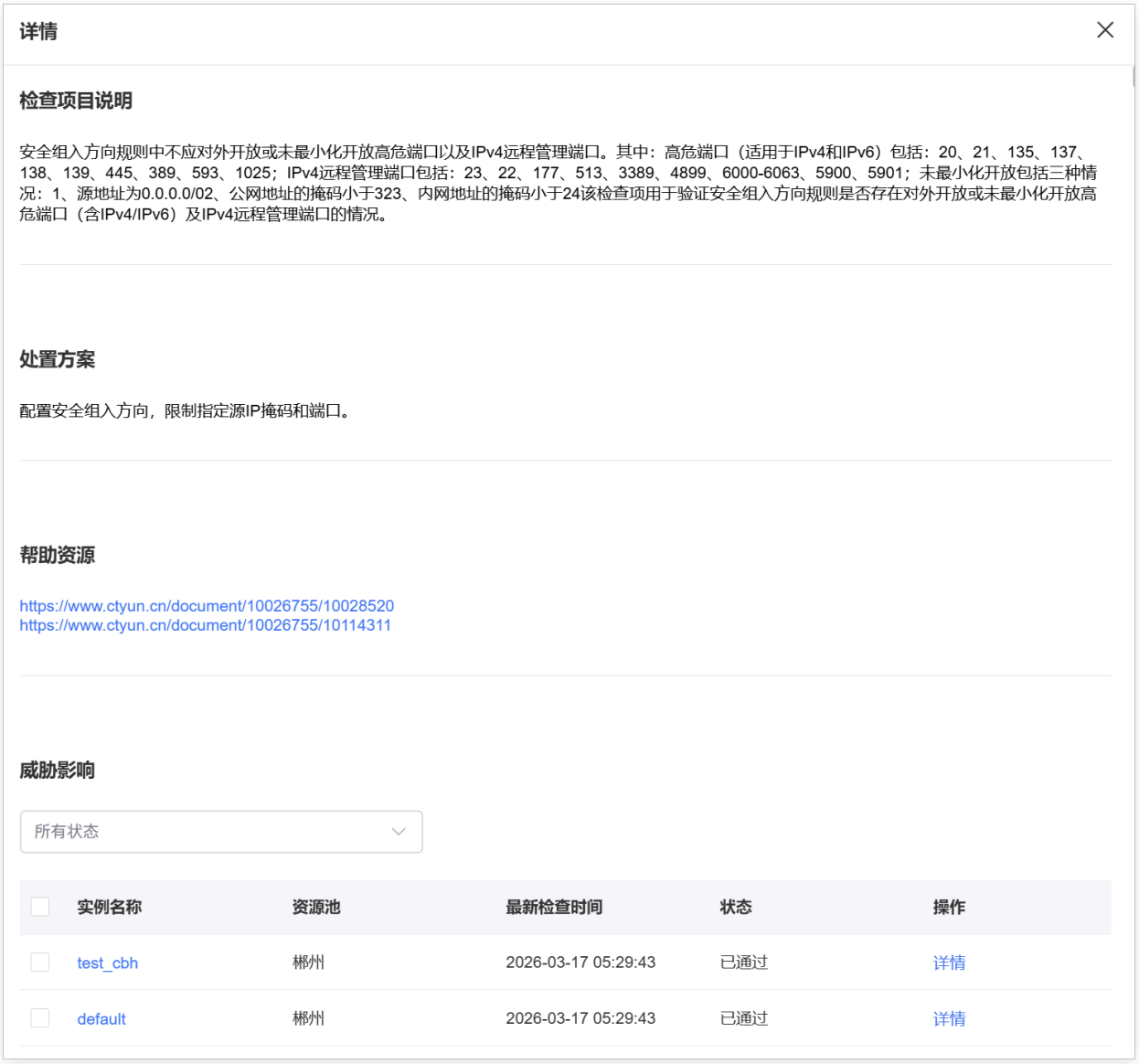


4. 开始验证后，对应检查项的状态会变为“检查中”。
5. 验证完成后，状态会变为“已通过”或“未通过”，可单击“操作”列的“详情”查看检查结果。



查看检查结果

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“风险管理 > 云安全态势管理”。
3. 选择需要检查结果的检查项，单击“操作”列的“详情”按钮查看检查结果。



将检查项加入白名单

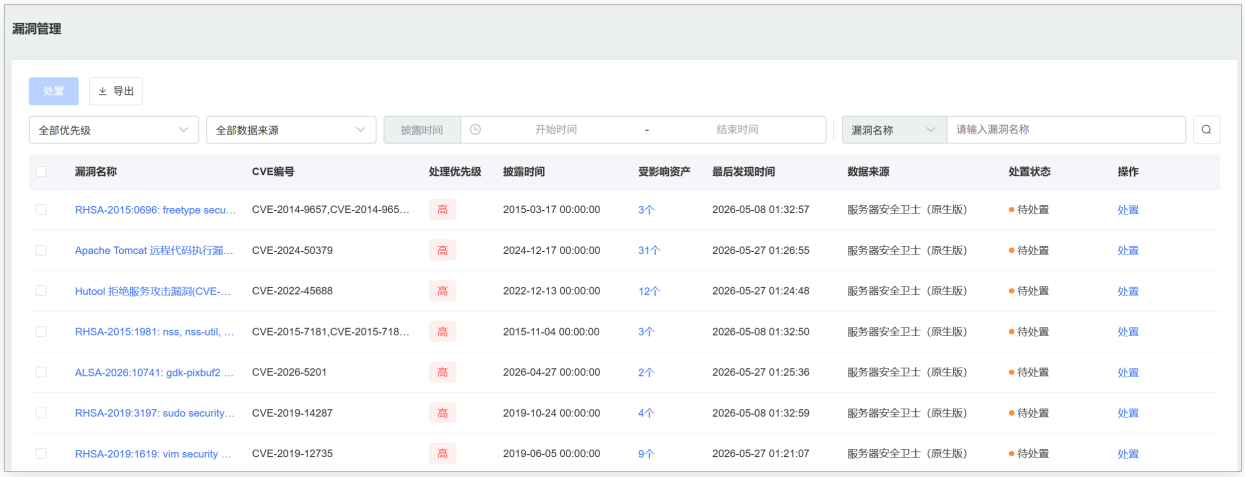
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“风险管理 > 云安全态势管理”。
3. 选择需要加白的检查项，单击“操作”列的“加白名单”按钮。



4. 在弹出的对话框中单击“确认”即可加入白名单。

漏洞管理

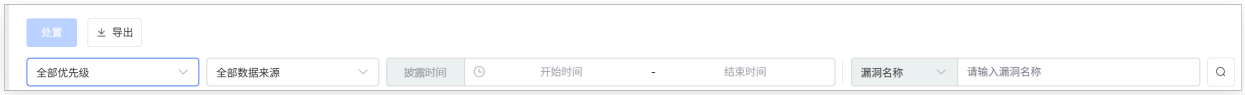
漏洞管理为租户提供漏洞查询及处置功能。



条件查询

支持条件查询，用户输入或选择相关条件内容。

查询条件支持漏洞优先级、漏洞来源、漏洞披露时间、漏洞名称、CVE编号、资产ID。



处置漏洞

提供处置能力，可直接或批量修改漏洞处置状态。状态枚举值：处置完成、待处置（此处修改漏洞状态仅用于云安全中心展示使用）。



修改处置状态可填写处置说明，便于后续查看状态变更原因。



查看漏洞详情

单击漏洞名称，可以查看漏洞影响的资产、漏洞的来源、漏洞来源参考和处置日志、



导出漏洞列表

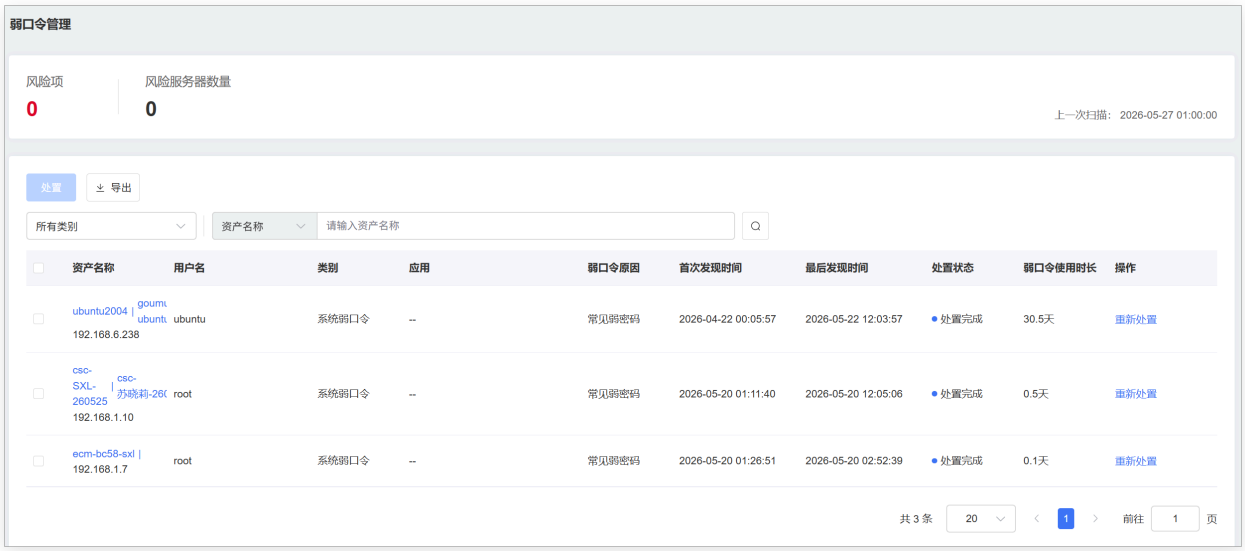
单击漏洞列表上方的“导出”，导出查询条件下的所有漏洞。

导出字段：漏洞名称、CVE编号、处理优先级、披露时间、受影响资产、最后发现时间、数据来源、处置状态。



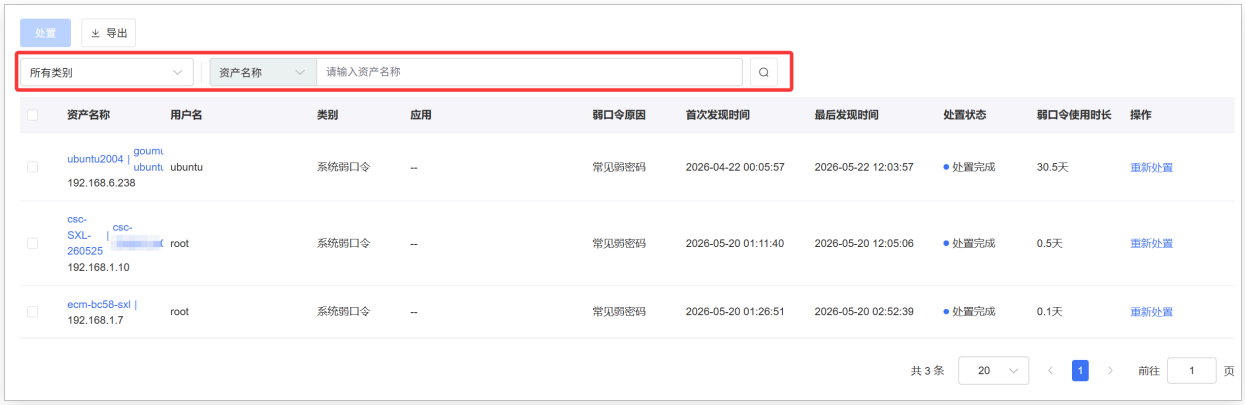
弱口令管理

为租户提供弱口令查询及处置功能。



条件查询

查询条件支持弱口令类别、资产名称、用户名查询。



处置弱口令

提供处置能力，可直接或批量修改弱口令处置状态。状态枚举值：处置完成、待处置（此处修改弱口令状态仅用于云安全中心展示使用）。

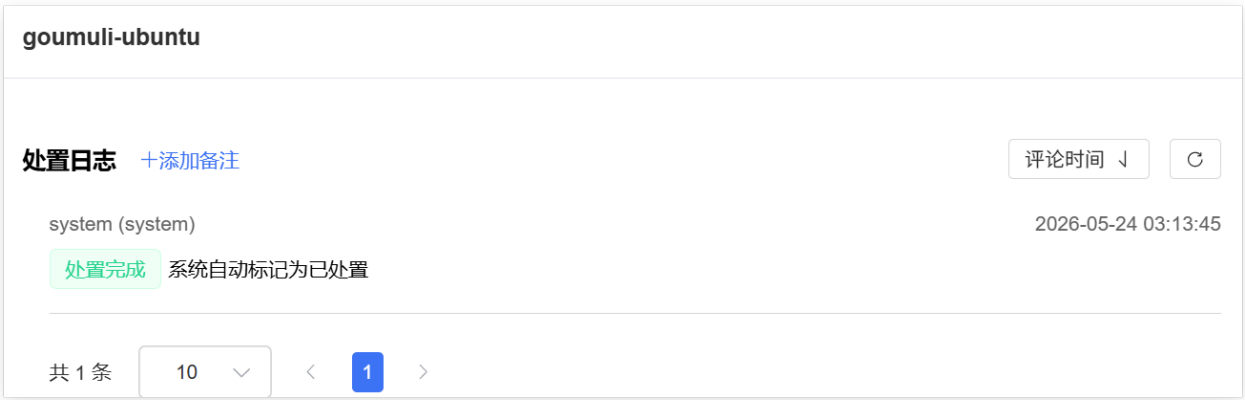


修改处置状态可填写状态变更原因。



查看弱口令详情

在弱口令详情中，可以查看所有历史状态变更记录的信息，包括：处置人、处置状态、处置说明和处置时间等。



导出弱口令列表

单击弱口令列表上方的“导出”，导出查询条件下的所有弱口令。

威胁运营

告警概览

告警概览由待处置告警数量、已处置告警数量、自动处置告警书、告警来源分布、告警类型TOP5、关联资产TOP5等指标展现。



AI智能分析告警

该功能为公测功能，新购用户可限时免费体验。

注意事项

- 智能分析内容为AI生成，可对单条告警刷新多次查询，每次返回的回答会略有差异，处置建议仅供参考，请您仔细甄别。
- 向AI输入的信息已进行敏感信息过滤。

约束限制

每日查询（含重新生成）上限为10次。

操作步骤

1. 进入告警列表，选择需要分析的告警，单击告警名称进入告警详情。
2. 单击下方的“智能分析”按钮。



3. 等待AI生成回答，该过程耗时约为30秒至60秒，您可收起弹框稍后查看。



告警管理

告警管理是为了便于对告警的统一管理、处置与后续分析。告警管理用于告警的统一管理，进行告警的处置。告警管理界面可以很详细地看到告警的基本属性，以及告警的处置情况，告警管理界面可以以告警编号、告警名称、告警分类、告警级别、告警工单状态、告警来源及时间段查询指定的告警工单。

前提条件

已开通云安全中心实例。

查看告警详情

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 告警管理”。
3. 在告警管理中，点击告警名。



4. 进入告警处置页面，可以看到告警相关详细信息。



处置告警

1. 在告警详情界面，点击“处置”。



2. 进入处置界面，可以选择处置方式、处置剧本、处置时限。



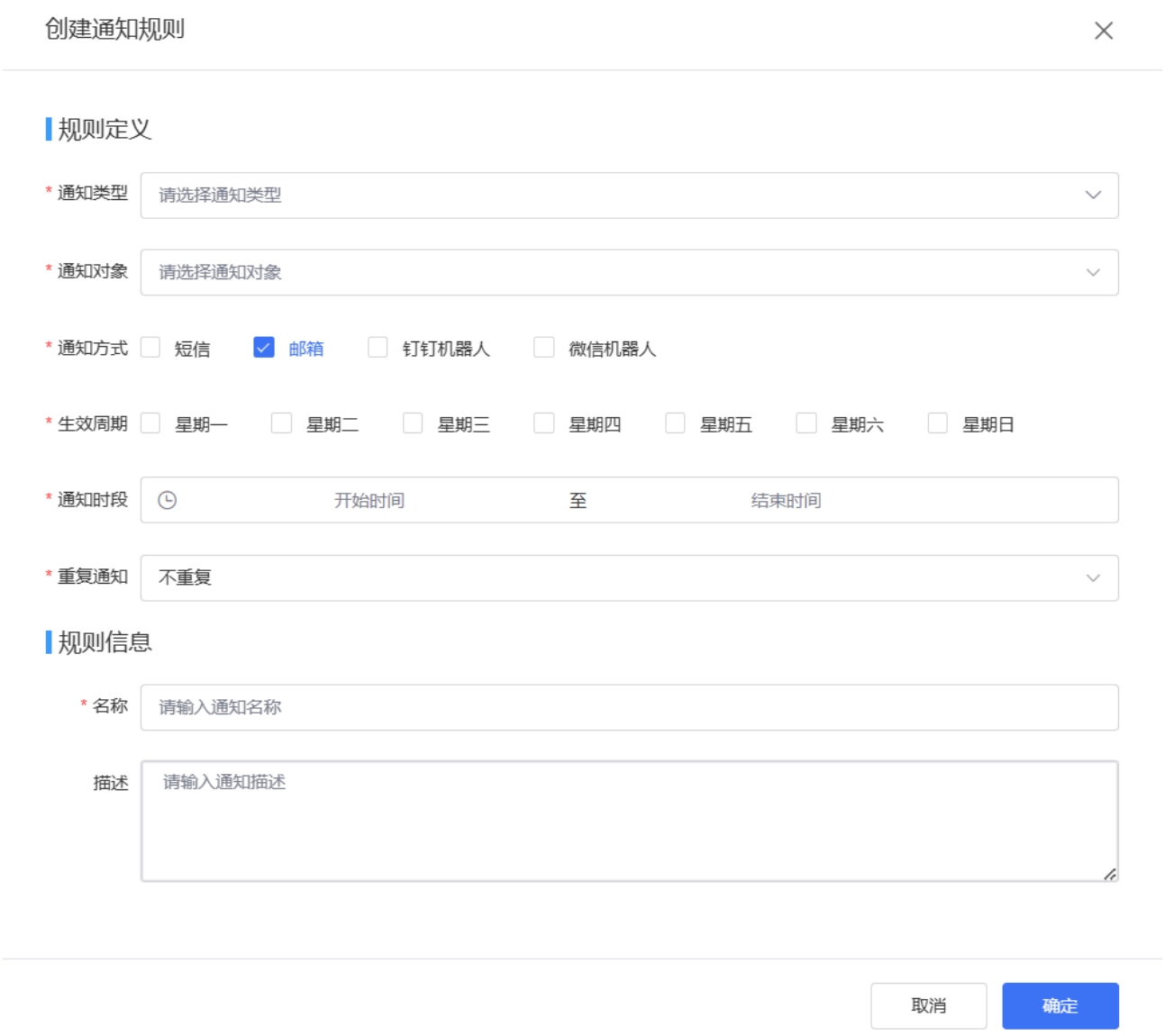
3. 配置完成后，单击“确认”即可完成告警处置。

通知管理

通知规则

创建通知规则

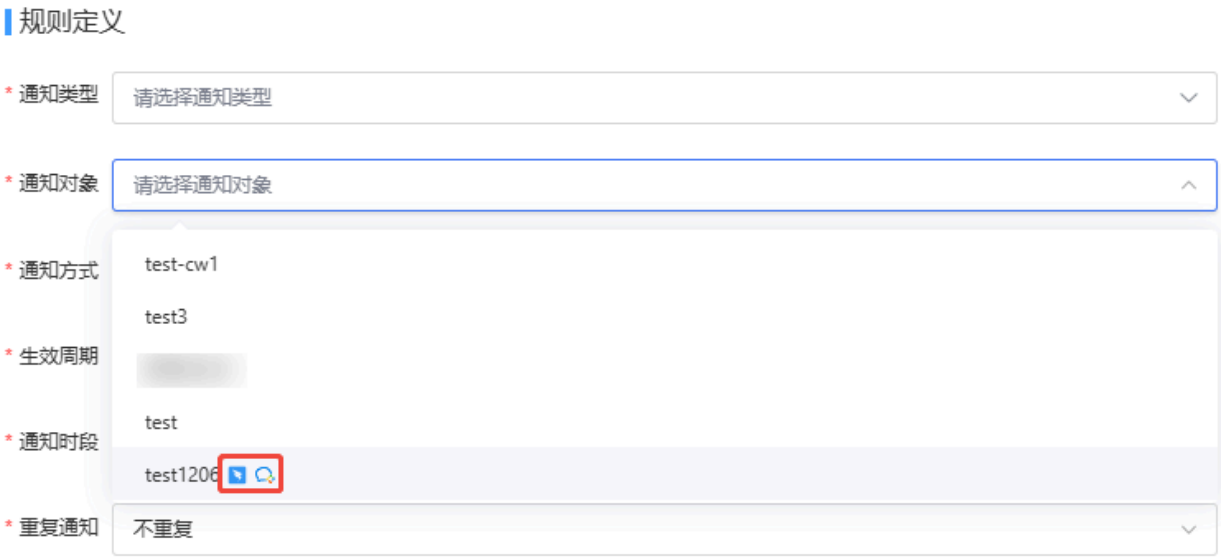
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 通知管理 > 通知规则”，进入通知规则页面。
3. 点击“新建”按钮，弹出创建通知规则窗口。



4. 配置通知规则信息。

> 说明
>
> 只有在生效周期和通知时段产生的告警会进行通知。

参数	说明
通知类型	选择需要通知的告警类型，数据来源于威胁建模中的类型（可多选）。
通知对象	选择通知联系人，数据来源于在通知联系人页面创建的通知联系组（可多选）。

参数	说明
通知	选择告警通知的方式，支持短信、邮箱、钉钉机器人、微信机器人（可多选）。 说明 如果需要向钉钉或微信发送告警的消息，需要先在通知联系组中配置钉钉机器人或微信机器人，详细操作请参见 通知联系组 。 若通知联系组中配置了钉钉机器人与微信机器人，则会显示相应图标，如下所示： 
生效周期	选择需要通知的星期（可多选）。
通知时段	选择需要通知的时间段。
重复通知	配置对于已通知但未及时处置的告警是否采用重复策略进行通知。
规则信息	用于标识特定规则的信息。

5. 配置完成后，单击“确定”，回到通知规则页面，可以看到已创建的通知规则，状态默认为“启用”。

管理通知规则

创建通知规则后，支持对通知规则进行管理，包括启用、停用、编辑、删除操作。



通知联系人

通知联系人由联系人和联系组组成，其中通知联系人需要填写名称、手机号以及邮箱。

通知联系人

新建联系人

1. 点击“新建”，创建联系人。
2. 填写姓名、手机号以及邮箱等信息。

   “是否同时设置为每日告警提醒和每日日报接收的联系人”开关默认打开。关闭则不会收到相关通知。



3. 单击“确定”，完成创建。

配置日志分析量通知接收人和日报接收人

若您未配置日志分析量通知接收人和日报接收人时，页面上方会展示如下横幅通知：



若您需要接收日志分析量不足的通知、接收日报，您可以执行以下步骤创建通知接收人：

1. 登录云安全中心控制台。
2. 单击页面上方横幅通知中的“前往配置”，跳转进入通知联系人页面。
3. 点击“新建”，创建联系人。

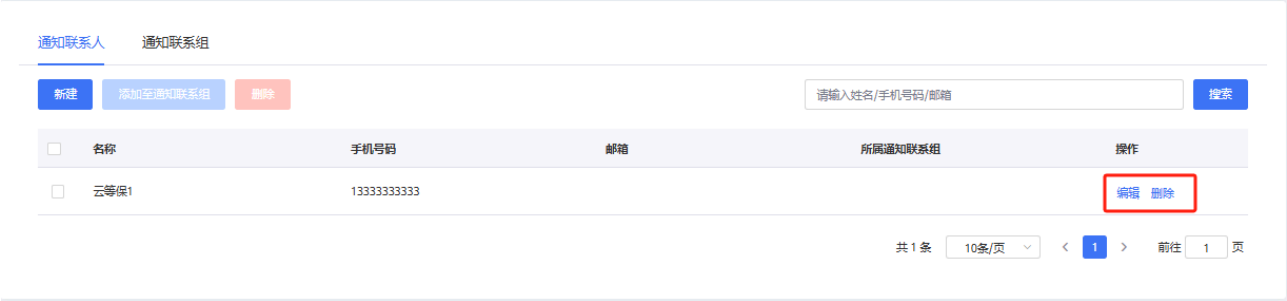
4. 填写姓名、手机号以及邮箱等信息。

   “是否同时设置为每日告警提醒和每日日报接收的联系人”开关默认打开。

5. 单击“确定”，完成创建。

编辑联系人

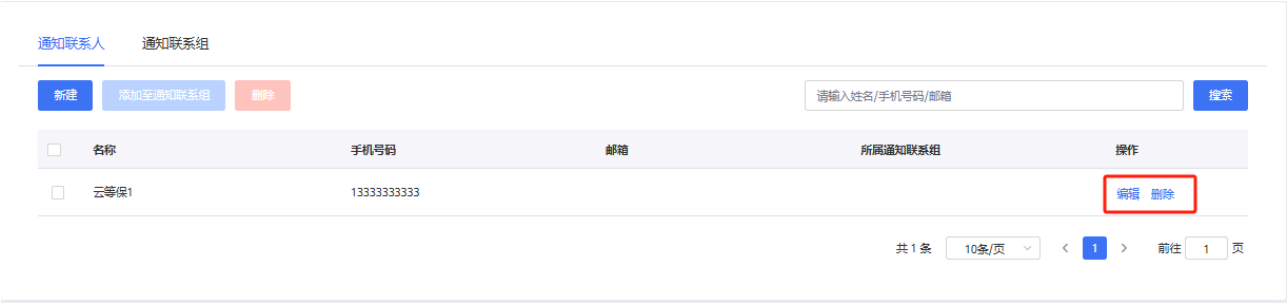
点击“编辑”按钮实现联系人信息的变更。



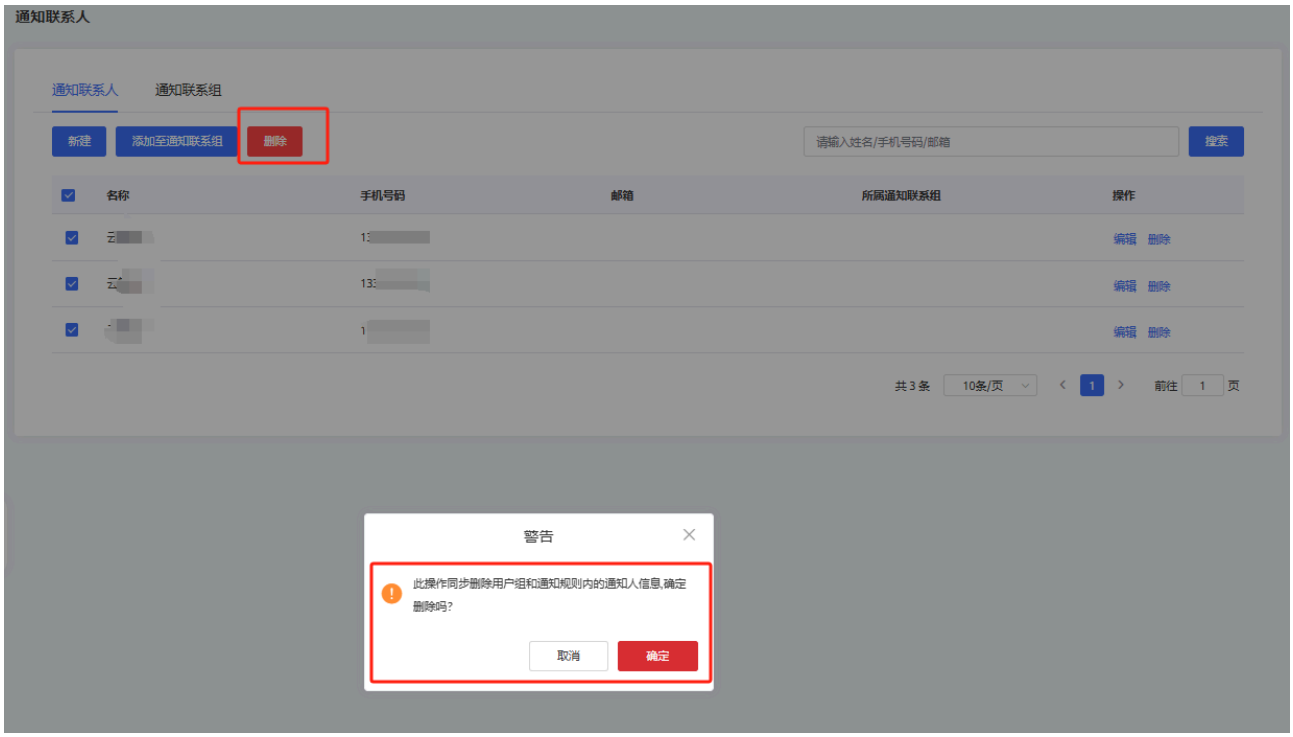
删除联系人

> 注意
>
> 删除联系人会同步删除用户组和通知规则内的通知人信息。

- 单个删除：选择需要删除的联系人，点击删除按钮。



- 多个删除：多选联系人，点击删除按钮。



通知联系组

新建联系组

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 通知管理 > 通知联系人”。
3. 在“通知联系组”页签，单击“新建”，弹出创建联系组窗口。



4. 配置联系组参数。

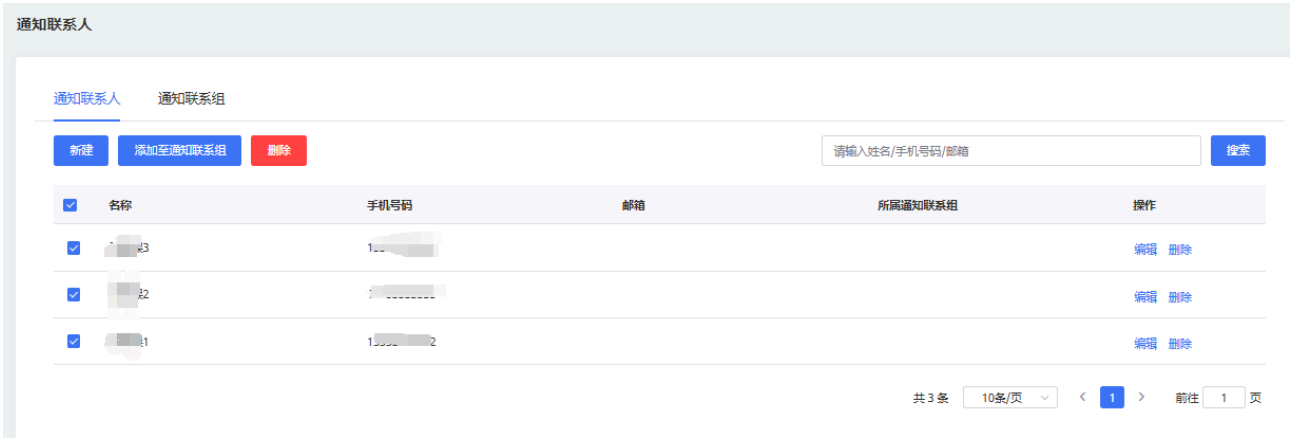
参数	说明
联系组组名	自定义联系组组名。
钉钉机器人	可根据需要开启钉钉机器人。 开启钉钉机器人，需要输入token和secret，获取方式请参见 如何获取钉钉机器人的token和secret？ 。
微信机器人	可根据需要开启微信机器人。 开启微信机器人，需要输入key，获取方式请参见 如何获取企业微信机器人的key？ 。

参数	说明
选择联系人	勾选需要添加到组的联系人，点击向右按钮将待选联系人移动到已选联系人中。 

5. 点击“确定”，完成联系人组的新建。

快捷添加入联系人组

1. 在联系人页面多选联系人。
2. 点击添加至通知联系组。

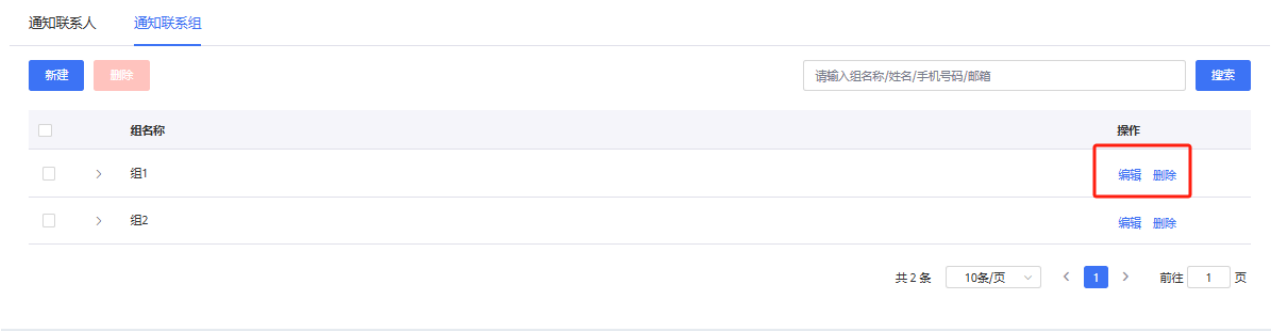


3. 选择需要添加的通知联系组。
4. 点击确定，实现快捷添加。

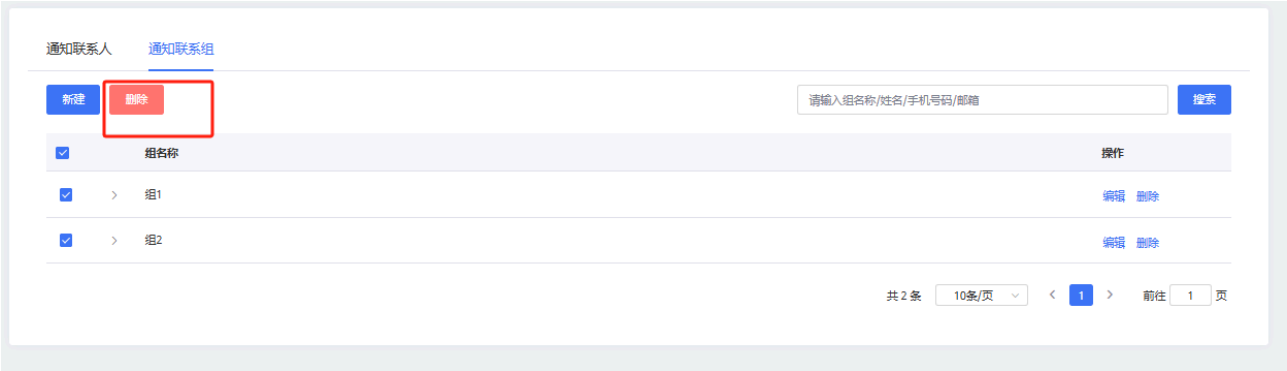
删除联系组

> 说明
>
> 删除联系组不会删除联系人。

- 单个删除：选择需要删除的联系组，点击删除按钮。



- 多个删除：多选需要删除的联系组，点击删除按钮。在弹出的提示框中，单击“确定”。



威胁检测

威胁建模

可以通过关键字、快捷方式、规则类型和标签查询威胁建模规则。

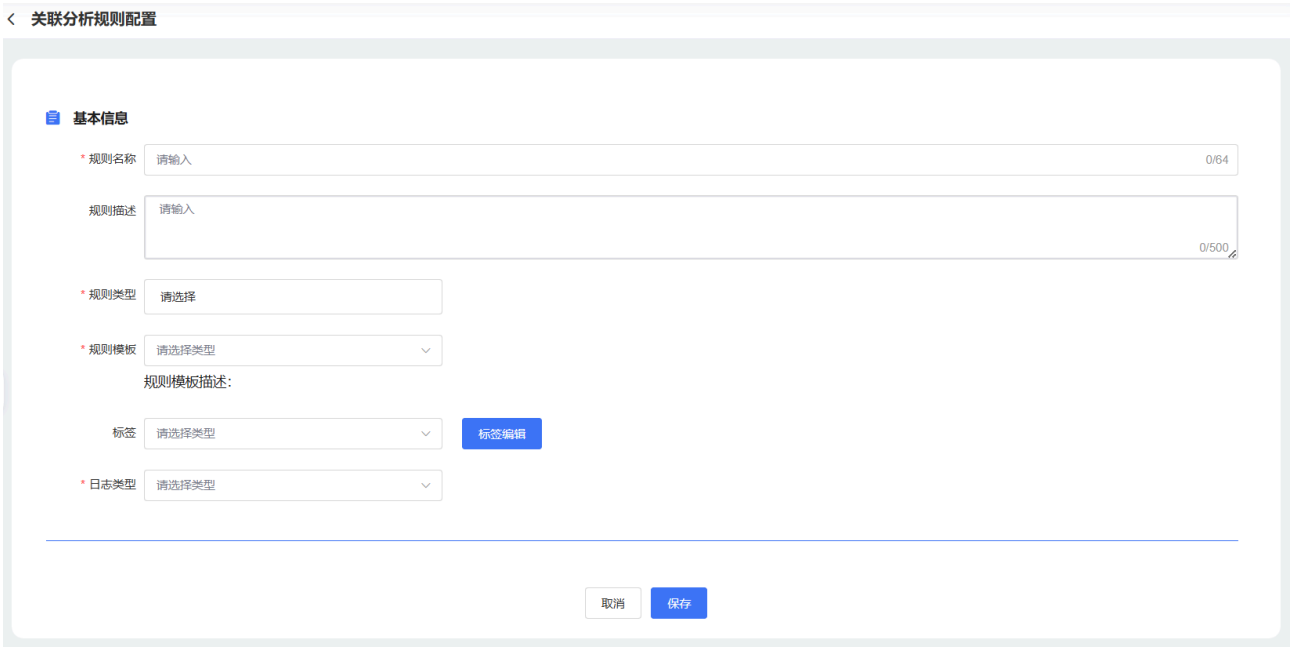
用户初次订购时会复制所有的威胁建模模板，并开启对应的威胁建模规则（如：租户订购了Web应用防火墙原生版，集成配置开启开关，则会开启对应的威胁建模规则）。

新建规则

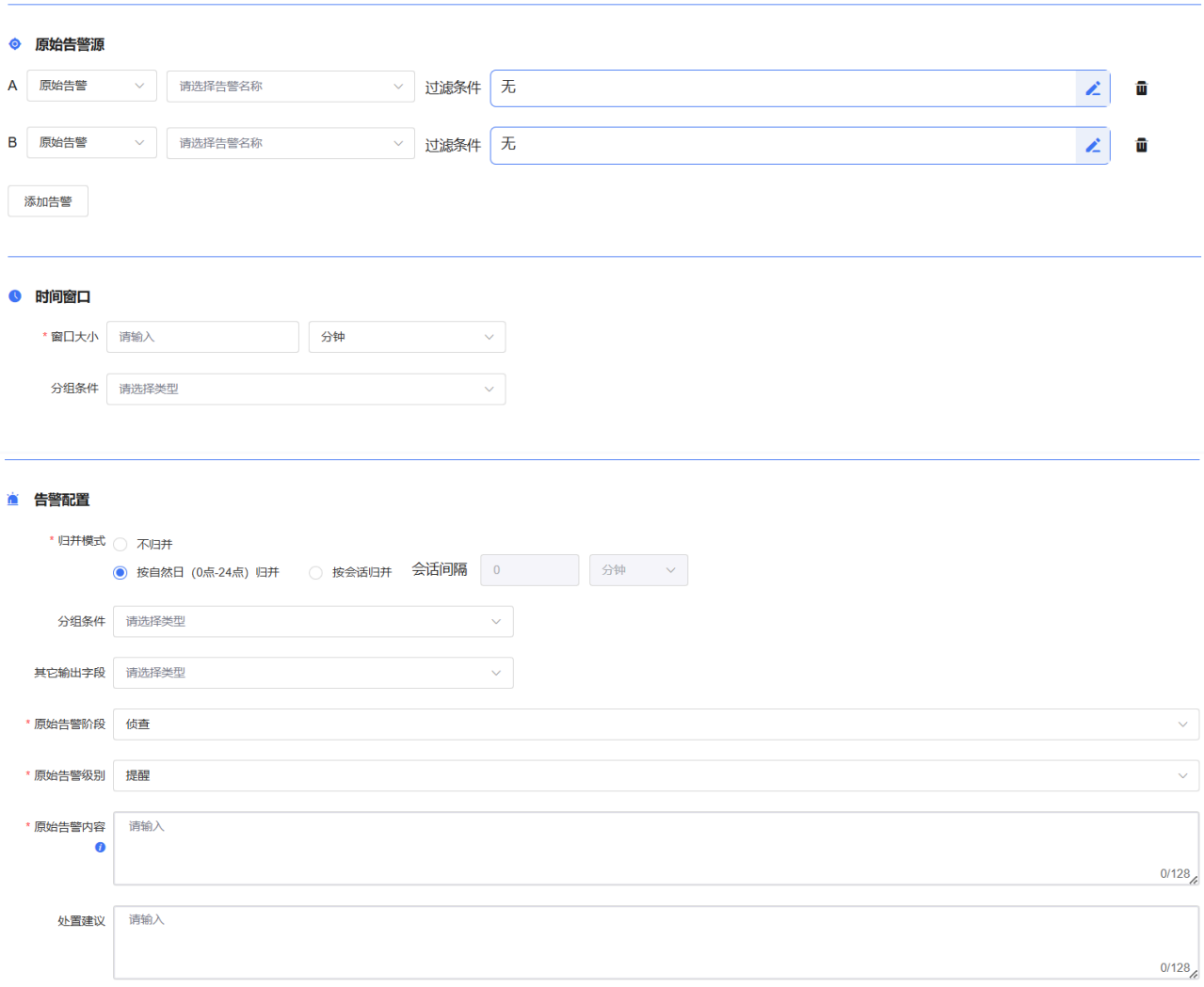
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 威胁检测 > 威胁建模”。
3. 单击“新建”。



4. 基本信息填写，带有*的为必填项。



5. 选择规则类型和规则模板后，还需要配置原始告警源、时间窗口、告警配置等。其中时间窗口需要在2小时以内。

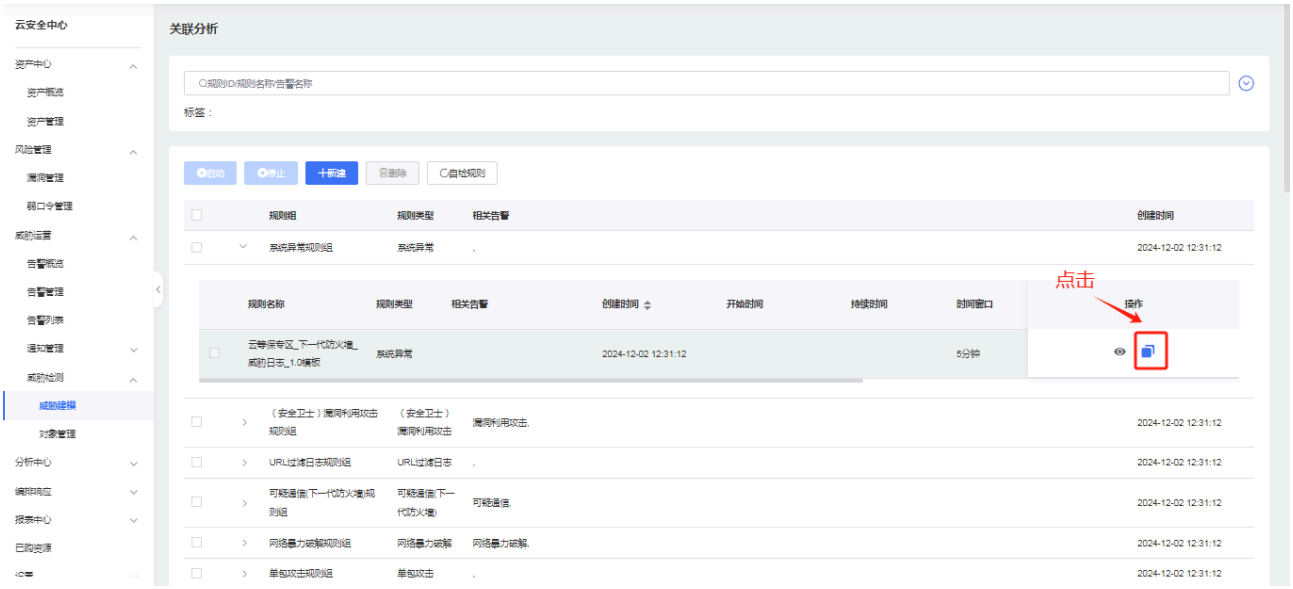


6. 配置完成后，单击“保存”。列表中可以看到新建的规则。



复制规则

1. 选择模板规则或者已经创建好的规则。
2. 点击复制按钮复制规则。



3. 编辑规则信息。
4. 保存规则（规则名称不能相同）。

启动规则

新建规则默认为停止状态，在规则操作列单击启动图标，或勾选规则后，单击列表上方的“启动”，即可启动规则。

停止规则

在规则操作列单击停止图标，或勾选规则后，单击列表上方的“停止”，即可停止规则。

删除规则

注意

启动状态的规则，不允许删除，删除规则前，请先停止规则。

在规则操作列单击删除图标，或勾选规则后，单击列表上方的“删除”，即可删除规则。

自检规则

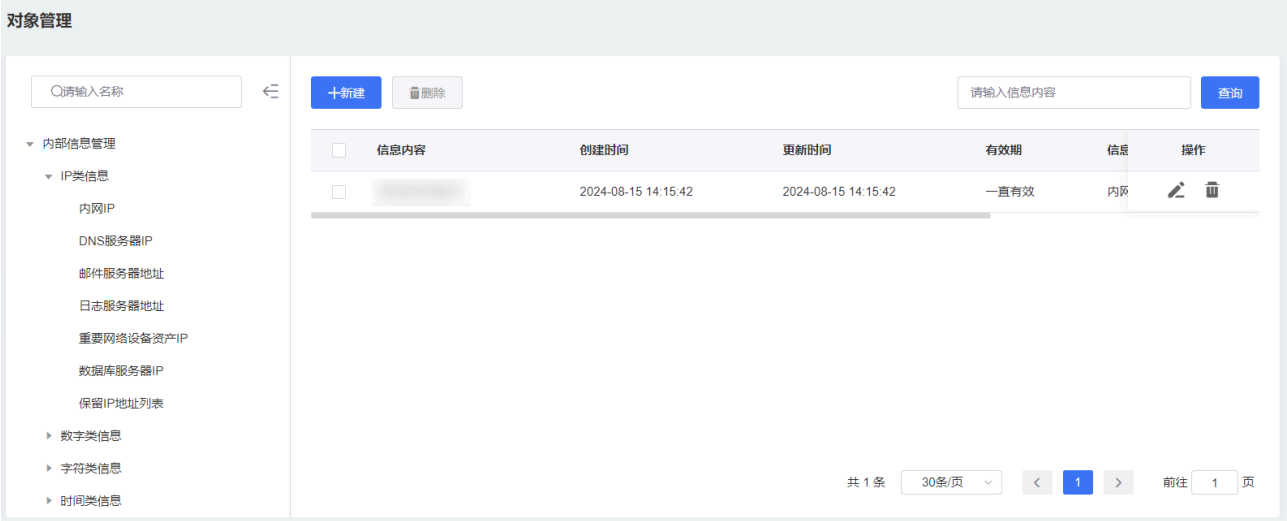
进入规则页面时，系统会自动检测规则的可用性，也可以单击列表上方的“自检规则”，手动检测规则的可用性。

注意

如果日志在集成配置中关闭了自动转告警，则会使对应的规则不生效，不产生告警。

对象管理

展示有价值的内部信息，在关联分析时，对于IP类型、数字类型或字符类型的字段，可以添加过滤条件信息，便于进行分析。通过导入内容包，系统已内置一些信息。



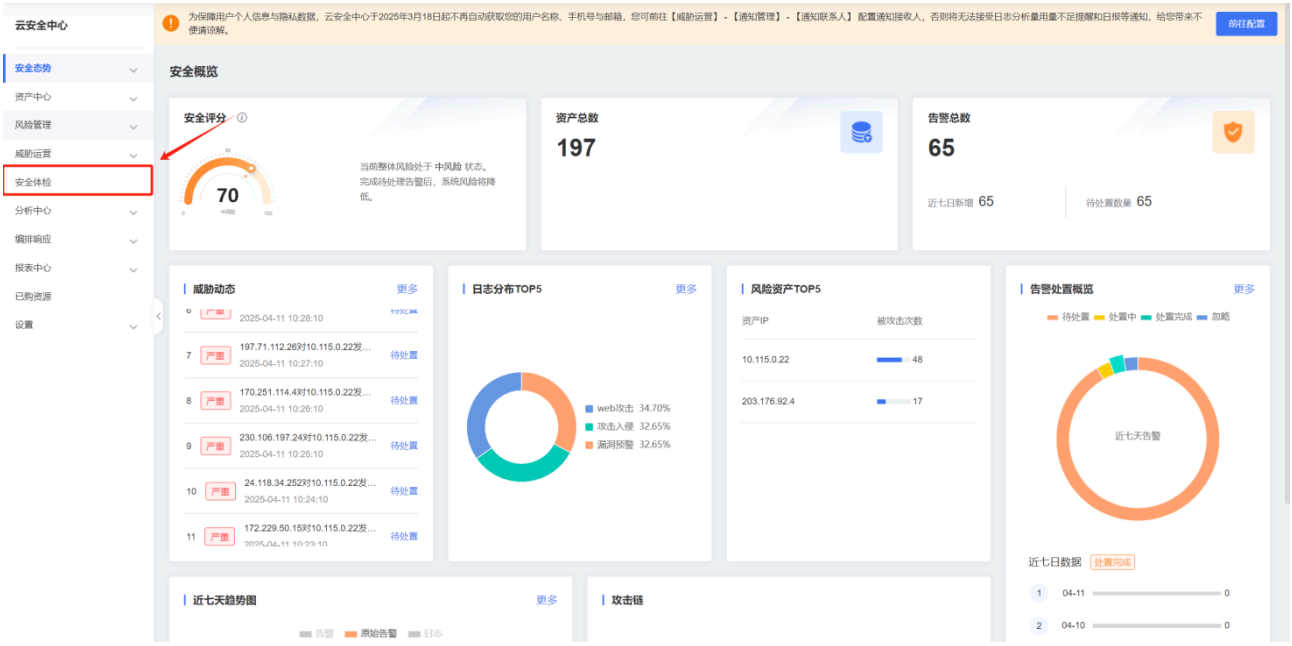
安全体检

云安全中心提供体安全体检产品的功能，可支持的场景包括高危端口开放情况、弱口令、漏洞开放情况，并输出体检报告。用户可根据需求单独购买。

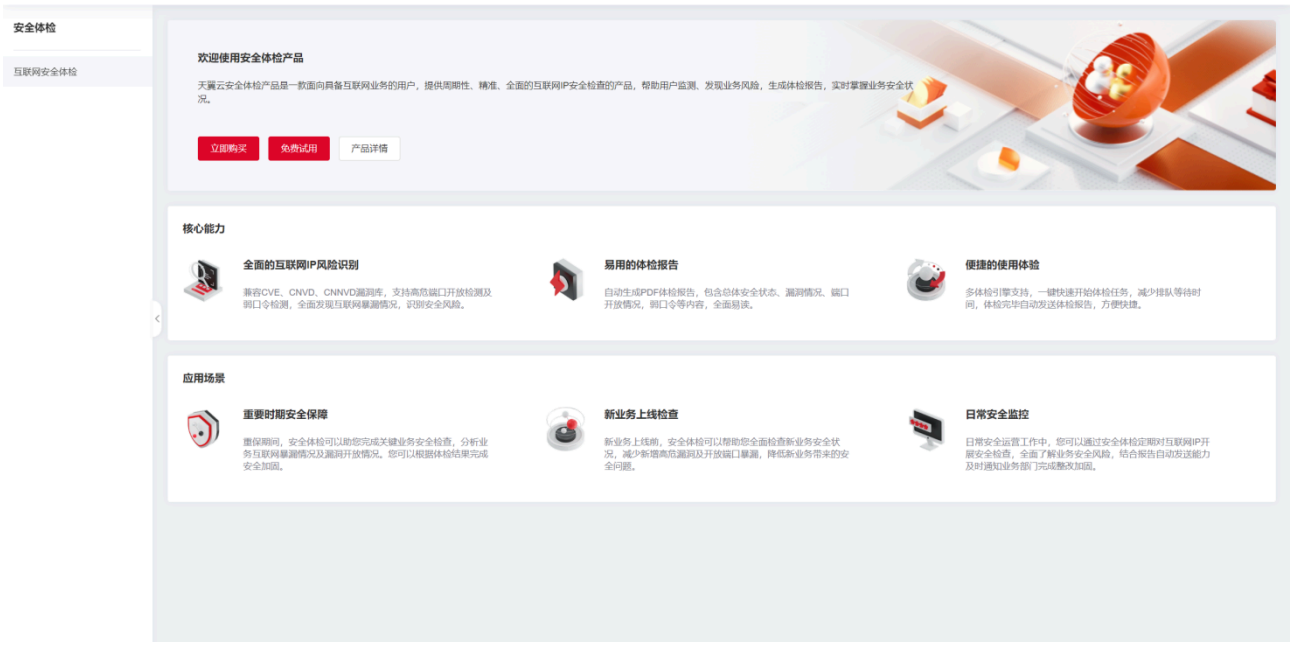
更多信息请参见 安全体检 。

使用安全体检

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在产品服务列表页，选择“安全 > 云安全中心”，进入云安全中心控制台。
4. 在左侧导航栏，选择“安全体检”。



5. 跳转到安全体检控制台，详细操作指导请参见 安全体检产品文档 。



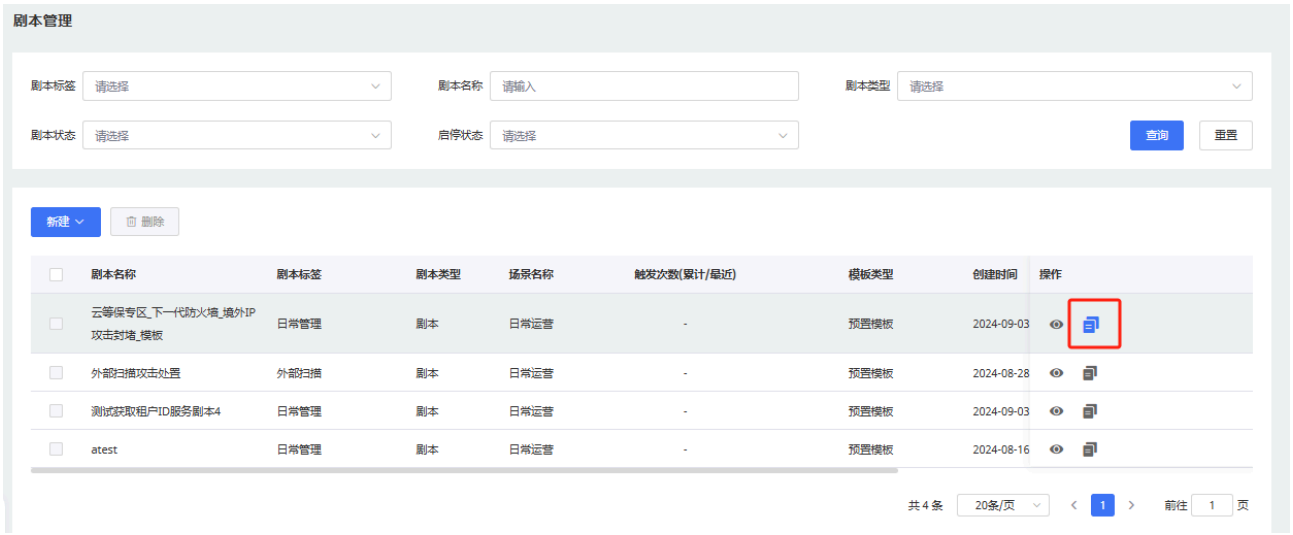
编排响应

剧本管理

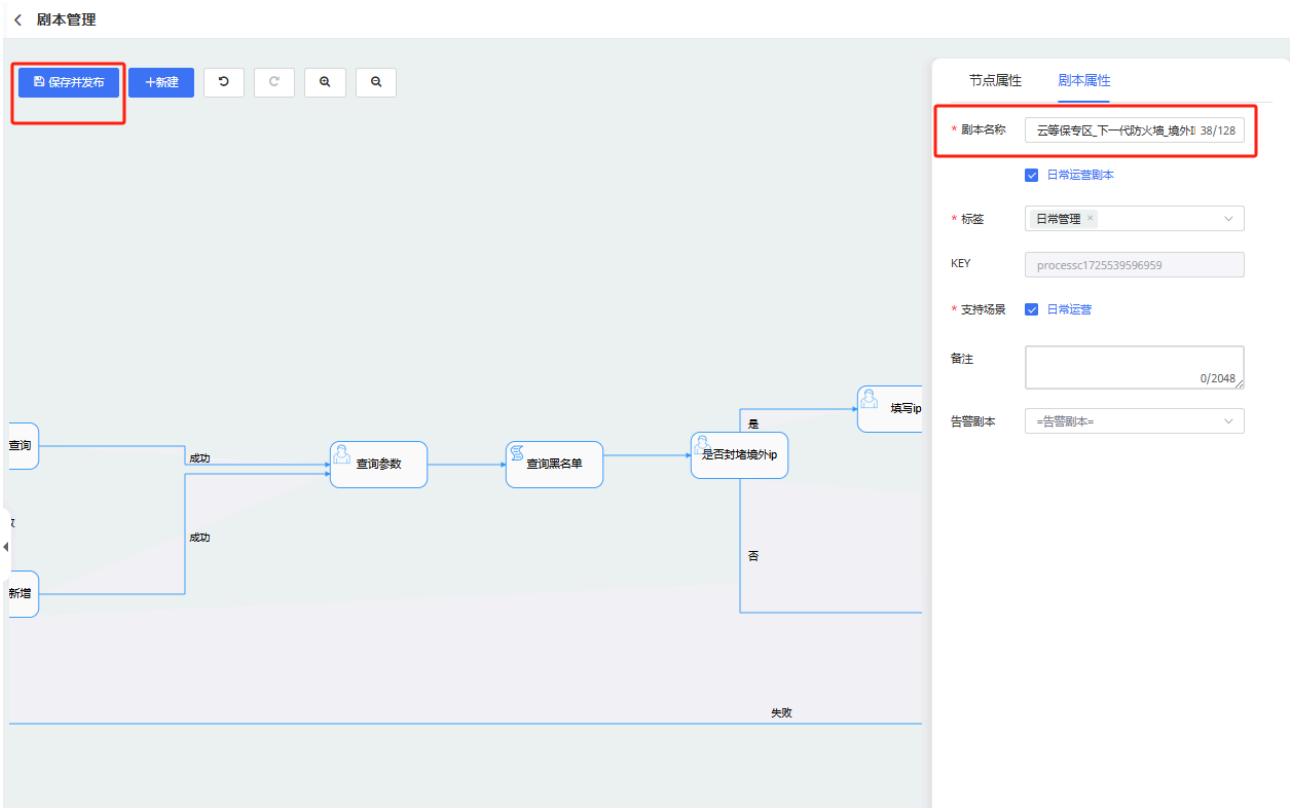
为了提高告警处置的自动化程度及效率，提高告警解决方案的复用性。可以使用剧本将某些处置操作模板化、程序化。在类似告警发生时，可以自动规则匹配或人工选择相关剧本进行自动化的处置。其中的剧本匹配规则，则用于告警发生后，自动匹配并调用剧本进行操作。剧本管理模块则用于对这些剧本和剧本匹配规则进行统一管理。剧本管理的的剧本列表，可以查看、导出相关的剧本。

复制剧本

1. 选择已经创建好的剧本。
2. 点击复制按钮。



3. 编辑剧本信息，确保剧本名称不重复。



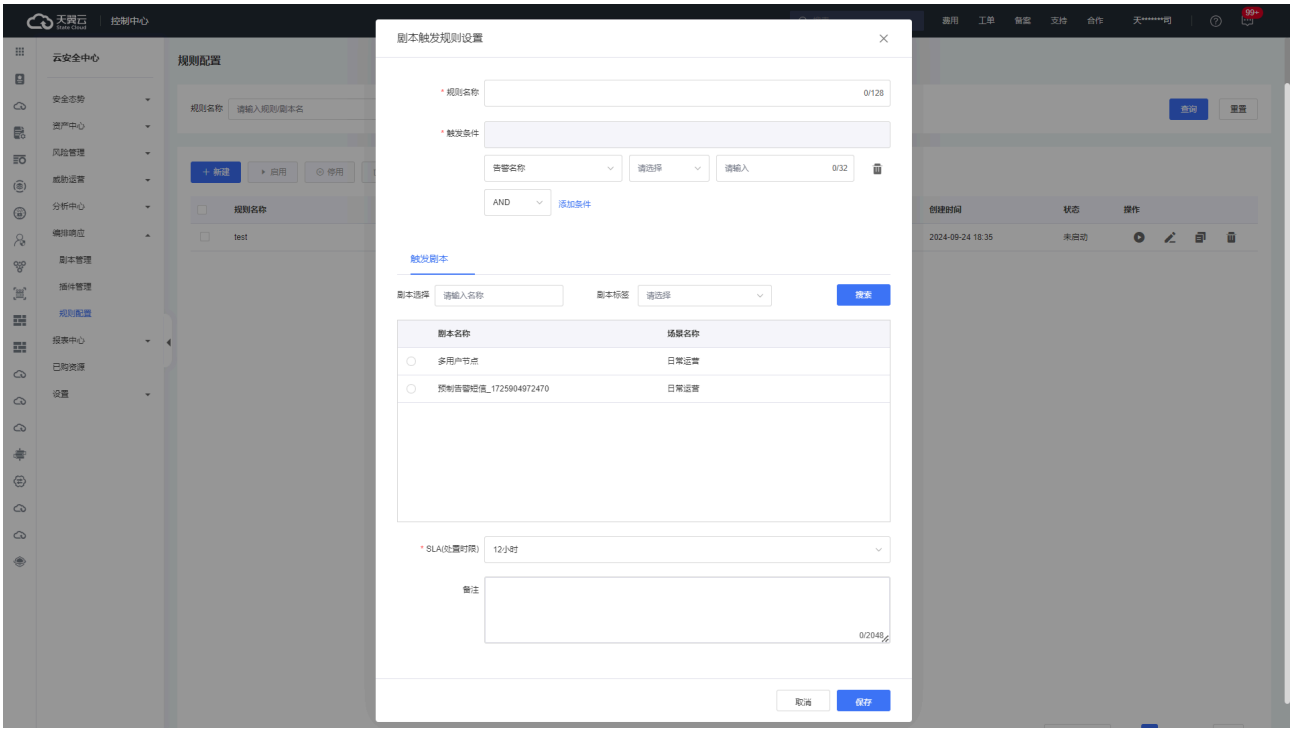
4. 点击保存并发布，完成剧本复制。

规则配置

规则配置模块可以进行规则的新建、查找、启动、暂停、查看与删除。

新建规则

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“编排响应 > 规则配置”，进入规则配置页面。
3. 点击“新建”，新建剧本触发规则。填写规则名称，以及剧本触发条件，再勾选相关剧本即可。



启动规则

规则新建完成后，默认为“未启动”，单击操作列的启动图标，启动规则。



报表中心

报表任务

报表任务功能，实现管理和维护报表任务，用户可以自定义报表的生成周期，每个用户需要自行管理自己的报表任务。

说明

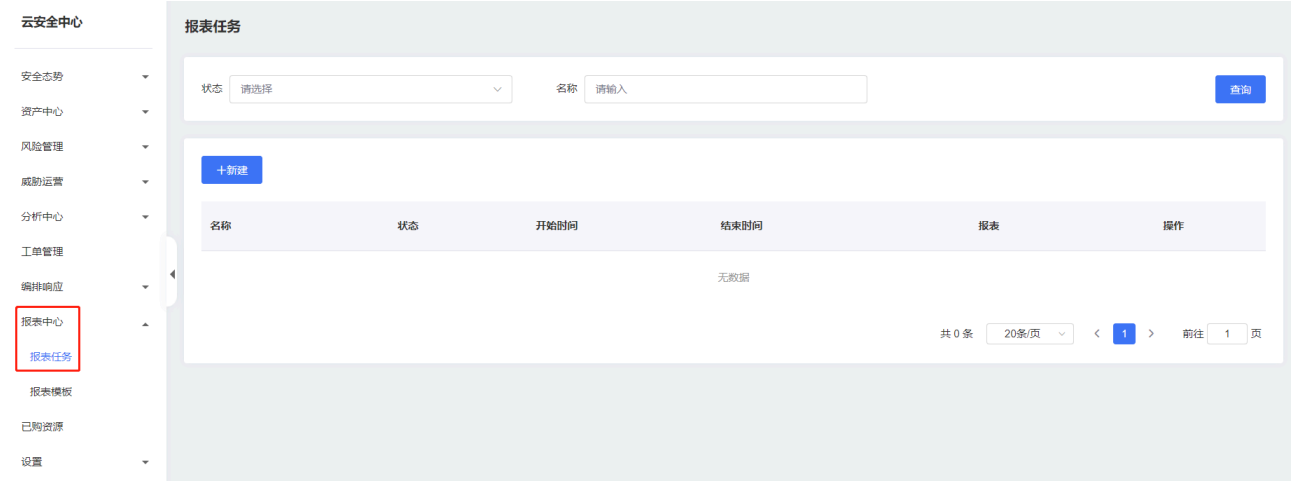
周期报表任务执行时发送报表短信到用户在系统配置的手机号。

前提条件

已创建报表模板。

新建报表任务

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“报表中心 > 报表任务”。



3. 单击“新建”，弹出新建报表任务对话框。填写报表名称、选择报表模板、选择报表类型（支持即时报表任务、周期报表任务）。



4. 配置完成后，单击“保存”。

管理报表任务

- 启动周期性任务

  在周期性报表任务的操作列，单击“立即启动”图标。（周期性报表任务最多启动10个任务）



- 编辑报表任务

  在周期性报表任务的操作列，单击“编辑”图标。报表名称不支持修改，其余参数均可修改。



查看报表

单击如下图标，查看已生成的报表列表。并支持下载报表到本地。



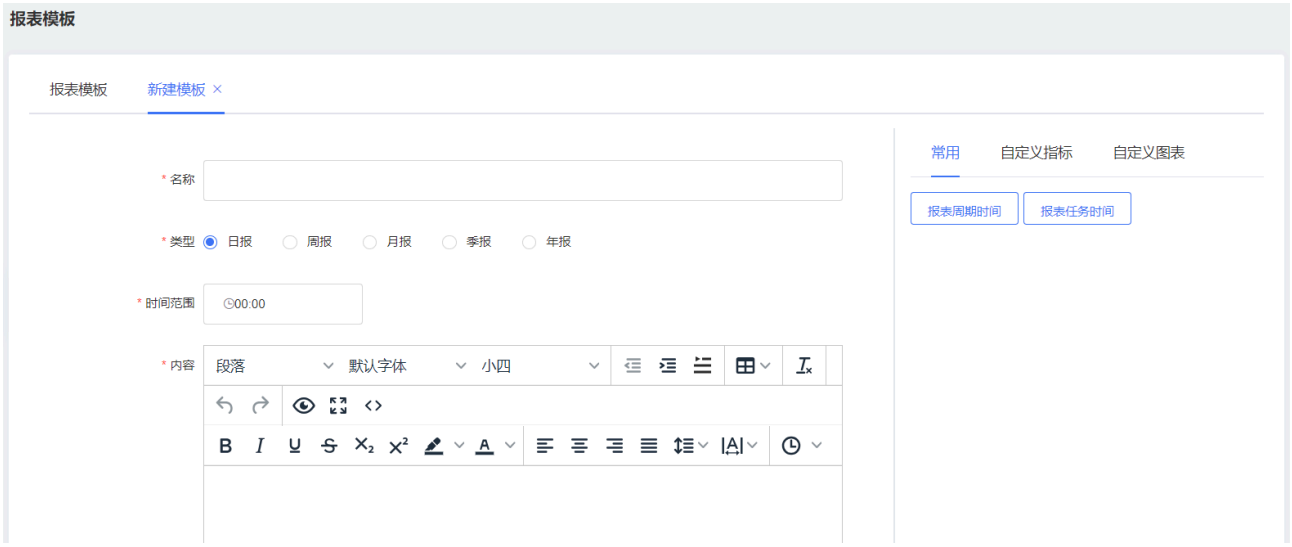
报表模板

报表模板，维护和定义报表模板，用户可以自定义报表的模版，每个用户需要自行管理自己的报表模版。

支持自定义指标、自定义图表以及报表预览等功能。

新建模板

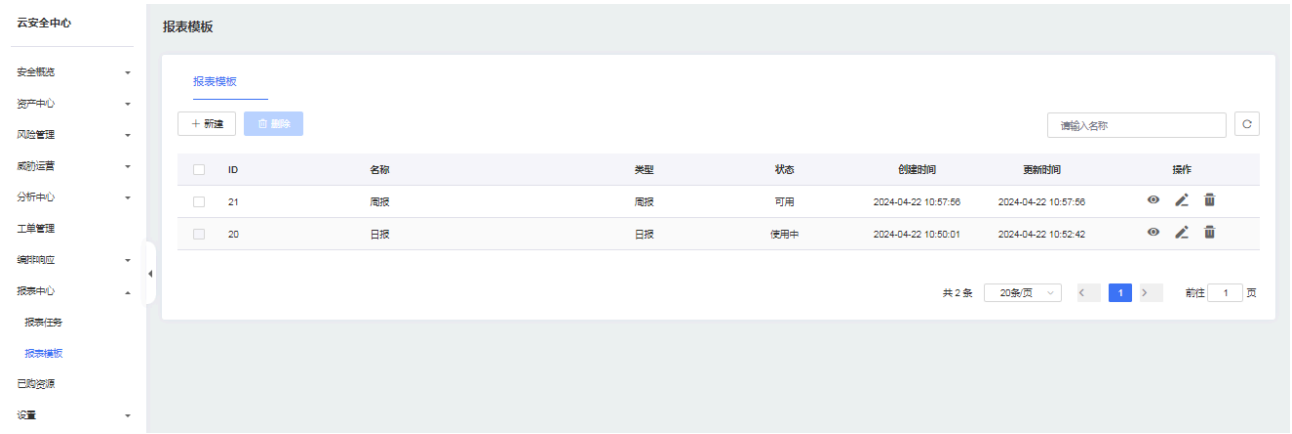
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“报表中心 > 报表模板”。
3. 单击“新建”，进入新建模板页面。



4. 配置模板名称、类型、时间范围和报表内容。

   其中类型指定的时间为报表自定义指标的默认数据周期时间（当自定义指标中指定了绝对时间后，会覆盖默认数据周期时间）。

5. 单击“保存”，保存模板。

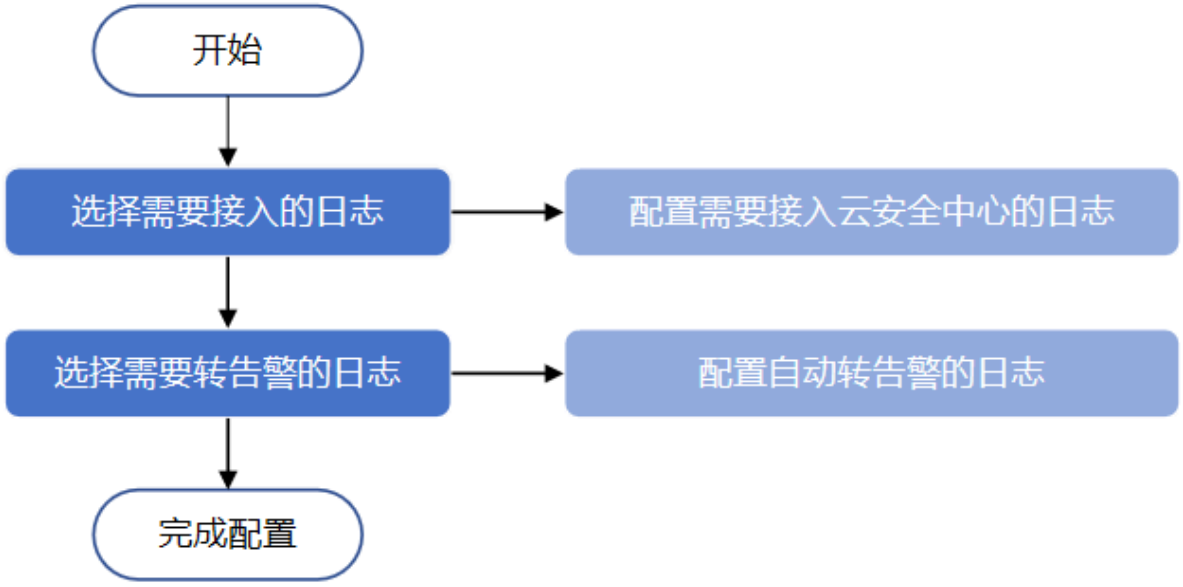


设置

集成配置

开通云安全中心实例后，系统默认会接入部分日志数据并对用户进行初始化配置。您可以根据自己的业务特性修改初始化配置。

打开云安全中心的“设置>集成配置”，在集成配置中选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。



支持的日志类型

产品	日志类型
云堡垒机（原生版）企业版	云堡垒机（原生版）资产登录
	云堡垒机（原生版）资产登出
	云堡垒机（原生版）剪切板操作
	云堡垒机（原生版）字符命令
	云堡垒机（原生版）文件操作
	云堡垒机（原生版）键盘操作
	云堡垒机（原生版）平台登录
	云堡垒机（原生版）平台登出
	云堡垒机（原生版）平台操作
	云堡垒机（原生版）数据库操作
服务器安全卫士（原生版）	服务器安全卫士（原生版）漏洞信息
	服务器安全卫士（原生版）弱口令
	服务器安全卫士（原生版）告警日志
数据库审计	数据库审计告警日志
云等保专区v1.0	云等保专区数据库审计
	云等保专区主机安全
	云等保专区下一代防火墙
	云等保专区堡垒机
	云等保专区Web应用防火墙
Web应用防火墙（原生版）	Web应用防火墙（原生版）告警日志

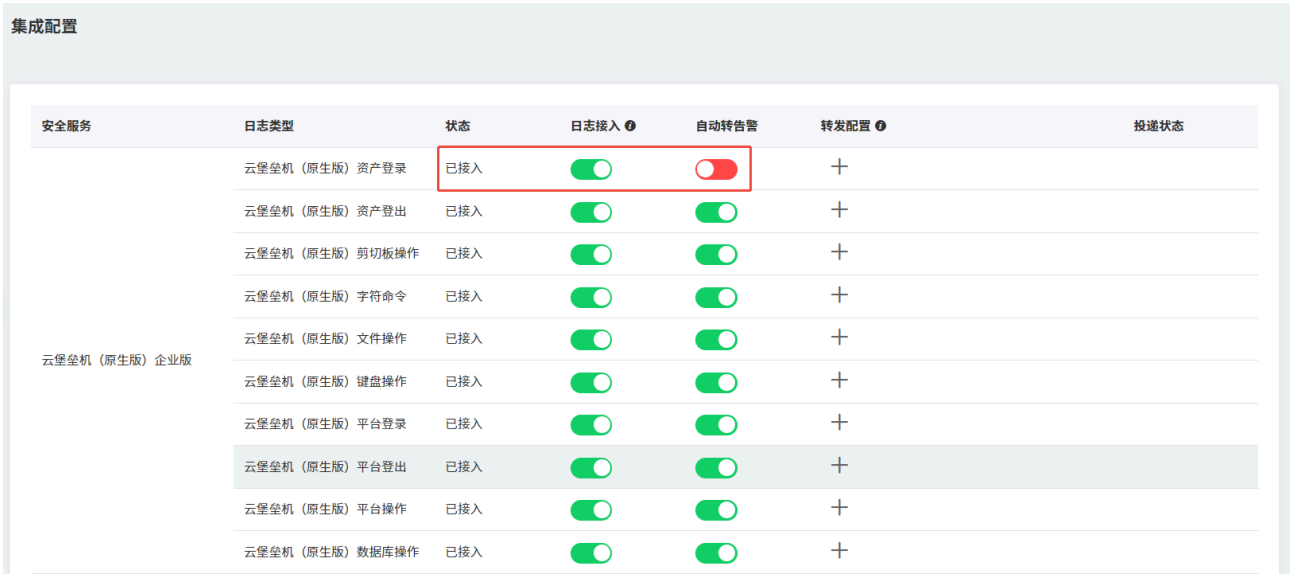
产品	日志类型
云防火墙（原生版）	云防火墙（原生版）威胁日志

前提条件

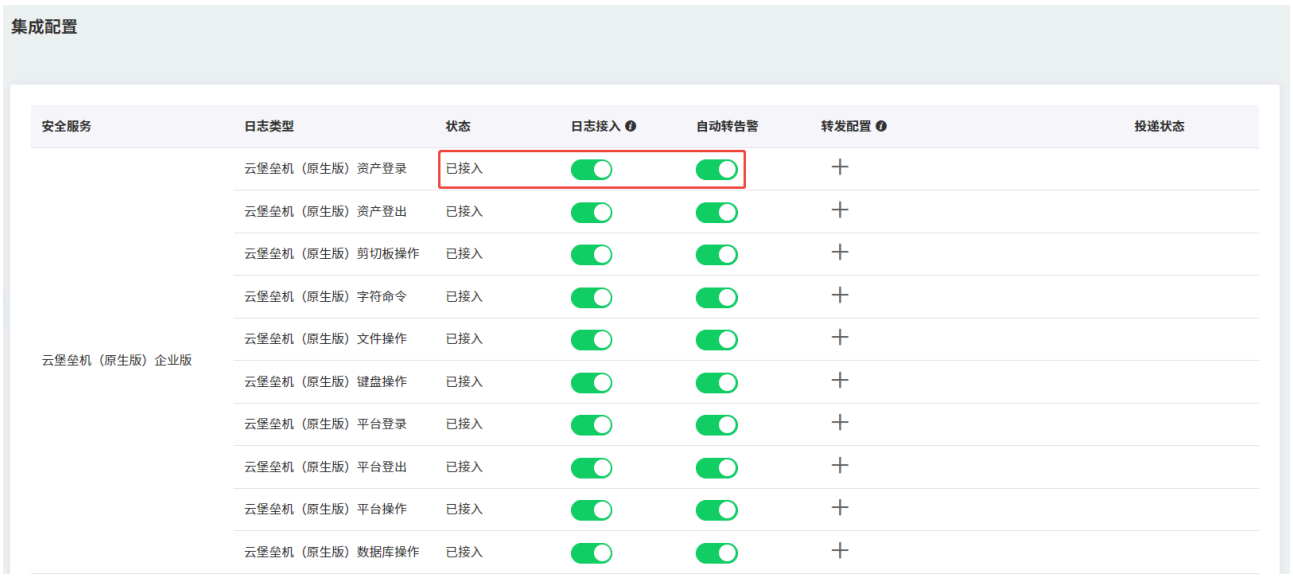
需确保要接入日志的数据源监控处于启用状态。具体操作请参见 数据源监控 。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“设置 > 集成配置”，打开数据集成配置页面。
3. 选择需要接入的日志，并打开日志接入开关。



4. 选择需要转告警的日志，并打开自动转告警的开关。



说明

- 需要先在数据源监控页面启用开关后，才可以在集成配置页面中开启日志和告警配置。
- 系统默认会接入部分日志，用户如有需要，可以自行关闭。
- 选择需要接入的日志时，只能针对您已经购买的云产品。
- 选择需要转告警的日志，只能针对已经选择接入的日志进行。
- 自动转告警打开，对应的日志类型才能产生告警。

5. 云安全中心已支持通过Kafka将日志、告警外发至第三方。选择需要外发的日志类型，并打开配置开关。具体操作请见 日志、告警外发设置 。

数据源监控

在数据源监控中可以查看到已经接入到系统的数据源。可以直接通过开关对数据源进行开启或关闭，云安全中心会根据您的操作对数据源数据进行收取或拒绝收取。

注意事项

选择需要接入的数据源时，只能针对您已经购买的云产品。

启用数据源

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“设置 > 数据源监控”，打开数据源监控页面。
3. 选择需要接入的数据源，在操作列单击启用图标，启用数据源。



停止数据源

注意

停止数据源后，对应的“集成配置”将不允许操作。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“设置 > 数据源监控”，打开数据源监控页面。
3. 选择需要停止的数据源，在操作列单击停止图标，停止数据源。



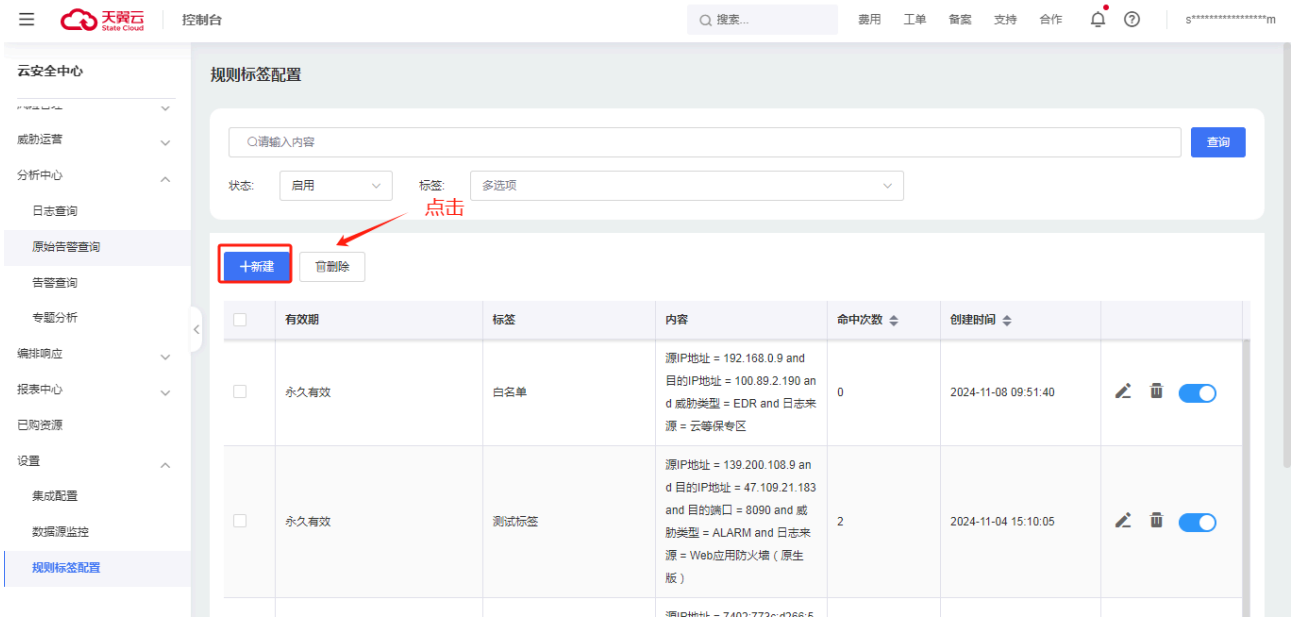
规则标签配置

云安全中心的规则标签功能，提供白名单及自定义的规则标签，用户可设置需要打标签的日志筛选范围，并赋予其白名单或自定义的标签。

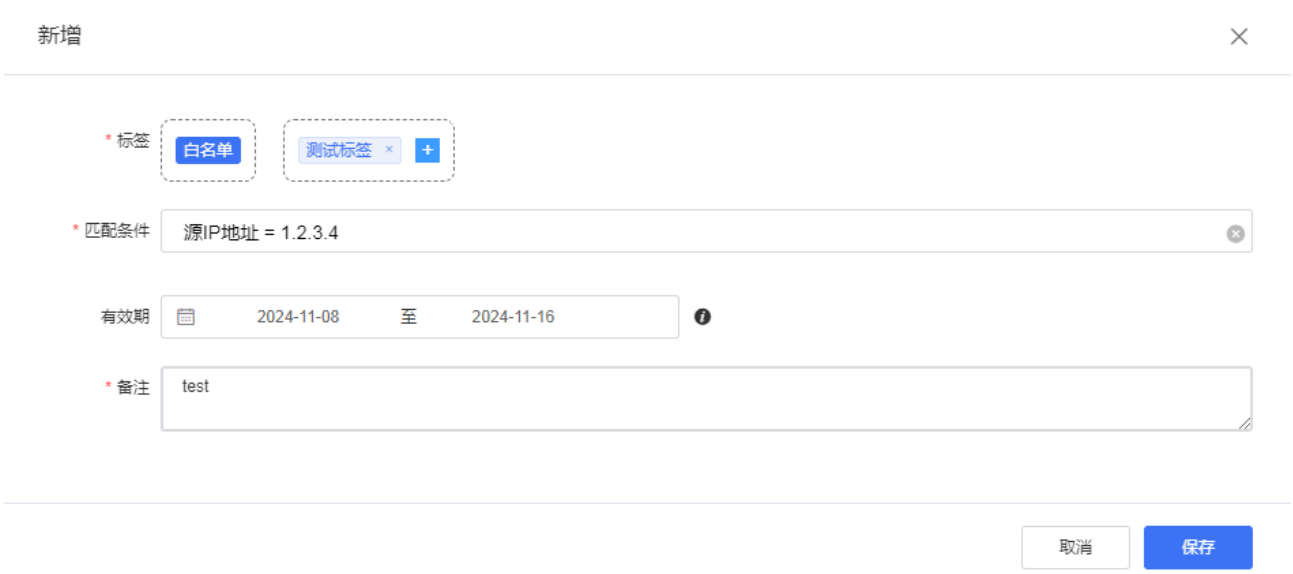
- 白名单标签：当日志解析出的内容匹配到了白名单标签规则，日志则会被标记为白名单，对应日志将不会产生告警。
- 自定义标签：当日志解析出的内容匹配到了自定义标签规则，日志则会被标记为自定义标签，仍然会产生告警。

新增标签规则

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“设置 > 规则标签配置”，单击“新建”。



3. 在弹出的新增窗口中，配置标签、匹配条件、有效期、备注信息。
   - 标签：支持选择一个或多个标签。
     - 标签设置为白名单时，当日志解析出的内容匹配到了标签规则，日志则会被标记为白名单，对应日志将不会生成告警。
     - 标签设置为自定义标签时，当日志解析出的内容匹配到了标签规则，日志则会被标记为自定义标签，不影响告警产生。
     - 标签同时设置了白名单标签和自定义标签时，当日志解析出的内容匹配到了标签规则，日志则会被标记为白名单+自定义标签，对应日志将不会生成告警。
   - 匹配条件：配置日志内容需要匹配的条件。
   - 有效期：标签规则仅在有效期内生效。若不配置，则永久有效。



4. 参数配置完成后，单击“保存”，回到规则标签配置页面。

启用/停止标签规则

- 启用标签规则，规则生效，日志匹配标签规则。

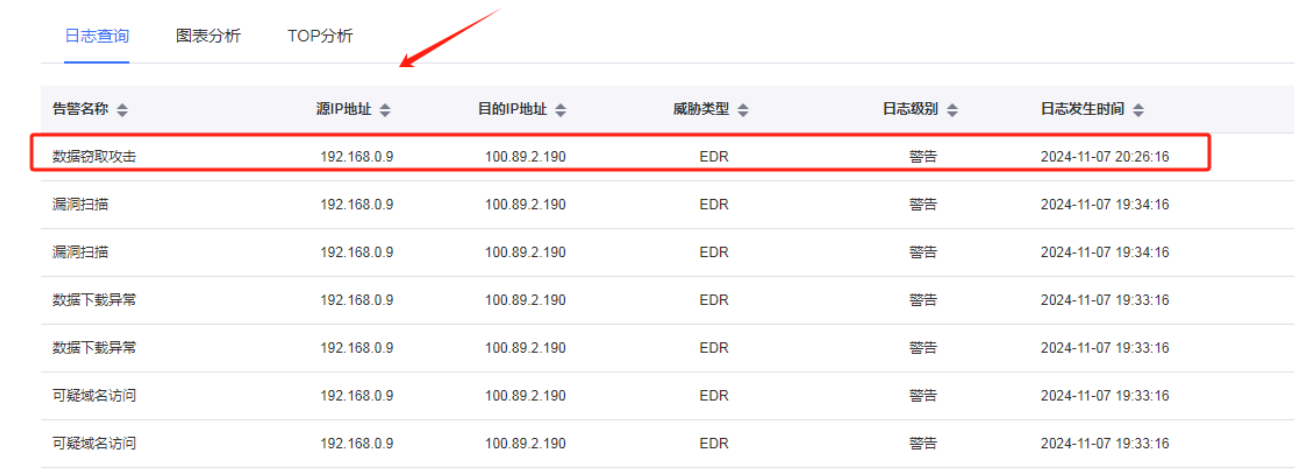


- 停用标签规则，规则失效，日志不匹配标签规则。



从日志添加标签规则

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“设置 > 规则标签配置”。
3. 在日志查询列表找到需要添加标签的日志，点击日志。



4. 在日志详情页，单击白名单按钮。



5. 在弹出的新增窗口中，配置标签、匹配条件、有效期、备注信息。参数配置完成后，单击“保存”。



查看日志的标签

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“设置 > 规则标签配置”。
3. 在日志查询列表的“规则标签”列，可以查看日志的标签。



4. 在日志查询列表找目标日志，点击日志。
5. 在日志详情页的基本信息中，可以看到“规则标签”。



查看审计事件

支持审计的操作列表

事件名称	读写类型
资产管理-资产导入模板下载	写类型
资产管理-资产导入	写类型
告警管理-工单处置-小结-上传文件	写类型
资产管理-资产导出	读类型

事件名称	读写类型
分析中心-图表分析-导出	读类型
告警管理-工单处置-小结-下载文件	读类型

查看云审计事件

1. 登录云审计产品控制台，默认进入云审计事件列表页面。
2. 事件来源选择“安全”，资源类型选择“云安全中心”，单击“查询”，筛选云安全中心事件。



3. 在需要查看的事件左侧，单击 展开该事件的详细信息。



4. 在需要查看的事件右侧，单击操作列的“查看详情”，弹出一个窗口显示该操作事件结构的详细信息。

   关于事件详情中字段详解，请参见 审计服务事件参考 。

事件详情


```
{
    "id": "d7ef06dfd34a4a6a8e26f701e660e5ca",
    "eventName": "资产管理-资产导入模板下载",
    "eventTime": "2025-03-03T17:17:57.570",
    "eventLevel": {
        "code": "null",
        "value": "
    },
    "eventType": {
        "code": "0",
        "value": "API调用事件（ApiCall）"
    },
    "eventActType": {
        "code": "1",
        "value": "写类型"
    },
    "srcRegion": "all",
    "srcServiceType": "安全",
    "srcProdTypeName": "云安全中心",
    "srcProdName": "云安全中心",
    "userId": "
    "accountId": "
    "reqData": "/business/assetManage/templateDownload",
    "createTime": "2025-03-03T17:17:57.739",
    "updateTime": "2025-03-03T17:17:57.739",
    "subUserEmail": "
}
```

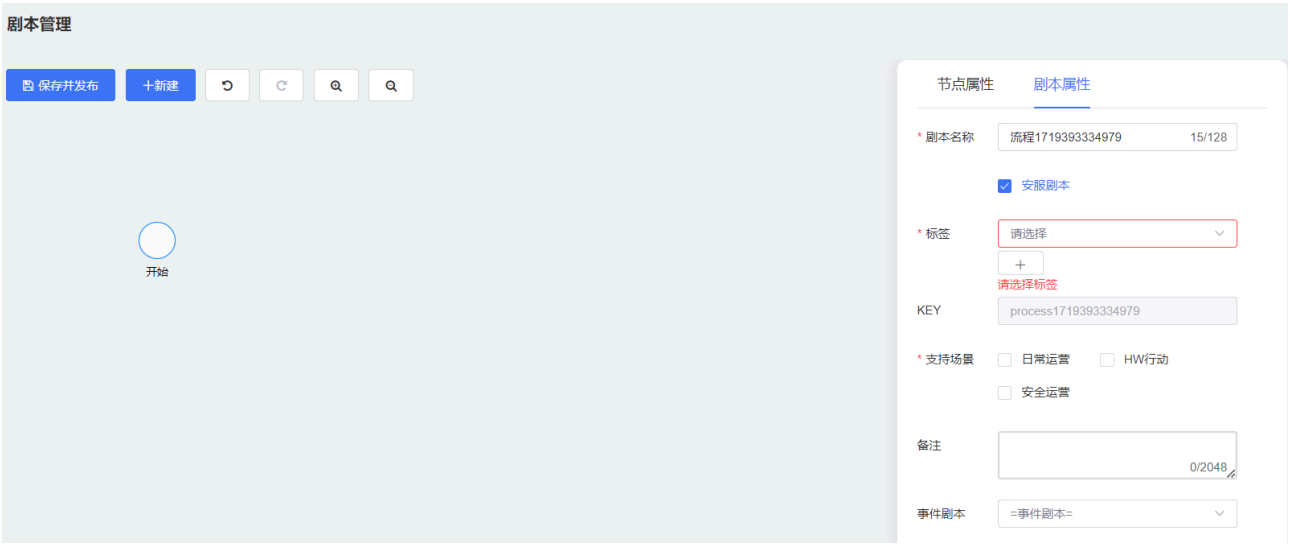
最佳实践

如何进行剧本管理

为了提高告警处置的自动化程度及效率，提高告警解决方案的复用性。可以使用剧本将某些处置操作模板化，程序化。在类似告警发生时，可以自动规则匹配或人工选择相关剧本进行自动化的处置。其中的剧本匹配规则，则用于告警发生后，自动匹配并调用剧本进行操作。剧本管理模块则用于对这些剧本和剧本匹配规则进行统一管理。剧本管理的的剧本列表，可以查看、新建、编辑、导入导出相关的剧本。

新建剧本

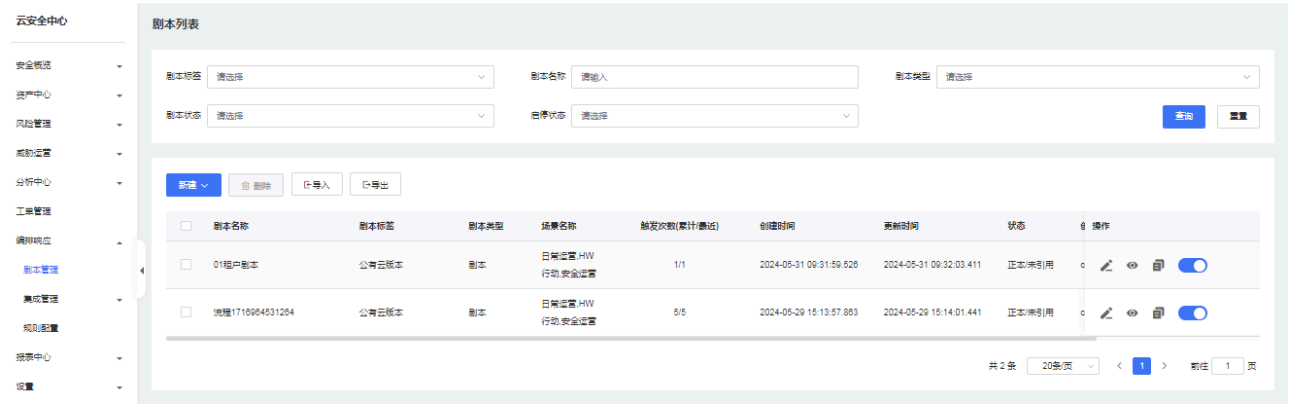
打开剧本管理的剧本列表界面，点击“新建”，创建一个只有一个开始节点的新剧本。剧本新增页面右侧可对剧本属性进行编辑。



说明

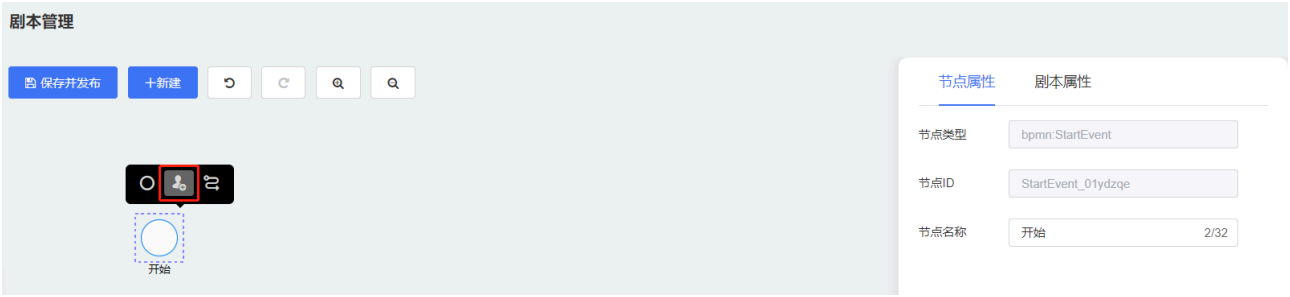
- 一个剧本有且只有一个开始节点和结束节点。
- 每个用户在新增的剧本编辑界面停留过长时，会最多保留一份新增草稿，在用户下次新增时会提示是否进入草稿。
- 在对已存在剧本进行修改时，若在修改页面停留时间过长，会自动为改剧本保留一份草稿，在下次重新对剧本进行编辑时提示是否进入草稿。
- 剧本保存时会对剧本进行校验，若该剧本存在不能到达或不能结束的孤立节点，需用户完善后才能保存。后续版本将会升级启停功能，非正常剧本允许保存，不允许启用。

新建完成后，可以在列表中看到新建的剧本。

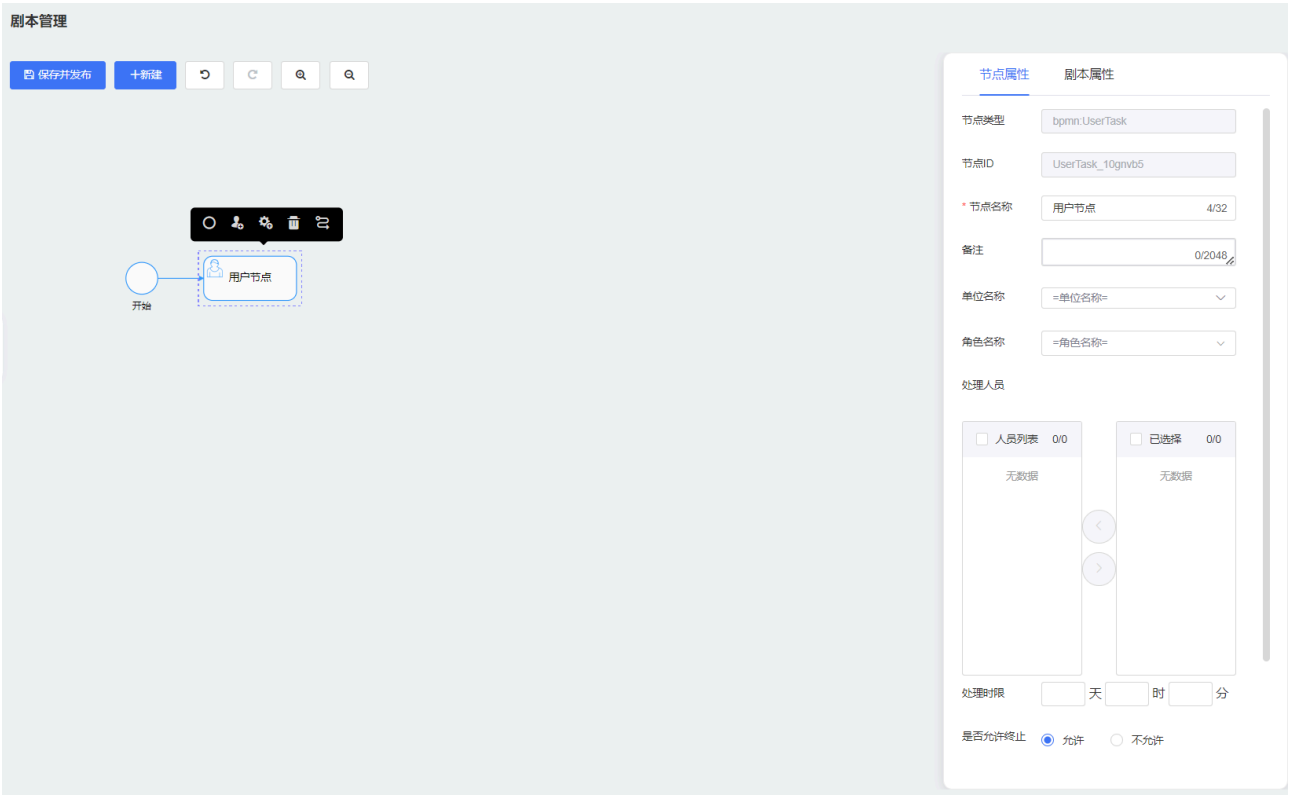


新增剧本节点

选择节点后，点下如下按钮，新增剧本节点。



新增的节点默认为用户节点。选取节点后，右侧可对节点属性进行编辑。



- 是否允许终止

  终止功能，剧本编辑界面如图所示。



有“终止”权限的人工节点（在剧本编辑中设置），可以“终止”当前告警工单的剧本执行。

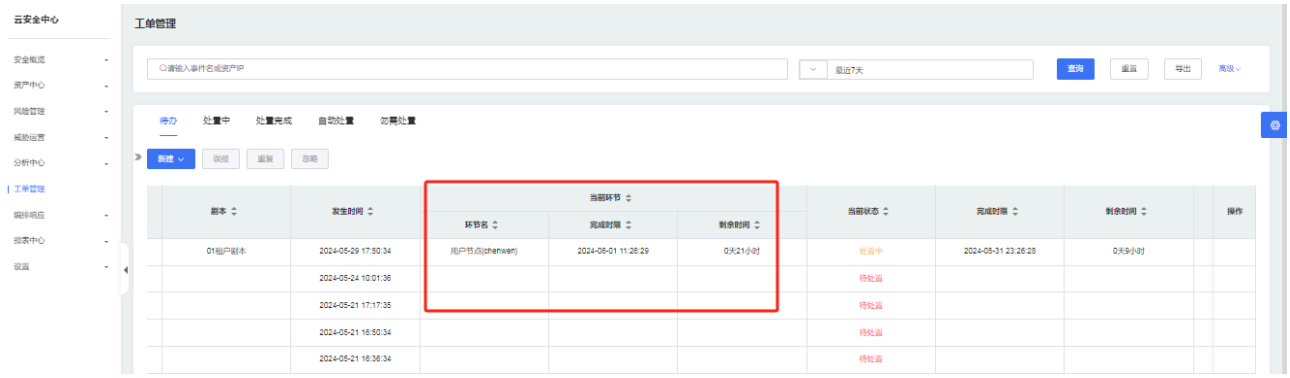


- 处理时限

  人工节点处理时限，剧本编辑中，人工节点编辑界面，可以设置该节点处理时限设置。设置人工节点处理超时时限，如下图所示。

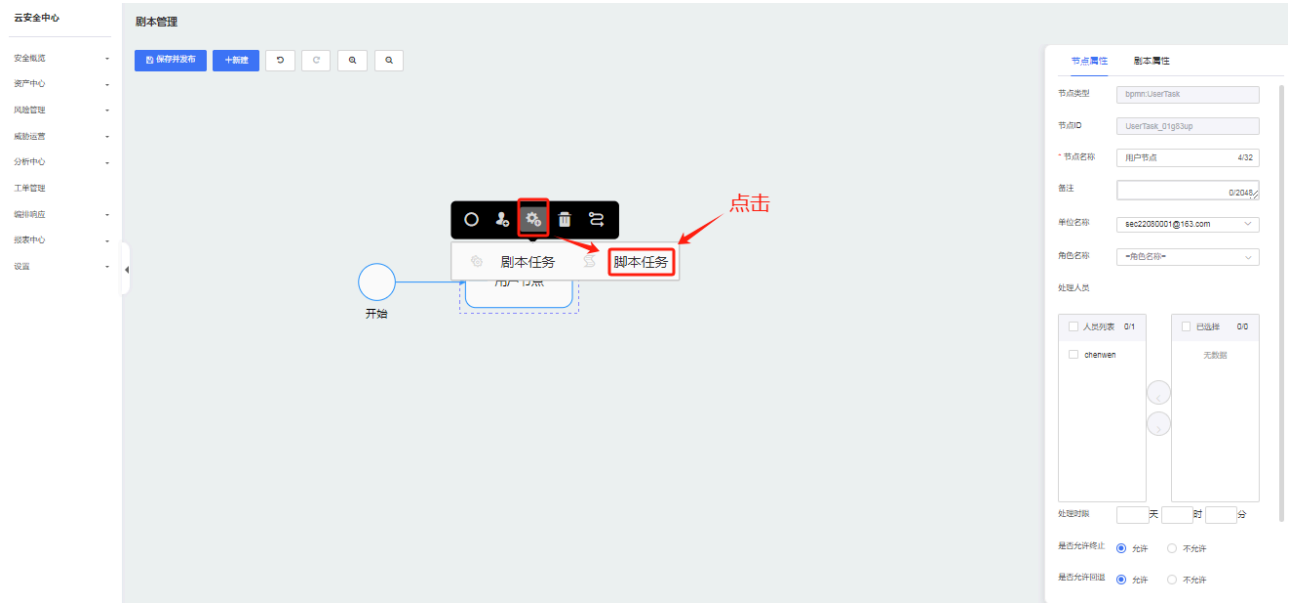


设置后，在告警管理列表和告警处置中会显示是否超时。



新增脚本任务节点

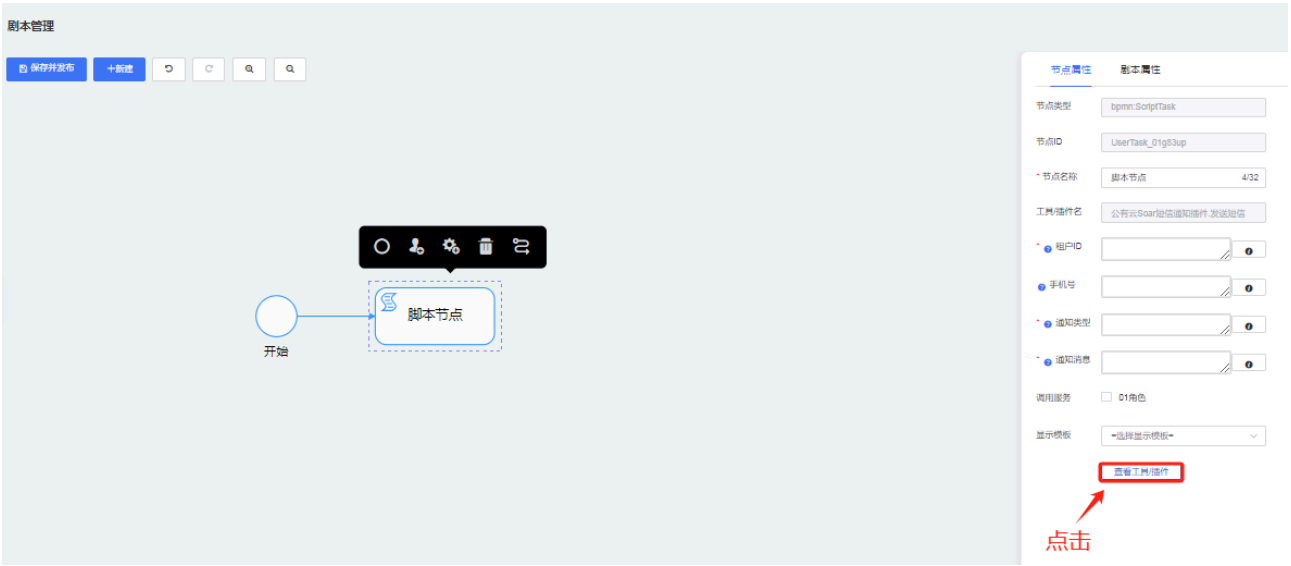
点击默认新增的用户节点，在节点上方显示节点工具，选择脚本任务。



切换为脚本任务后，系统默认从左侧弹出插件选取栏，可通过插件选取栏搜索相关插件或直接选取。



也可通过右侧的节点属性中的“查看工具/插件”按钮弹出插件选取栏。

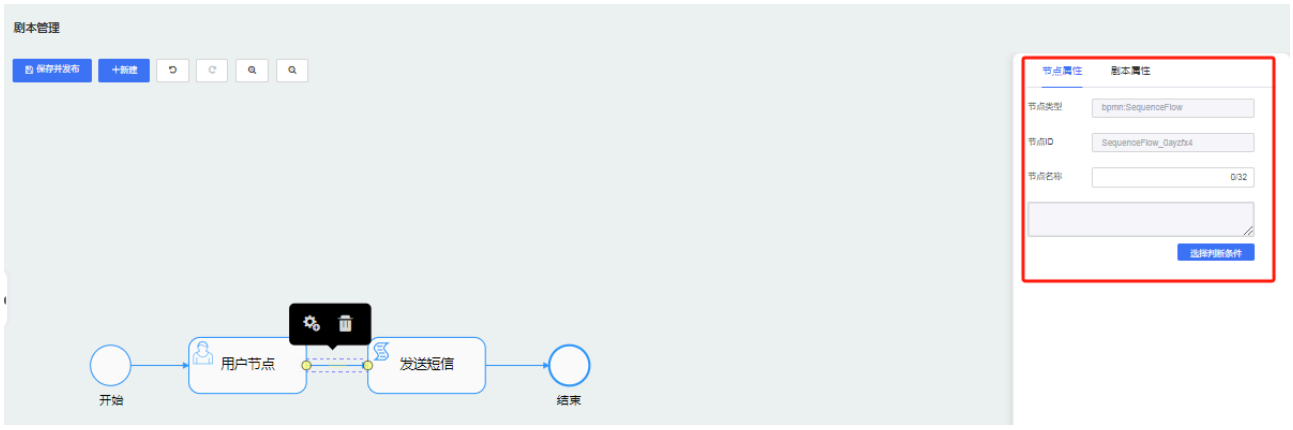


选取完插件后，设置插件的入参。

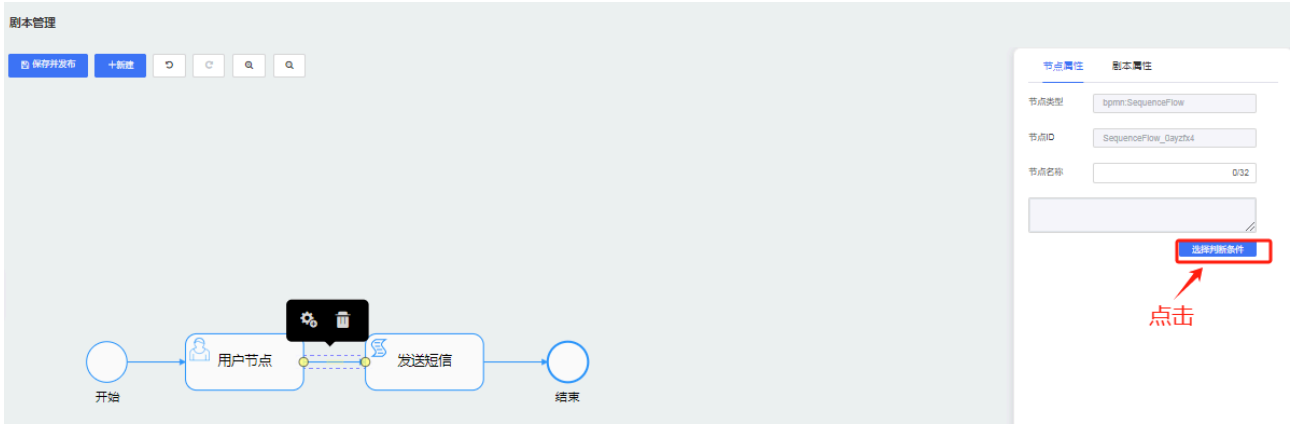


剧本线条设置

点击线条，可以在线条上增加线条说明，以及在线条上添加判断条件，以控制流程走向。



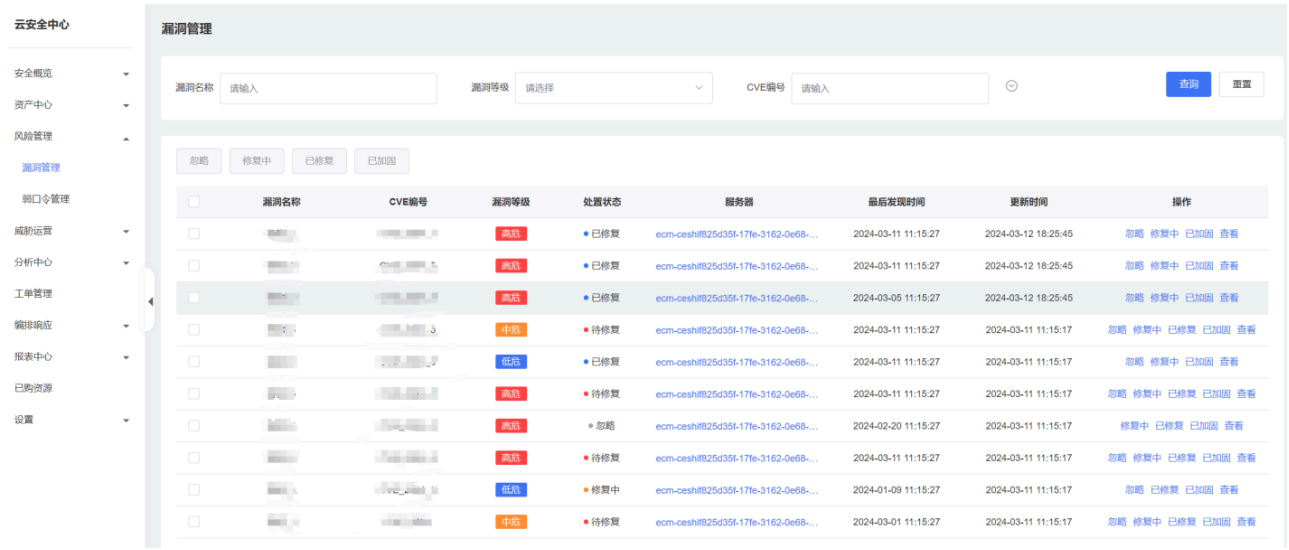
点击“选择判断条件”，增加或修改线条判断条件。



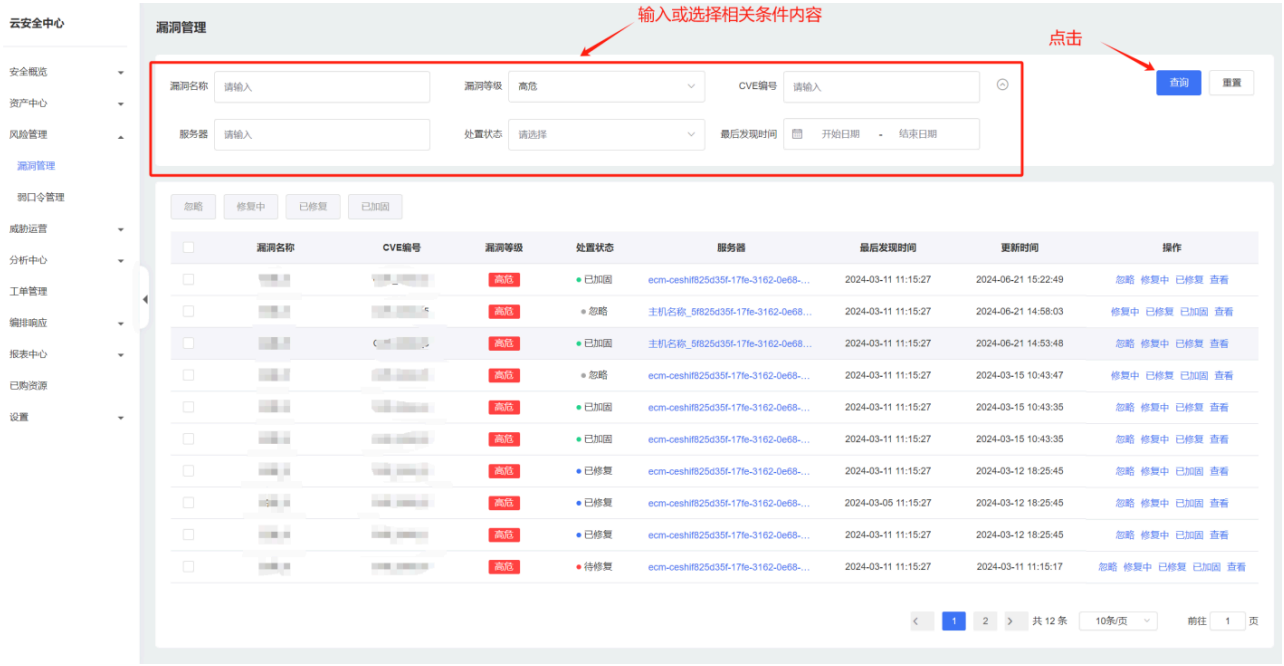


如何进行漏洞管理

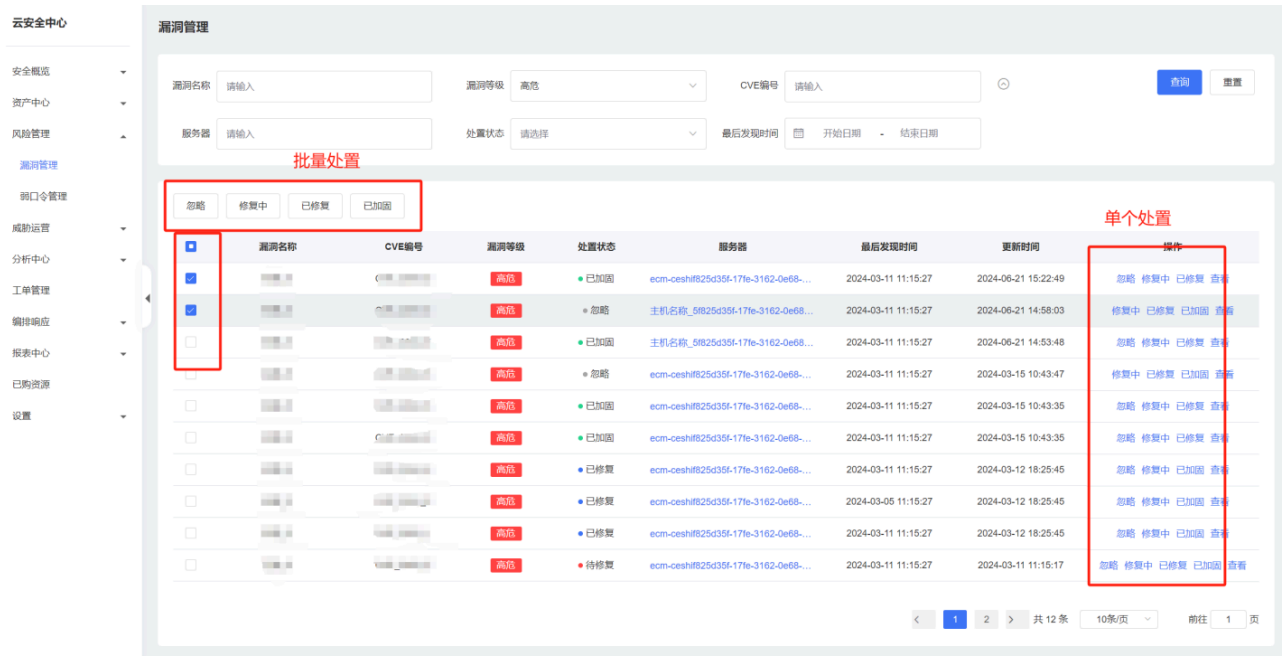
1. 进入风险管理-漏洞管理页面，为租户提供漏洞查询及处置功能。



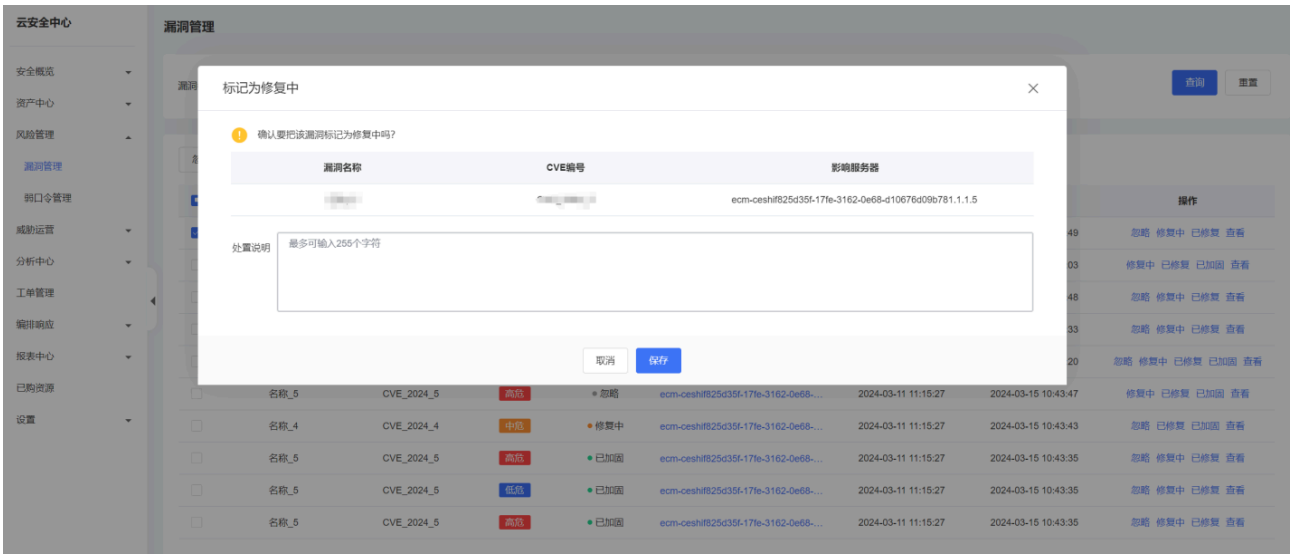
2. 支持条件查询，用户输入或选择相关条件内容。

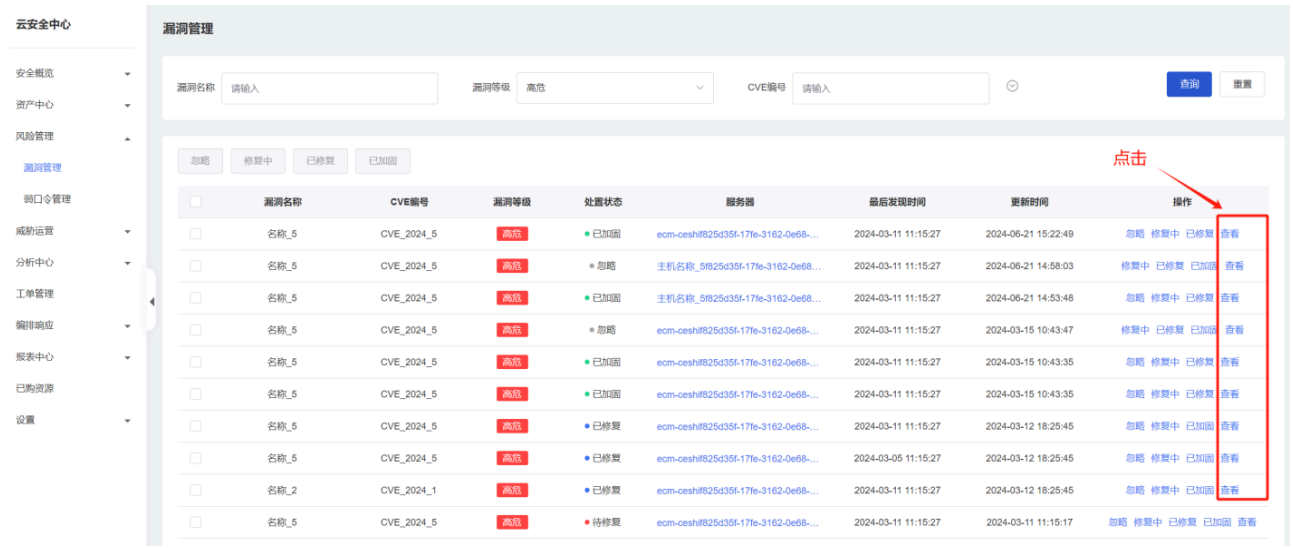


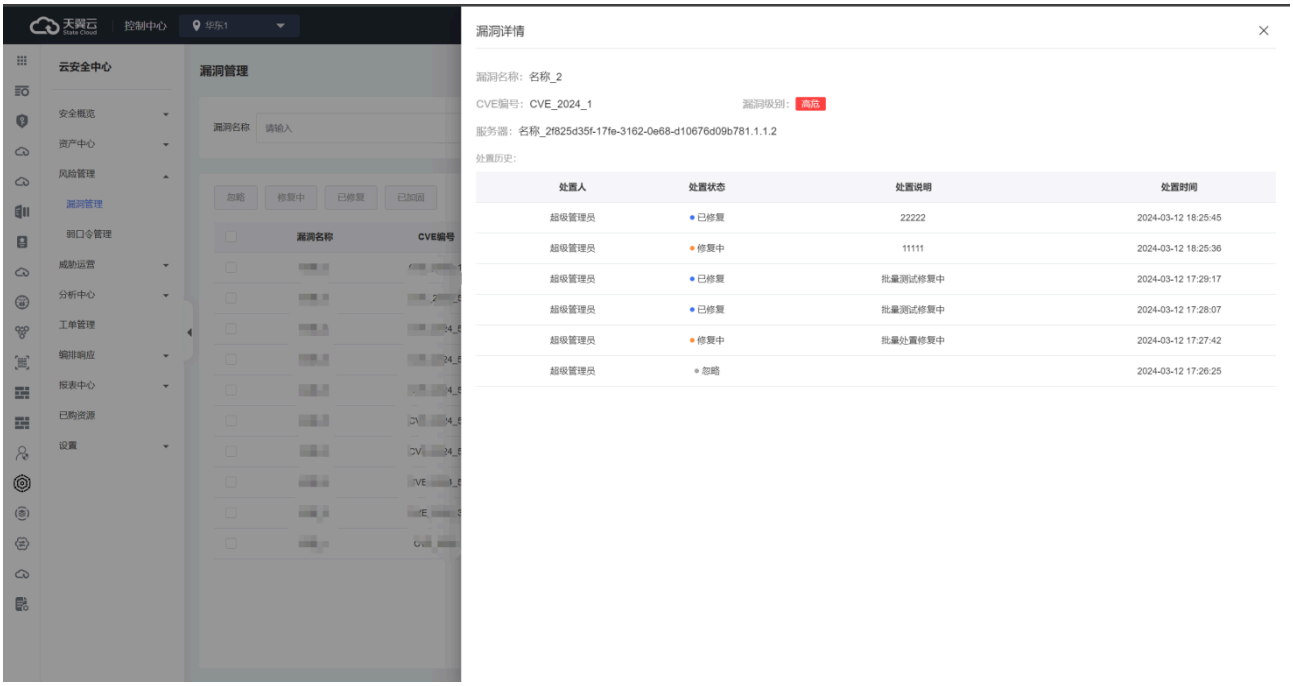
3. 提供处置能力，可直接或批量修改漏洞处置状态。状态枚举值：修复中、已修复、忽略、已加固等。修改处置状态可填写状态变更原因。



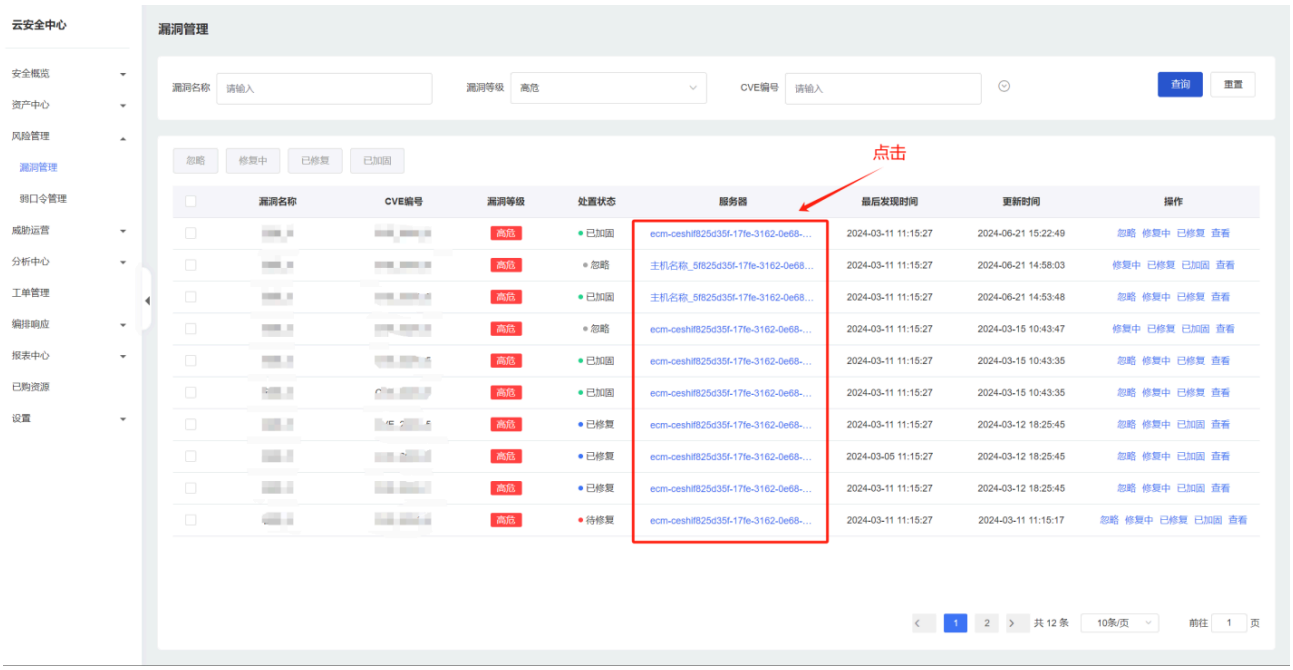
4. 进行处置，在漏洞详情中可以历史所有的状态变更记录的信息：处置人、处置状态、处置说明等。

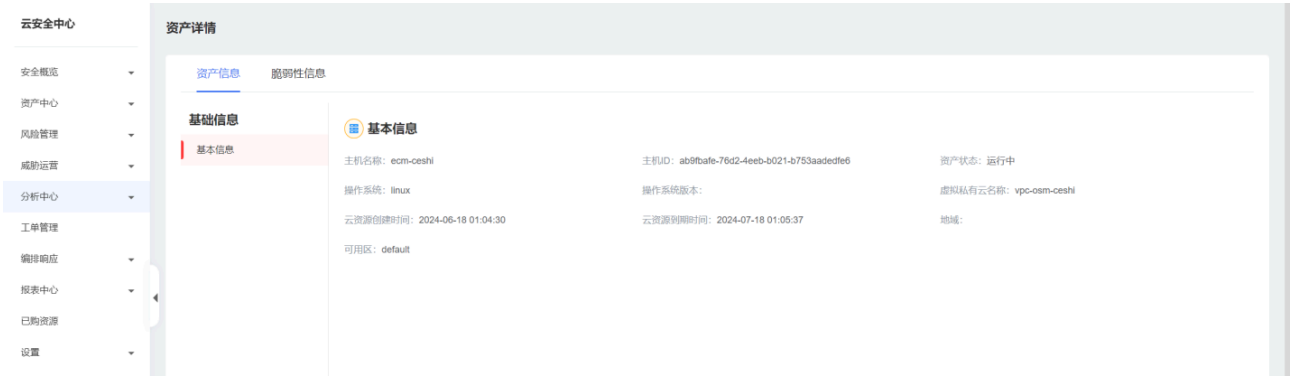






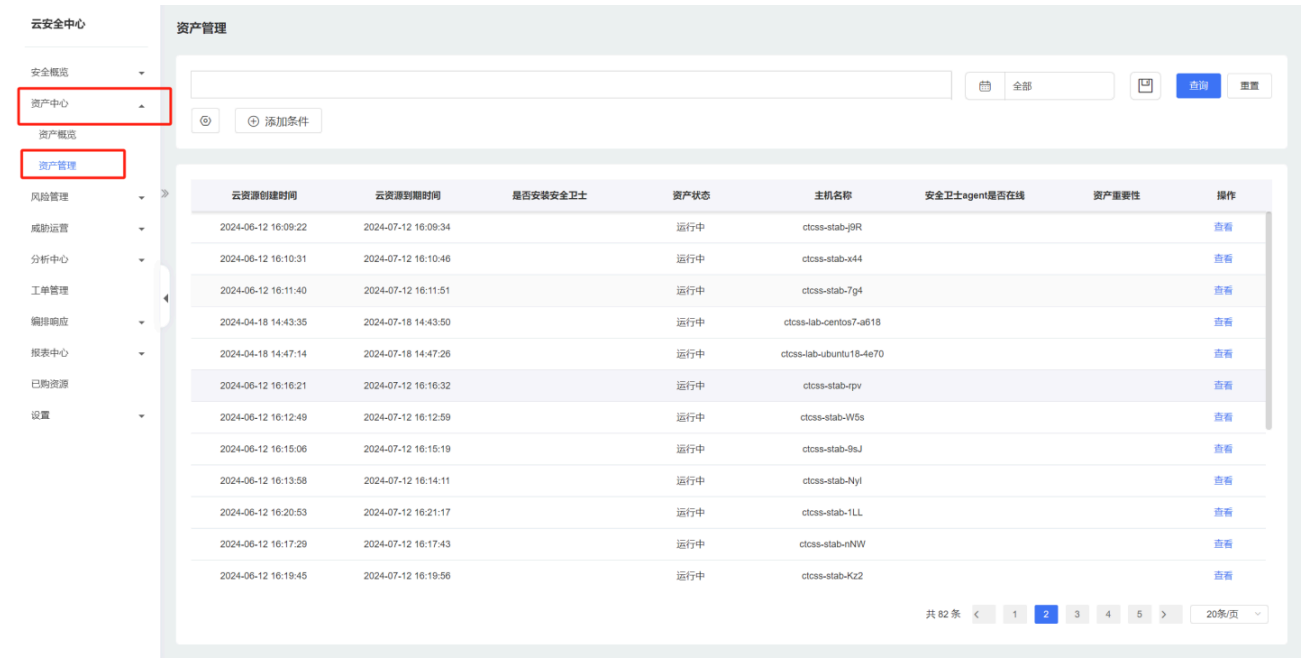
5. 每条漏洞能够关联资产信息，可快速查看关联的资产详情。



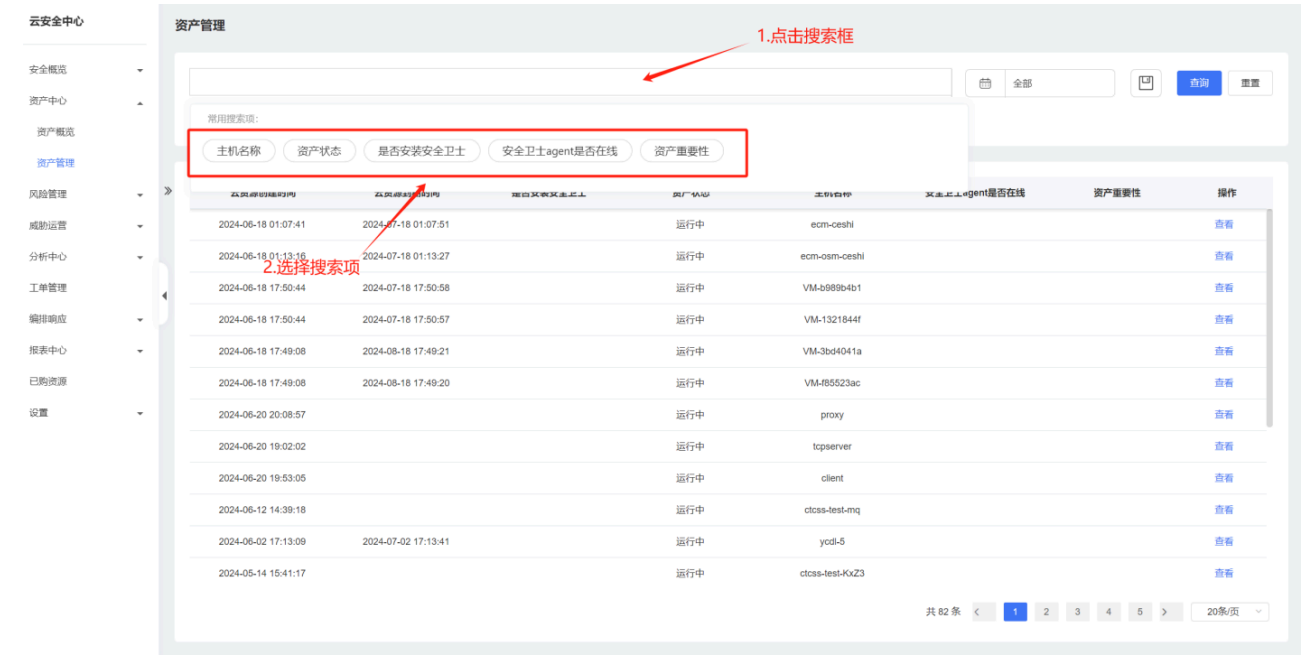


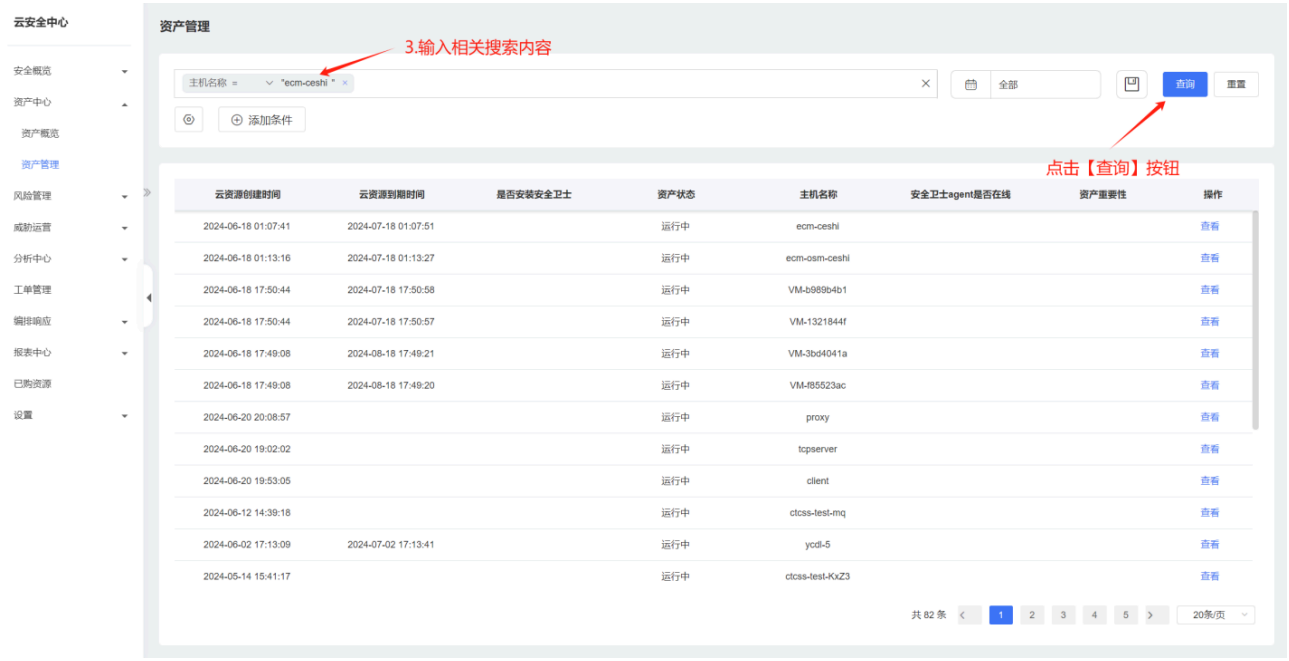
如何对资产进行查看管理

1. 进入资产中心-资产管理页面，为租户提供资产及资产属性的查询功能。

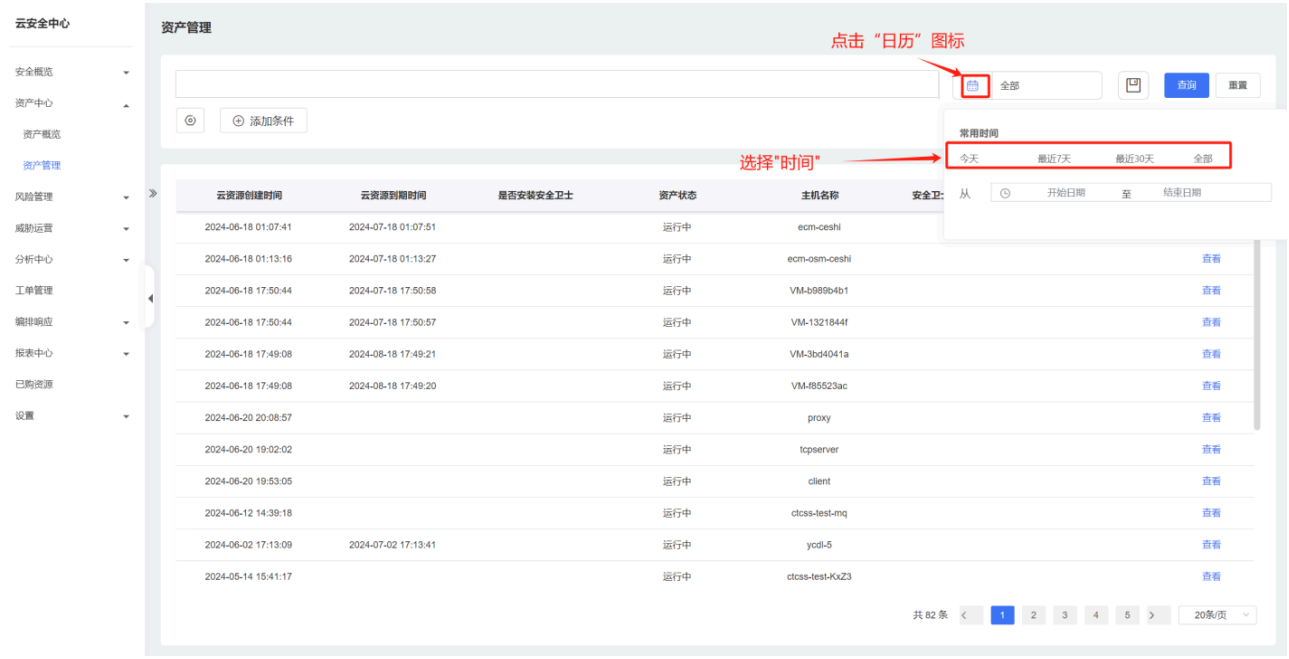

云安全中心
资产管理
安全概览
资产中心
资产概览
资产管理
风险管理
威胁运营
分析中心
工单管理
编排响应
报表中心
已购资源
设置
全部
查询
重置
添加条件
云资源创建时间
云资源到期时间
是否安装安全卫士
资产状态
主机名称
安全卫士agent是否在线
资产重要性
操作
2024-06-12 16:09:22
2024-07-12 16:09:34
运行中
ctcss-stab-j9R
查看
2024-06-12 16:10:31
2024-07-12 16:10:46
ctcss-stab-x44
2024-06-12 16:11:40
2024-07-12 16:11:51
ctcss-stab-7g4
2024-04-18 14:43:35
2024-07-18 14:43:50
ctcss-lab-centos7-a618
2024-04-18 14:47:14
2024-07-18 14:47:26
ctcss-lab-ubuntu18-4e70
2024-06-12 16:16:21
2024-07-12 16:16:32
ctcss-stab-rpv
2024-06-12 16:12:49
2024-07-12 16:12:59
ctcss-stab-W5s
2024-06-12 16:15:06
2024-07-12 16:15:19
ctcss-stab-9sJ
2024-06-12 16:13:58
2024-07-12 16:14:11
ctcss-stab-Nyl
2024-06-12 16:20:53
2024-07-12 16:21:17
ctcss-stab-1LL
2024-06-12 16:17:29
2024-07-12 16:17:43
ctcss-stab-nNW
2024-06-12 16:19:45
2024-07-12 16:19:56
ctcss-stab-Kz2
共 82 条
20条/页

2. 选择常用搜索项查询。

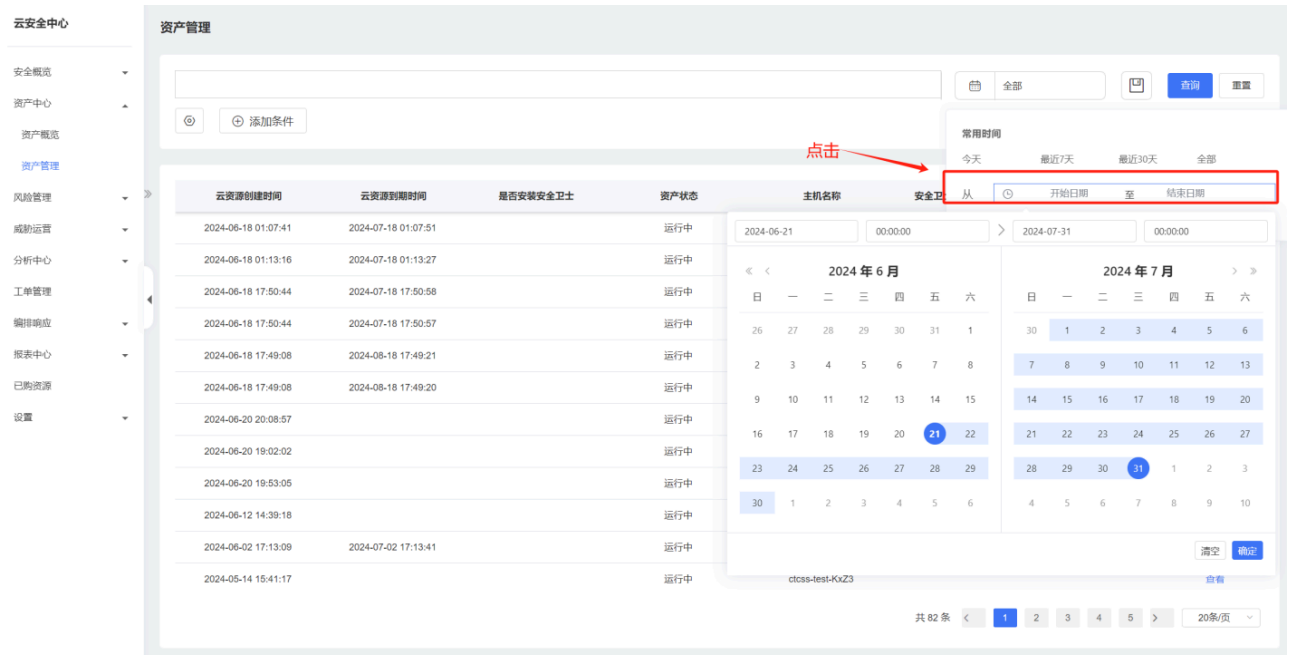

云安全中心
资产管理
1.点击搜索框
全部
查询
重置
常用搜索项:
主机名称
资产状态
是否安装安全卫士
安全卫士agent是否在线
资产重要性
2.选择搜索项
操作
2024-06-18 01:07:41
2024-07-18 01:07:51
运行中
ecm-ceshi
查看
2024-06-18 01:13:16
2024-07-18 01:13:27
ecm-osm-ceshi
2024-06-18 17:50:44
2024-07-18 17:50:58
VM-b989b4b1
2024-06-18 17:50:44
2024-07-18 17:50:57
VM-1321844f
2024-06-18 17:49:08
2024-08-18 17:49:21
VM-3bd4041a
2024-06-18 17:49:08
2024-08-18 17:49:20
VM-f85523ac
2024-06-20 20:08:57
proxy
2024-06-20 19:02:02
tcpserver
2024-06-20 19:53:05
client
2024-06-12 14:39:18
ctcss-test-mq
2024-06-02 17:13:09
2024-07-02 17:13:41
ycdl-5
2024-05-14 15:41:17
ctcss-test-KxZ3
共 82 条
20条/页



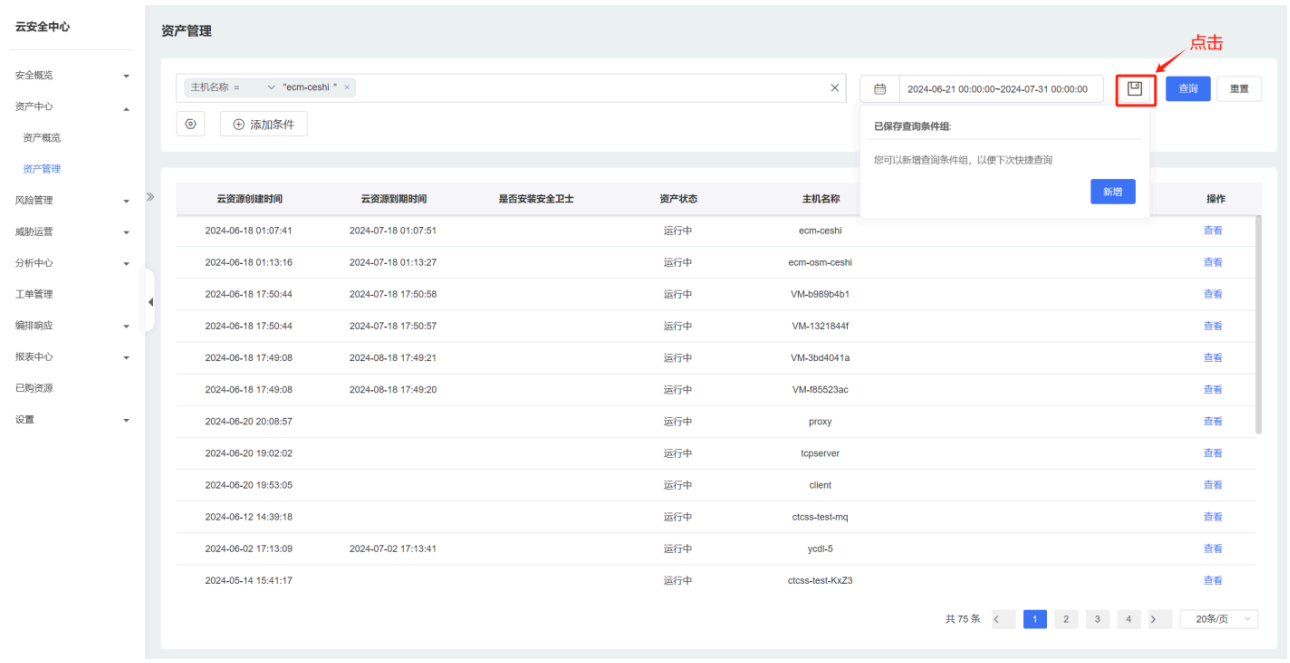
3. 选择常用时间查询。

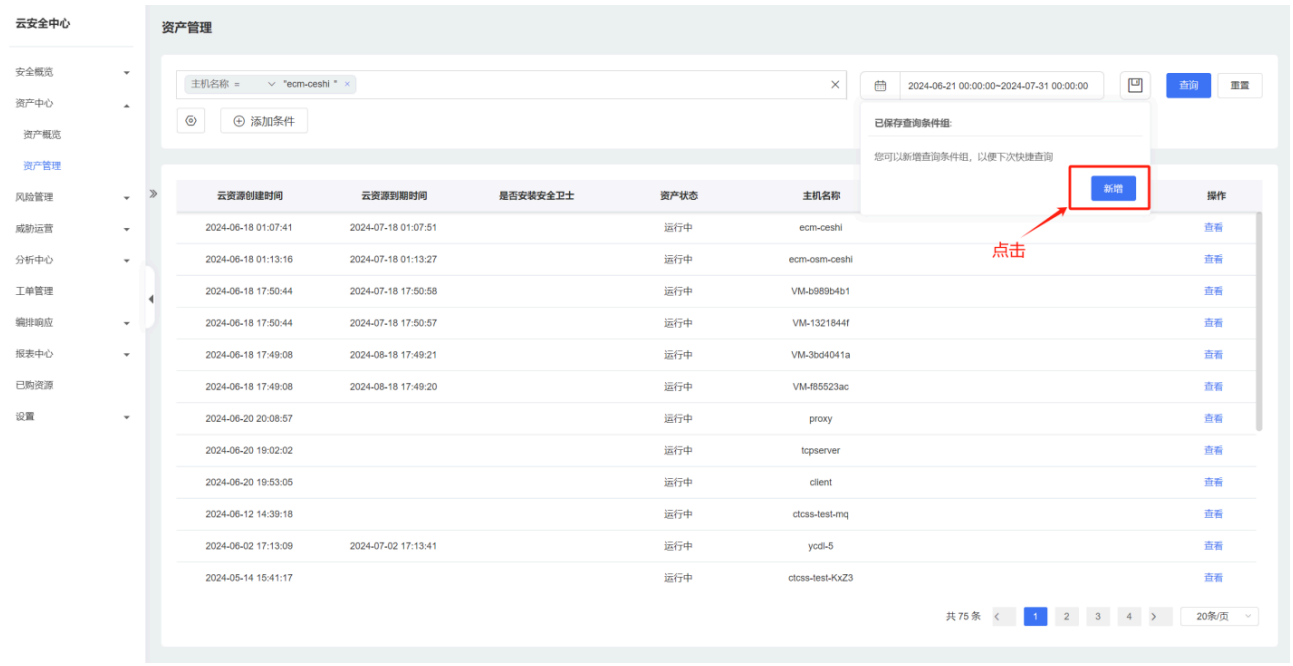


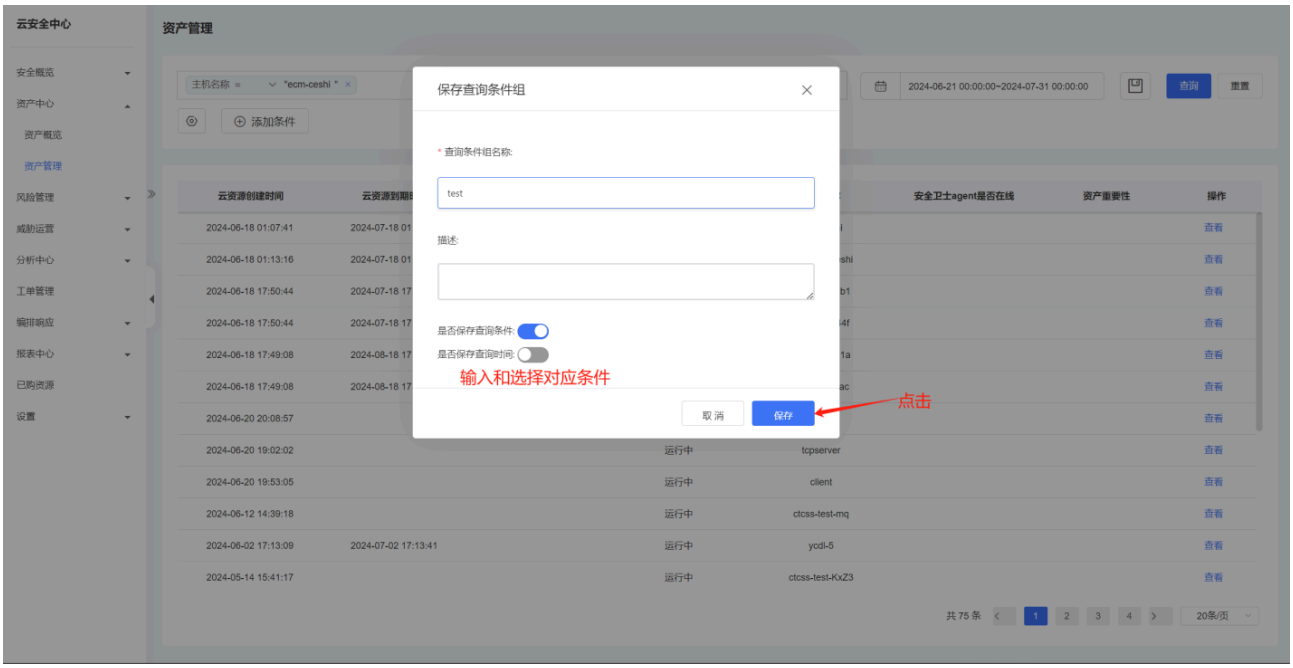
4. 选择时间段查询。



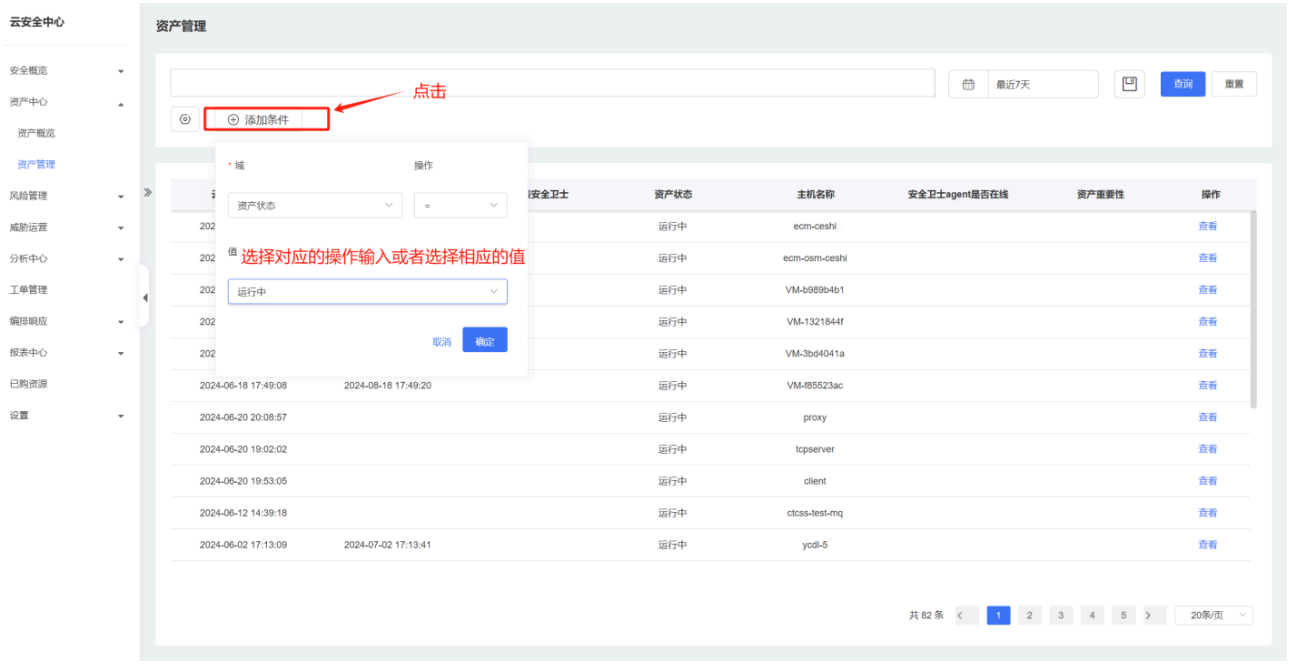
5. 查询条件组：保存查询条件，方便用户快速查询。




云安全中心
资产管理
主机名称 = "ecm-ceshi"
添加条件
2024-06-21 00:00:00~2024-07-31 00:00:00
查询
重置
已保存查询条件组:
您可以新增查询条件组，以便下次快捷查询
新增
点击
云资源创建时间
云资源到期时间
是否安装安全卫士
资产状态
主机名称
操作
2024-06-18 01:07:41
2024-07-18 01:07:51
运行中
ecm-ceshi
查看
2024-06-18 01:13:16
2024-07-18 01:13:27
ecm-osm-ceshi
2024-06-18 17:50:44
2024-07-18 17:50:58
VM-b989b4b1
2024-06-18 17:50:44
2024-07-18 17:50:57
VM-1321844f
2024-06-18 17:49:08
2024-08-18 17:49:21
VM-3bd4041a
2024-06-18 17:49:08
2024-08-18 17:49:20
VM-f85523ac
2024-06-20 20:08:57
proxy
2024-06-20 19:02:02
tcpserver
2024-06-20 19:53:05
client
2024-06-12 14:39:18
ctcss-test-mq
2024-06-02 17:13:09
2024-07-02 17:13:41
ycdl-5
2024-05-14 15:41:17
ctcss-test-KxZ3
共 75 条
20条/页


云安全中心
资产管理
保存查询条件组
查询条件组名称:
test
描述:
是否保存查询条件:
是否保存查询时间:
输入和选择对应条件
取消
保存
点击

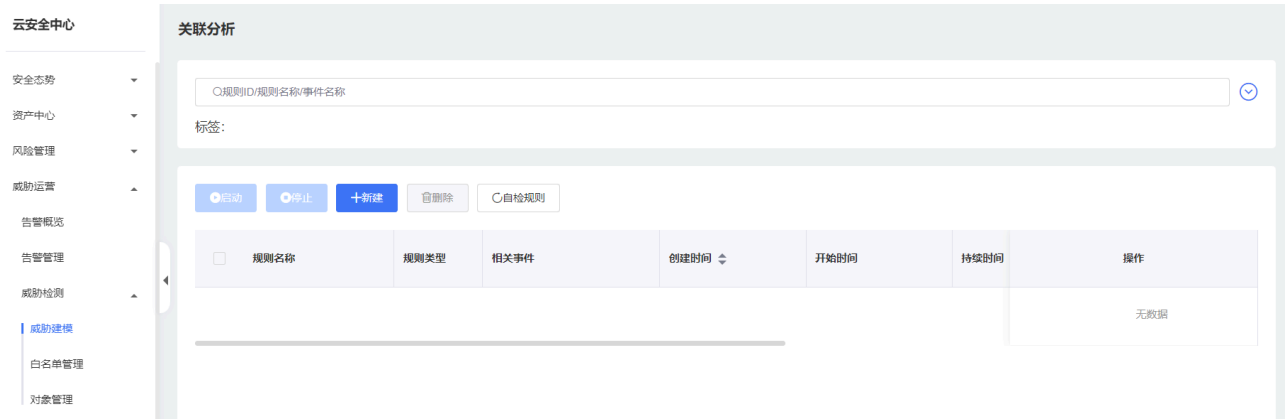
6. 添加条件查询。



如何进行威胁建模

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 威胁检测 > 威胁建模”。

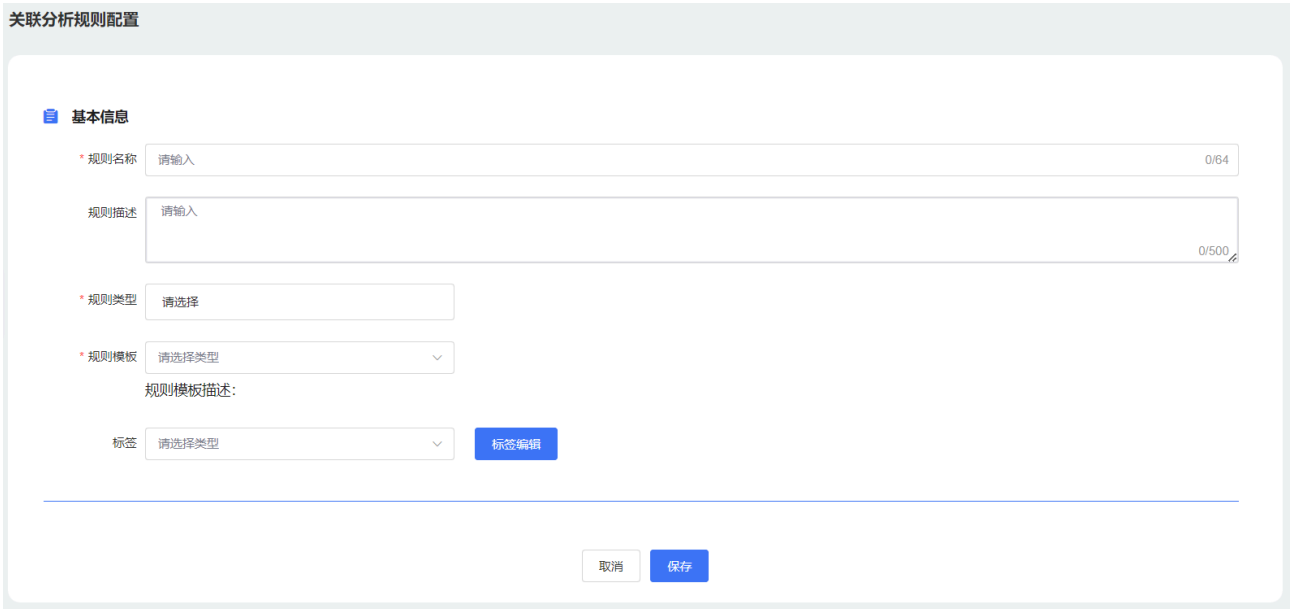
   可以通过关键字、快捷方式、规则类型和标签查询关联分析规则。



3. 单击“新建”。

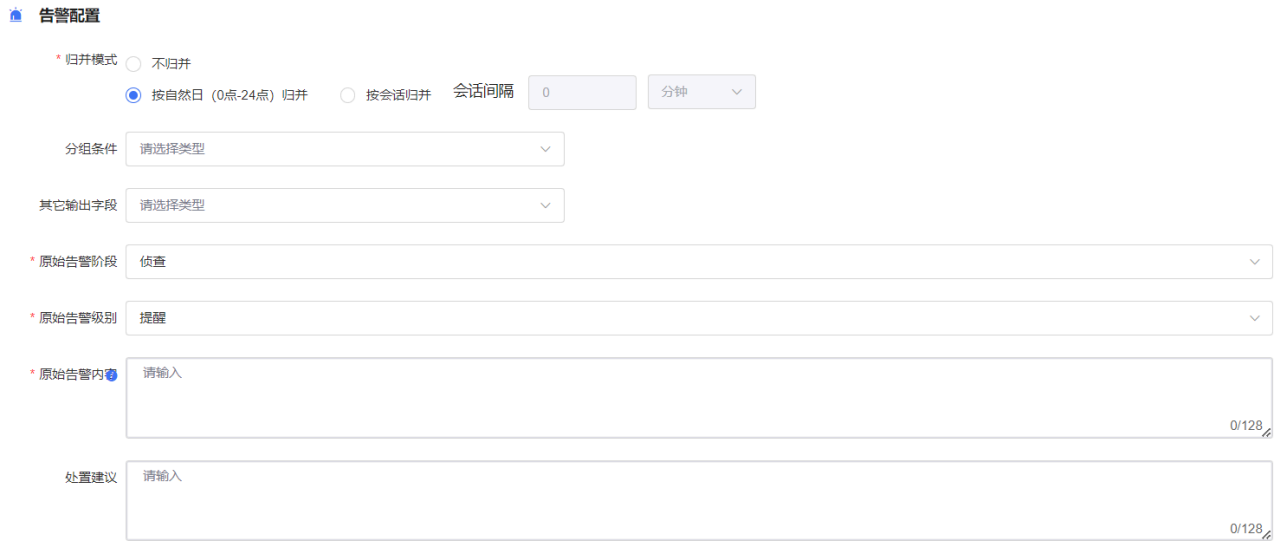


4. 基本信息填写，带有*的为必填项



5. 选择规则类型和规则模板后，还需要配置原始告警源、输出结果、告警配置等。





6. 配置完成后，单击“保存”。列表中可以看到新建的规则。



等级保护测评解读

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

等保标准章节	等保标准序号	云安全中心对应功能	功能解读
安全区域边界-边界防护	8.1.3.1	插件管理、威胁运营、编排响应	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。同时能够对非授权设备私自联到内部网络的行为进行检查，通过处置功能实现对相关访问进行限制。

等保标准章节	等保标准序号	云安全中心对应功能	功能解读
安全区域边界-访问控制	8.1.3.2	插件管理、威胁运营、编排响应	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。同时能够对非授权设备私自联到内部网络的行为进行检查，通过处置功能实现对相关访问进行限制。
安全区域边界-入侵防范	8.1.3.3	插件管理、威胁运营、编排响应	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，可在关键网络节点处检测、防止或限制从外部/内部发起的网络攻击行为，并对这些攻击行为进行分析、记录以及提供报警。
安全区域边界-恶意代码和垃圾邮件防范	8.1.3.4	插件管理、威胁运营、编排响应	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，可在关键网络节点处对恶意代码进行检测、分析，并通过处置功能实现对相关机器访问进行限制。
安全区域边界-安全审计	8.1.3.5	插件管理、威胁运营	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，可以在网络边界以及重要网络节点进行安全审计，记录包括相关告警事件的日期和时间、用户、告警类型、告警是否成功及其他与审计相关的信息，通过威胁运营，能将单独用户行为审计和数据分析。

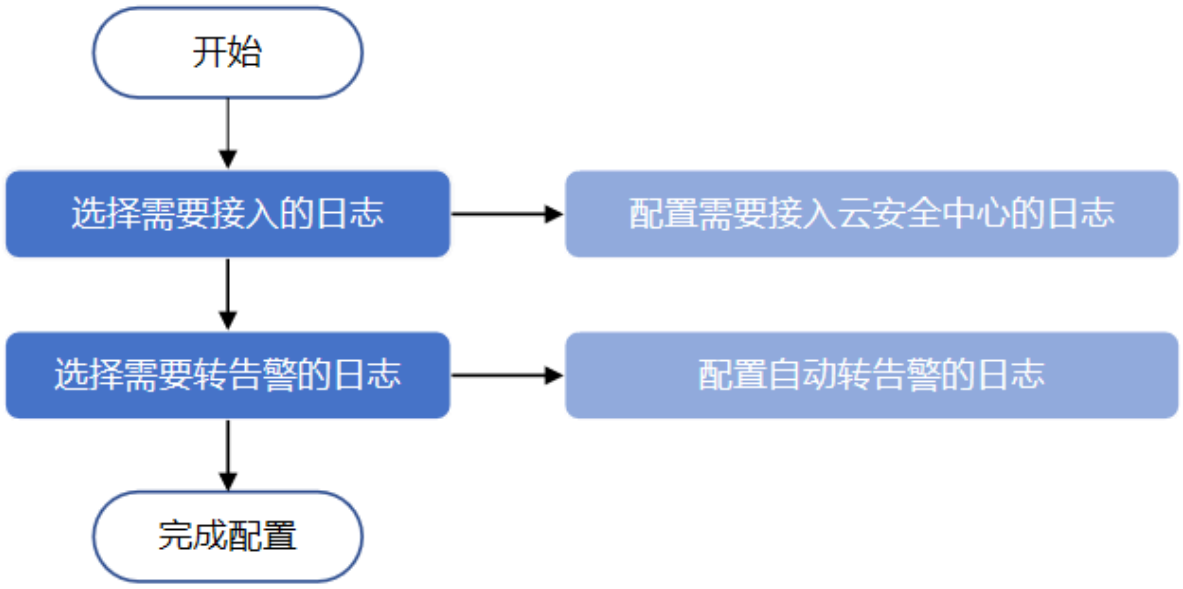
等保标准章节	等保标准序号	云安全中心对应功能	功能解读
安全计算环境-安全审计	8.1.4.3	插件管理、威胁运营	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，可以在网络边界以及重要网络节点进行安全审计，记录包括相关告警事件的日期和时间、用户、告警类型、告警是否成功及其他与审计相关的信息。云安全中心日志通过多副本实时存储多分，保障用户日志在其存储周期内不丢失、可恢复。
安全计算环境-入侵防范	8.1.4.4	插件管理、威胁运营、编排响应	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞，同时应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警。
安全计算环境-恶意代码防范	8.1.4.5	插件管理、威胁运营、编排响应	云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，能够及时采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为。通过处置功能将其有效阻断。

等保标准章节	等保标准序号	云安全中心对应功能	功能解读
安全区域边界-集中管控	8.1.5.4	插件管理、威胁运营、编排响应	• 云安全中心通过获取WAF、防火墙以及安全卫士等日志数据，以及不同安全设备的处置集成，实现对分布在网络中的安全设备或安全组件进行管控。 • 通过内网建立一条安全的信息传输路径,对网络中的安全设备或安全组件进行管理。 • 形成对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。 • 通过实时的日志采集，对分散在各个设备上的审计数据进行收集汇总和集中分析,并保证审计记录的留存时间符合法律法规要求。 • 同时在应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。 • 通过编排响应能对网络中发生的各类安全告警进行识别、报警和分析。

如何接入产品日志

打开云安全中心的设置>集成配置，在集成配置中选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。

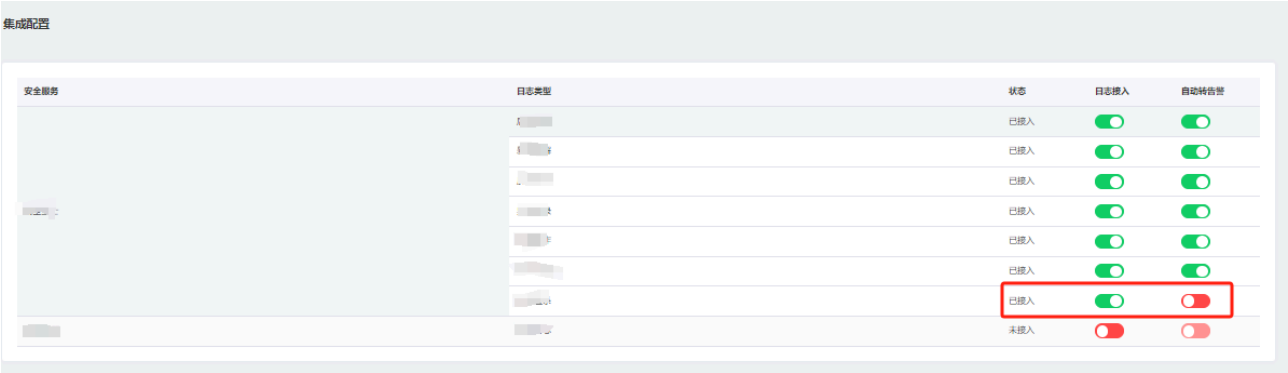
接入流程如下：



1. 登录云安全中心控制台。
2. 选择“设置 > 数据源监控”，打开数据源监控页面。
3. 在操作列点击“启用”，确保数据源监控处于启用状态。



4. 选择“设置 > 集成配置”，打开数据集成配置页面。
5. 选择需要接入的日志，并打开日志接入开关。



6. 选择需要转告警的日志，并打开自动转告警的开关。



说明

- 系统默认会接入部分日志，用户如有需要，可以自行关闭。
- 需要先在数据源监控页面启用开关后，才可以在集成配置页面中开启日志和告警配置。
- 选择需要接入的日志时，只能针对您已经购买的云产品。
- 选择需要转告警的日志，只能针对已经选择接入的日志进行。

基于云安全中心进行风险治理

应用场景

企业云资源规模扩张后，普遍存在资产底数不清、云服务配置不合规、安全基线落地难、等保合规整改无抓手等问题，传统人工核查效率低、覆盖不全，易因配置漏洞引发数据泄露、权限越权等安全风险。

本场景依托云安全中心 CSPM（云安全态势管理）核心能力，实现云资产统一盘点、合规基线自动化检测、风险分级闭环处置，帮助企业快速满足等保 2.0 及行业监管合规要求，系统性降低云原生配置风险。适用于等保合规自查整改、云资产风险普查、日常安全配置巡检、重大活动前安全排查等业务场景。

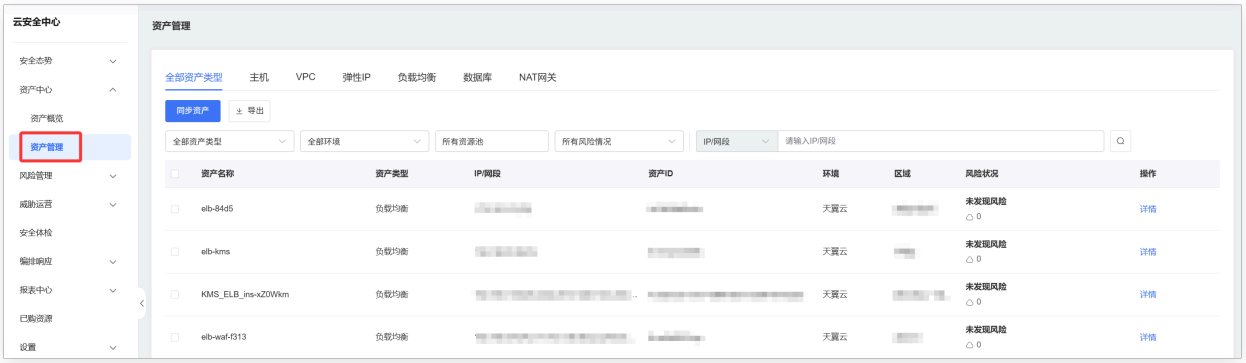
典型案例

通过云安全中心资产中心完成全量 300 + 云资源自动盘点与标签分类，启用云安全最佳实践基线开展全域检测，定位出 68 项高危配置风险；针对存储桶公开访问、安全组宽端口等高频问题形成标准化整改 SOP，落地每周自动巡检机制。 治理后高危配置风险数量下降 92%，未再发生因配置漏洞导致的安全事件，资产盘点与风险核查耗时从每周 2 人天缩短至 1 小时。

操作步骤

云资产统一纳管与全景盘点

1. 登录 云安全中心控制台 。
2. 在左侧导航栏选择“资产中心 > 资产管理”，进入资产管理页面，云安全中心系统自动同步账号下 云主机、云数据库、弹性IP、VPC 等全量云资源，完成资产自动发现；按资源类型、地域、项目维度分类梳理，补全资产标签与负责人信息，建立完整云资产台账，消除资产盲区。

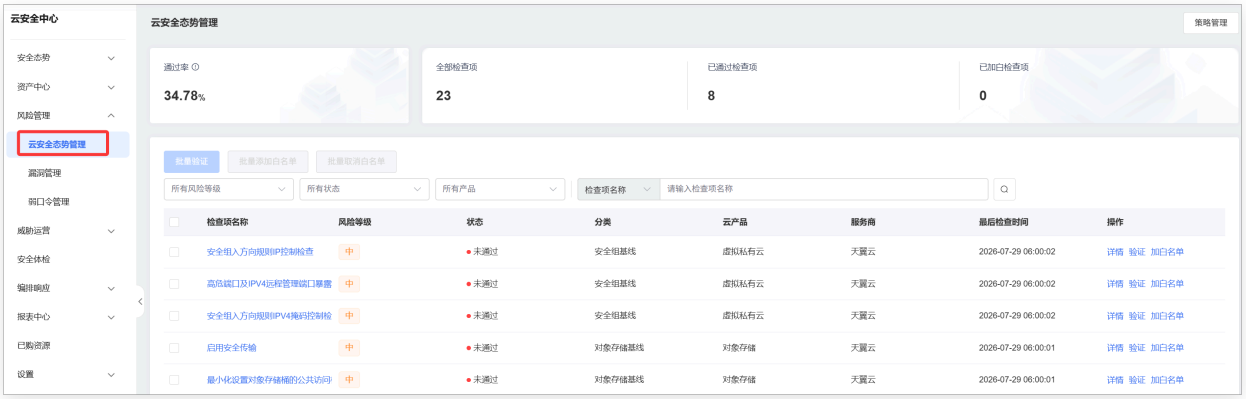


合规基线策略配置与批量检测

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“风险管理 > 云安全态势管理”。



3. 选择对应合规标准（如天翼云安全最佳实践基线）；根据业务场景指定检测资产分组与检测周期，启用定时检测任务；针对存储桶公开访问、安全组全端口开放、弱口令等高危配置项，单独设置高优先级检测规则，确保核心风险优先覆盖。



风险分级核查与闭环处置

检测完成后，可在云安全态势管理模块查看全部不合规项，系统自动按高、中、低风险等级分类统计；



针对高危风险查看详情与官方整改建议，一键分派给对应资产负责人并明确整改时限；对可自动化处置的风险通过控制台一键整改，对需业务侧配合的风险导出整改清单同步落地。



整改验证与常态化运营

整改完成后对对应风险项执行“验证”，验证通过的风险自动闭环；结合业务迭代持续优化基线策略，形成“检测 - 处置 - 验证 - 优化” 的风险治理闭环。


批量验证
批量添加白名单
批量取消白名单
所有风险等级
所有状态
所有产品
检查项名称
请输入检查项名称
检查项名称
风险等级
状态
分类
云产品
服务商
最后检查时间
操作
安全组入方向规则IP控制检查
中
未通过
安全组基线
虚拟私有云
天翼云
2026-07-29 06:00:02
详情
验证
加白名单

常见问题

产品咨询类

云安全中心是否只是对其他云安全产品日志进行采集分析?

云安全中心产品除了采集其他安全产品的日志进行统一管理外，还提供编排响应以及处置的能力，能够对告警形成自己的处置流程，并进行自动化处置。云安全中心打通了云上的各类安全产品形成联动响应处置，帮助用户提升威胁响应处置效率。

云安全中心如何帮助客户满足等保合规要求?

云安全中心提供的插件管理、威胁运营、编排响应等功能，可以满足等保的“边界防护”、“访问控制”、“入侵防范”、“恶意代码和垃圾邮件防范”、“安全审计”、“恶意代码防范”、“集中管控”等要求。具体可参见 等级保护测评解读 。

云安全中心支持采集云上哪些安全日志?

云安全中心目前支持采集云上安全产品的安全告警日志，包括Web应用防火墙（原生版）、服务器安全卫士（原生版）、云等保专区、数据库审计、云堡垒机（原生版）企业版等产品。具体的日志类型请参见 支持的日志类型 。

短信使用余量是否会进行提醒?

云安全中心会在短信剩余500条时、以及短信全部使用完时，提醒用户短信剩余量。

云安全中心没有收到告警，可能的原因是什么?

若已在日志发送端配置好日志转发，但在云安全中心反复刷新仍未收到日志，请先检查网络是否可达，网络不可达将导致日志接收失败。

建议您依次检查：

1. IP端口配置是否无误。
2. 是否在云安全中心“设置 > 集成配置”页面打开了日志接入与自动转告警开关。
3. 使用运维工具检测到端口网络是否通畅。
4. 若需要接入云等保v1.0的安全原子能力，请确认是否升级了proxy组件。

若以上检查确认无误，请您通过官网工单系统或联系工程师排查问题并解决。

计费购买类

同一个账号可以购买多个云安全中心实例吗?

云安全中心为全局服务，同一个账号下仅可购买一个云安全中心实例，对应一个主资源版本。购买云安全中心实例后，您可以购买扩展资源。

云安全中心实例到期后，数据还会保留吗?

购买的云安全中心实例到期后如未按时续费，公有云平台会提供一定的保留期。

- 保留期内，平台会冻结云安全中心的服务，用户配置的各类数据会继续生效，但用户无法访问云安全中心。
- 保留期满，用户若仍未续费，平台会清除实例资源，用户原有的配置信息将会被删除，同时云安全中心将不再获取第三方日志、用户云上资产等信息。

云安全中心实例可以降低规格吗?

云安全中心实例不支持降级，同时已绑定的扩展资源也不支持单独退订。如您需要降低当前规格，你可以先退订当前的云安全中心实例，再重新购买云安全中心实例。

云安全中心是否支持自动续订?

支持。

您可以在购买套餐的同时勾选自动续订，同时也支持在使用过程中，在订单中心中设置自动续订。

云安全中心存在规格差异吗?

当前云安全中心只有一个标准版，标准版的服务如下所示。

版本	即时通知服务	日志分析量
标准版	10000条/月	50G/月

云安全中心有哪些扩展服务可以购买?

云安全中心支持2种类型的扩展资源，用户可支持根据实际使用需求购买日志分析量扩展资源和态势大屏扩展资源。其中，态势大屏扩展资源只可购买一次，日志分析量扩展资源的购买资源最小单位为50G，即扩展资源需要购买50G的整数倍。

续费时是否可同时变更云安全中心版本或规格?

续费时您只能为当前的云安全中心实例版本规格进行续费，增加使用时长。续费时不能同时变更云安全中心的规格。您可以在续费完成后，对云安全中心实例版本进行升级。

扩展资源购买上限是什么?

当前云安全中心提供态势大屏扩展资源及日志分析量拓展包。

态势大屏扩展资源订购上限为1个，日志分析量拓展包订购暂无订购上限。请您根据业务需要按需订购。

云安全中心是否支持按需计费?

当前云安全中心不支持按需计费。

云安全中心有促销折扣吗?

当前云安全中心暂无优惠折扣。

在使用期间购买了扩展资源 ，资源到期时间是何时?

扩展资源购买后与主资源绑定，资源到期时间与主资源一致。

购买的扩展资源，支持单独退订吗?

不支持。扩展资源购买后与主资源绑定，不支持单独退订。

退订重购后，原实例的配置数据可以保留吗?

用户退订后在15天内重新购买实例时，可恢复原有配置。当重新购买时距离退订已超过15天，原资源已释放且配置数据已删除，则无法恢复。

如何选择日志分析量扩展资源?

购买日志分析量扩展资源时，您需要测算接入云安全中心的所有日志数据总量，确保您选购的日志分析量能覆盖每月的日志数据总量。

日志分析量扩展资源会过期吗?

每月优先使用主资源赠送的日志分析量，当赠送部分使用完毕后再消耗日志分析量扩展资源。未用完的日志分析量扩展资源会一直累积（赠送部分每月清零不进行累积）。

如何查看当前购买产品的产品规格?

购买、续订、升级扩容后可以通过产品信息页面查看所购买产品的规格，同时个人消息中心以及用户绑定的手机也能够收到相关的购买成功提示短信。

查看购买后的云安全中心规格方式如下：

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全>云安全中心”。
3. 进入产品服务页面，选择“已购资源”。



> 说明
>
> 购买成功后需要等待一段时间相关规格才能刷新，预计等到1-2分钟左右。

配置类

数据接入相关

为什么要进行数据接入?

云安全中心（CT-CSC，Cloud Security Center，简称CSC）作为用户侧的安全中心，其核心数据来源是用户的各种安全设备。

云安全中心数据接入要如何配置?

打开云安全中心的“设置 > 集成配置”，在集成配置页面选择需要接入的日志类型即可。

云安全中心告警需要如何配置?

1. 打开云安全中心的“设置 > 集成配置”，在集成配置页面选择需要接入的日志类型。
2. 部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。

   同时云安全中心还支持自定义转告警配置，即通过云安全中心的“威胁运营 > 威胁检测 > 威胁建模”功能实现自定义告警配置。

告警通知相关

如何获取钉钉机器人的token和secret?

在配置告警通知联系组时，若开启钉钉机器人，需要输入token和secret，可以根据以下步骤获取钉钉机器人的token和secret。

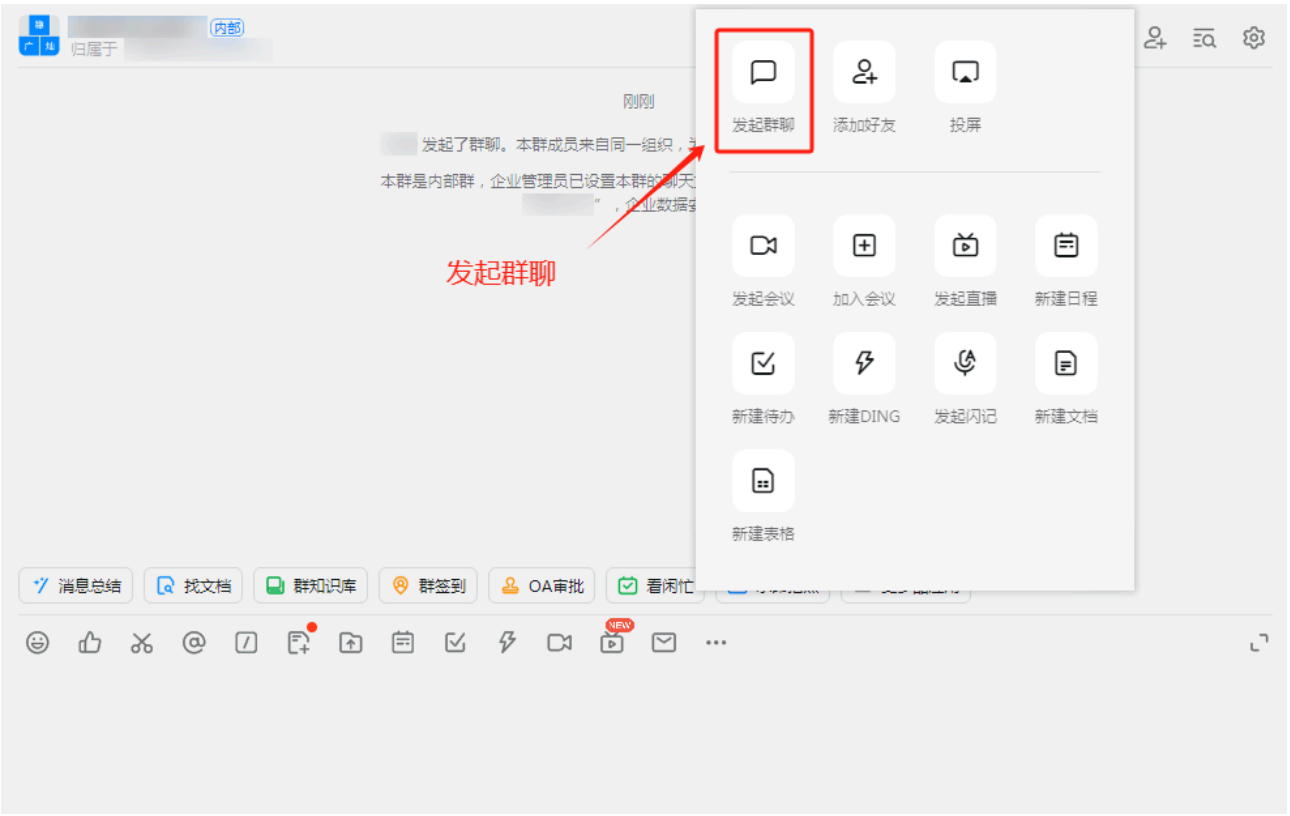
步骤一：创建钉钉群聊

若您已有钉钉群聊，则可跳过此步骤。

1. 登录钉钉客户端，在左上角切换到需要创建群聊的组织团队。



2. 单击客户端右上角的“+”图标，单击“发起群聊”。



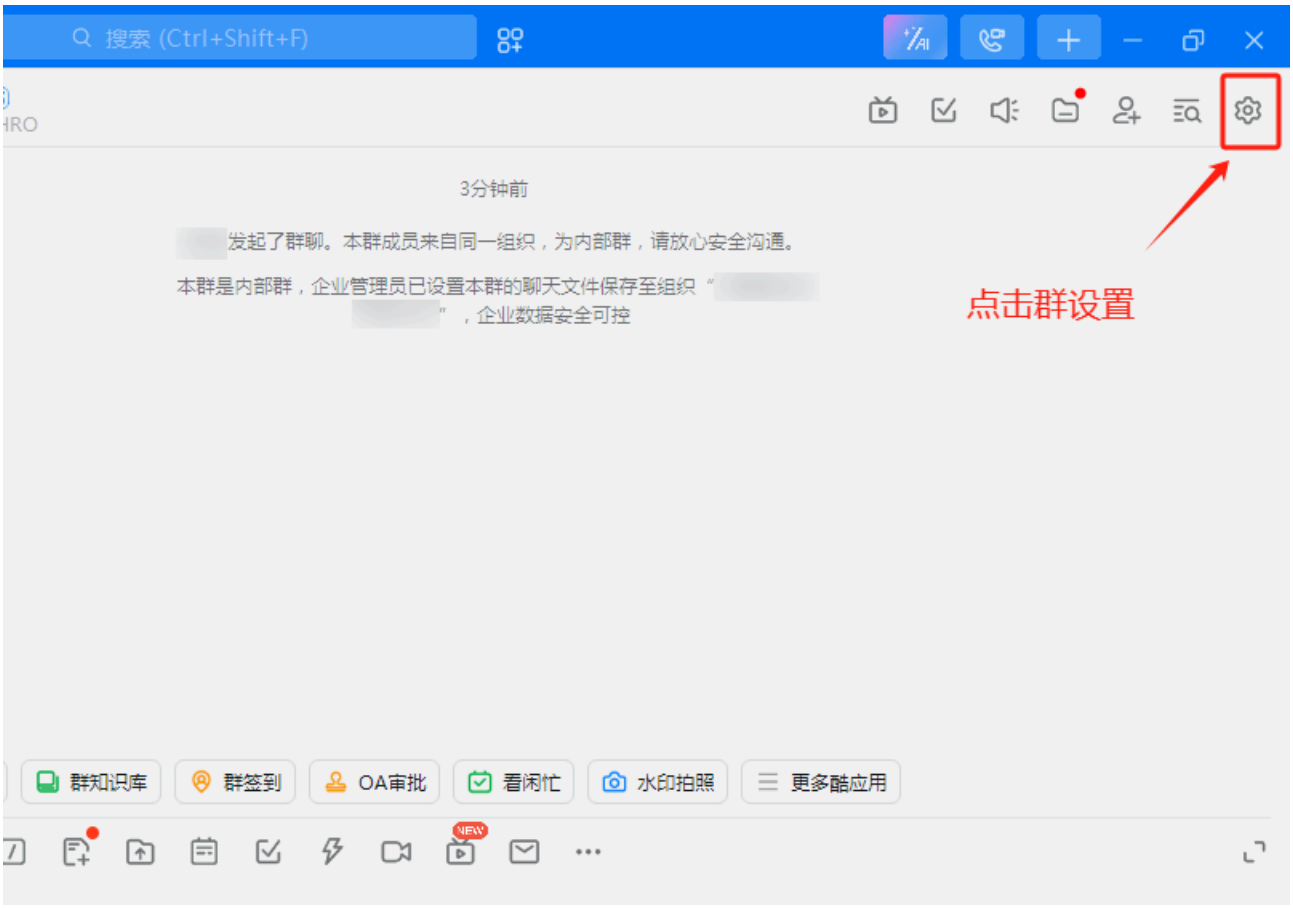
3. 勾选联系人、设置群名称等信息后，单击“确定”创建群聊。



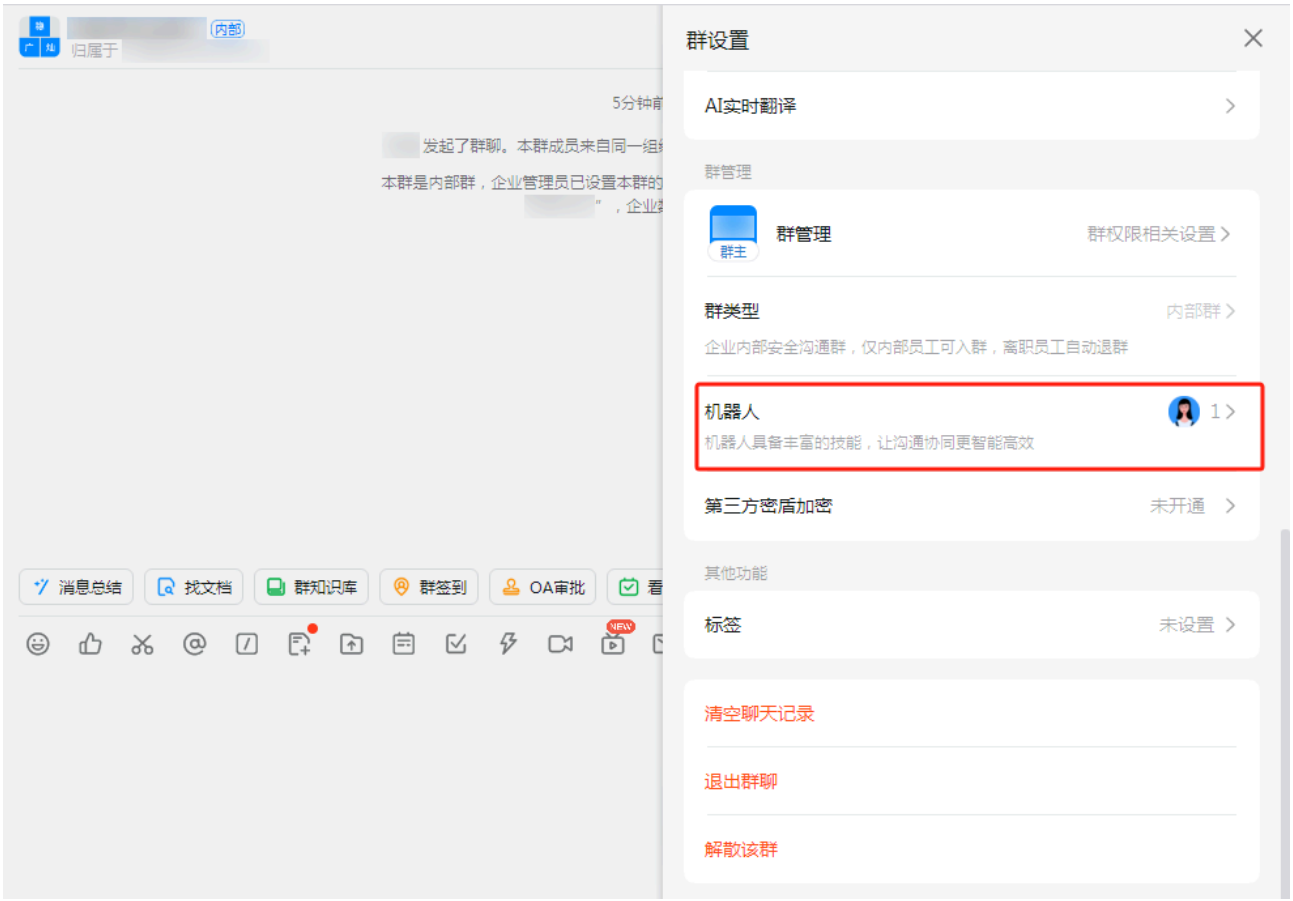
步骤二：添加钉钉机器人

若您已有钉钉机器人，则可跳过此步骤。

1. 登录钉钉客户端，选择需要添加钉钉机器人的群聊。
2. 单击群聊右上角的“群设置”图标。



3. 在群设置页面，下拉点击“机器人”。



4. 点击“添加机器人”。



5. 选择“自定义”机器人。



6. 在机器人详情页面，点击“添加”。



7. 配置机器人信息。安全设置勾选“加签”，复制并记录加签后的密钥信息。

> 说明
>
> 勾选“加签”后，产生的密钥即为 通知联系组配置钉钉机器人 所需的secret。



8. 勾选“我已阅读并同意《自定义机器人服务及免责条款》”，单击“完成”。
9. 复制并记录Webhook地址。

> 说明
>
> Webhook地址中，“access_token=”后的部分即为 通知联系组配置钉钉机器人 所需的token。



步骤三：获取钉钉机器人的token和secret

若添加钉钉机器人时，未记录机器人的token和secret，后续可以通过机器人设置页面获取。

1. 点击机器人头像。


内部
归属于
13分钟前
发起了群聊。本群成员来自同一组织，为内部群，请放心安全沟通。
本群是内部群，企业管理员已设置本群的聊天文件保存至组织“
”，企业数据安全可控
添加了机器人: test
test
机器人
大家好！我是 test 机器人，很高兴为你们服务。
消息总结
找文档
群知识库
群签到
OA审批
看闲忙
水印拍照
更多酷应用
Enter 发送，Ctrl+Enter 换行
发送

2. 点击“机器人设置”。



3. 复制并记录Webhook地址、加签的密钥。

参数	说明	示例
token	Webhook地址中，“access_token=”后的部分即为通知联系组配置钉钉机器人所需的token。	例如：Webhook地址为https://oapi.dingtalk.com/robot/send?access_token=84baa7a8cd8408d98cd6cb69bf11eb1c0599d641b99af35b9811cde048371de7，则token为84baa7a8cd8408d98cd6cb69bf11eb1c0599d641b99af35b9811cde0483
secret	复制的密钥即为通知联系组配置钉钉机器人所需的secret。	SECf96f0ae46193a9f27c0aca682aff86278365f7622b3e4cfe608be412e4cb31cb

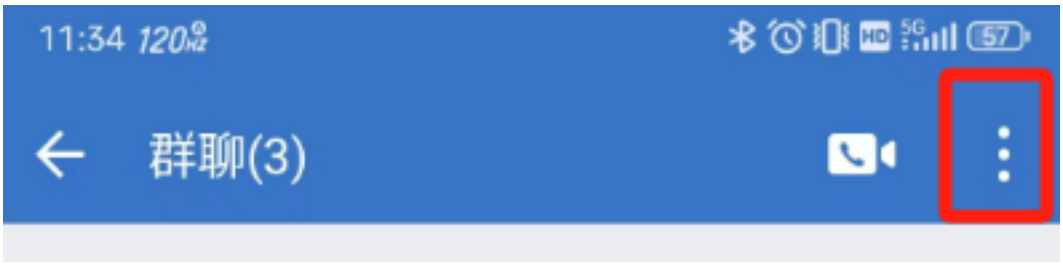


如何获取企业微信机器人的key?

在配置告警通知联系组时，若开启微信机器人，需要输入key，请根据以下步骤获取微信机器人的key。

> 注意
>
> 企业微信群必须是内部群，外部群无法添加机器人。

1. 登录企业微信客户端，选择需要添加微信机器人的群聊。
2. 单击群聊右上角的“更多”图标。



3. 在群管理模块，选择“群机器人”，添加群机器人。



4. 复制并记录Webhook地址。

Webhook地址中，“key=”后的部分即为 通知联系组配置微信机器人 所需的key。

说明

例如：Webhook地址为https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=0317a550-1837-46ea-bf69-4a04dcd876c0，则key为0317a550-1837-46ea-bf69-4a04dcd876c0。

