态势感知（专业版）

用户使用指南

天翼云科技有限公司

目 录

1 产品介绍 1

1.1 什么是态势感知（专业版） 1

1.2 产品功能 1

1.3 产品优势 6

1.4 应用场景 6

1.5 计费说明 7

1.6 与其他云服务的关系 8

1.7 基本概念 8

2 服务委托授权 11

3 购买态势感知（专业版） 13

3.1 选择计费模式 13

3.2 购买专业版 13

3.3 增加配额 15

3.4 续费 16

3.5 退订 17

4 安全总览 19

4.1 总览 19

4.2 安全评分 23

5 工作空间 26

5.1 工作空间概述 26

5.2 新增工作空间 27

5.3 空间管理 28

5.3.1 查看工作空间详情 28

5.3.2 编辑工作空间 30

5.3.3 删除工作空间 31

5.4 空间托管 32

5.4.1 概述 32

5.4.2 创建托管视图 33

5.4.3 创建托管 34

5.4.4 托管授权 35
5.4.5 管理托管 36
6 查看已购资源 41
7 安全治理 42
7.1 概述 42
7.2 安全遵从包规格说明 43
7.3 使用流程 47
7.4 服务授权 48
7.5 订阅安全遵从包 48
7.6 用户自评估 49
7.7 安全合规总览 51
7.8 查看治理结果 52
7.9 查看策略扫描结果 55
7.10 下载安全合规报表 58
7.11 取消订阅安全遵从包 58
8 安全态势 60
8.1 态势总览 60
8.2 安全报告 68
8.2.1 创建/复制安全报告 68
8.2.2 查看安全报告 71
8.2.3 下载安全报告 74
8.2.4 管理安全报告 75
8.3 任务中心 76
8.3.1 查看待办任务 76
8.3.2 处理待办任务 78
8.3.3 查看已处理任务 79
9 资产管理 81
9.1 资产管理概述 81
9.2 设置资产订阅 81
9.3 查看资产信息 82
9.4 导入/导出资产 83
9.5 删除资产 85
10 风险预防 86
10.1 基线检查 86
10.1.1 基线检查概述 86
10.1.2 新增自定义基线检查计划 87
10.1.3 立即执行基线检查 89

10.1.4 执行手动检查 90
10.1.5 查看基线检查结果 91
10.1.6 处理基线检查结果 94
10.2 漏洞管理 98
10.2.1 漏洞管理概述 98
10.2.2 查看漏洞详情 99
10.2.3 修复漏洞 101
10.2.4 导入/导出漏洞 104
10.2.5 忽略/取消忽略漏洞 106
10.3 策略管理 107
10.3.1 策略管理概述 107
10.3.2 新增/编辑应急策略 107
10.3.3 查看应急策略 110
10.3.4 删除应急策略 111
10.3.5 批量阻断/批量取消阻断 112
11 威胁运营 114
11.1 事件管理 114
11.1.1 查看事件信息 114
11.1.2 新增/编辑事件 116
11.1.3 导入/导出事件 120
11.1.4 关闭/删除事件 122
11.2 告警管理 124
11.2.1 查看告警信息 124
11.2.2 告警转事件或关联事件 126
11.2.3 新增/编辑告警 128
11.2.4 导入/导出告警 132
11.2.5 关闭/删除告警 134
11.3 情报管理 136
11.3.1 新增情报指标 136
11.3.2 关闭情报指标 138
11.3.3 导入/导出情报指标 139
11.3.4 管理情报指标 141
11.4 智能建模 146
11.4.1 查看已有模型模板 146
11.4.2 新建/编辑模型 147
11.4.3 查看已有模型 154
11.4.4 管理模型 155
11.5 安全分析 156
11.5.1 安全分析概述 156

11.5.2 使用流程 157
11.5.3 配置索引 157
11.5.4 查询与分析 159
11.5.5 下载日志 166
11.5.6 查询与分析语法-SQL 语法 167
11.5.6.1 基本语法 167
11.5.6.2 约束与限制 168
11.5.6.3 查询语句 168
11.5.6.4 分析语句语法 169
11.5.6.5 分析语句-SELECT 170
11.5.6.6 分析语句-GROUP BY 171
11.5.6.7 分析语句-HAVING 173
11.5.6.8 分析语句-ORDER BY 173
11.5.6.9 分析语句-LIMIT 173
11.5.6.10 分析语句-函数 174
11.5.6.11 分析语句-聚合函数 178
11.5.7 快速查询 179
11.5.8 快速添加日志告警模型 181
11.5.9 图表统计 184
11.5.9.12 图表统计概述 184
11.5.9.13 表格 184
11.5.9.14 折线图 186
11.5.9.15 柱状图 188
11.5.9.16 饼图 190
11.5.10 管理数据空间 192
11.5.10.1 新增数据空间 192
11.5.10.2 查看数据空间详情 194
11.5.10.3 编辑数据空间 196
11.5.10.4 删除数据空间 197
11.5.11 管理管道 198
11.5.11.1 创建管道 198
11.5.11.2 查看管道详情 200
11.5.11.3 编辑管道 201
11.5.11.4 删除管道 203
11.6 数据消费 205
11.7 数据投递 207
11.7.1 新增数据投递 207
11.7.2 数据投递授权 211
11.7.3 查看数据投递情况 212

11.7.4 管理数据投递任务 214
11.7.5 投递日志数据至 LTS 218
11.8 数据监控 220
12 安全编排 223
12.1 安全编排概述 223
12.2 内置剧本、流程和资产连接 223
12.3 安全编排使用流程 227
12.4 （可选）配置并启用流程 228
12.5 配置并启用剧本 232
12.6 运营对象管理 234
12.6.1 数据类 234
12.6.1.1 查看已有数据类 234
12.6.2 类型管理 236
12.6.2.1 管理告警类型 236
12.6.2.2 管理事件类型 243
12.6.2.3 管理威胁情报 249
12.6.2.4 管理漏洞类型 256
12.6.2.5 查看自定义类型 262
12.6.3 分类&映射 263
12.6.3.1 查看已有分类映射 263
12.6.3.2 创建/复制/编辑分类映射 264
12.6.3.3 管理分类映射 268
12.7 剧本编排管理 270
12.7.1 剧本 270
12.7.1.1 提交剧本版本 270
12.7.1.2 审核剧本版本 271
12.7.1.3 启用剧本 273
12.7.1.4 管理剧本 274
12.7.1.5 管理剧本版本 279
12.7.2 流程 284
12.7.2.1 审核流程版本 284
12.7.2.2 启用流程 286
12.7.2.3 管理流程 287
12.7.2.4 管理流程版本 293
12.7.3 资产连接 301
12.7.3.1 新增资产连接 301
12.7.3.2 管理资产连接 303
12.7.4 实例管理 307
12.7.4.1 查看剧本实例监控 307

12.8 页面布局管理 309
12.8.1 查看已有布局模板 309
12.8.2 查看已有布局 310
12.9 插件管理 311
12.9.1 概述 311
12.9.2 查看插件详情 311
13 设置 313
13.1 数据采集 313
13.1.1 数据采集概述 313
13.1.2 采集数据 313
13.1.3 采集管理 321
13.1.3.1 管理连接 321
13.1.3.2 管理解析器 325
13.1.3.3 管理采集通道 332
13.1.3.4 管理采集节点 338
13.1.4 组件管理 340
13.1.4.1 管理节点 340
13.1.4.2 管理组件 344
13.2 数据集成 345
13.2.1 支持接入的日志 345
13.2.2 接入数据 347
13.3 检测设置 349
13.4 目录定制 350
14 常见问题 353
14.1 产品咨询 353
14.1.1 为什么没有看到攻击数据或者看到的攻击数据很少？ 353
14.1.2 态势感知（专业版）的数据来源是什么？ 353
14.1.3 态势感知（专业版）与其他安全服务之间的关系与区别？ 353
14.1.4 态势感知（专业版）与 HSS 服务的区别？ 354
14.1.5 如何更新安全评分？ 356
14.1.6 如何处理暴力破解告警事件？ 357
14.1.7 数据同步/一致性相关问题 358
14.1.8 Agent 安装失败问题排查 358
14.2 购买咨询 363
14.2.1 态势感知（专业版）如何收费？ 363
14.2.2 态势感知（专业版）支持退订吗？ 363
14.2.3 态势感知（专业版）即将到期，如何续费？ 363
14.2.4 态势感知（专业版）到期后，会继续收费吗？ 364
14.2.5 如何修改或取消态势感知（专业版）自动续费？ 365

14.2.6 态势感知（专业版）可以免费使用吗？ 365
A 修订记录 366

1 产品介绍

1.1 什么是态势感知（专业版）

态势感知（专业版）是云原生的新一代安全运营中心，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。

1.2 产品功能

态势感知（专业版）基于云原生安全，提供全面的日志采集、安全治理、智能分析、态势感知、编排响应等快速闭环的安全信息和事件管理能力，助您守护云上安全。

提供有总览、工作空间管理、安全治理、安全态势、资产管理、风险预防、威胁运营、安全编排、数据采集、数据集成功能。

总览

总览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

表 1-1 安全概览功能介绍

功能模块	功能详情
安全评分	根据分析检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
安全趋势	呈现最近 7 天整体资产安全健康得分的趋势图。

工作空间管理

工作空间属于态势感知（专业版）顶层工作台，单个工作空间可绑定普通项目，可支撑不同场景下的工作空间运营模式。

表 1-2 工作空间功能说明

功能模块	功能详情
工作空间	• 空间管理： 单个工作空间可绑定普通项目，可支撑不同场景下的工作空间运营模式。 • 空间托管： – 工作空间数据委托：单租所有工作空间按照租户实际运营汇聚到某一个工作空间做集中安全运营，跨租汇聚安全运营。 – 工作空间委托：跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。

安全治理

安全治理为您提供安全治理模板与合规策略扫描服务，将安全遵从包内的法规标准条款转化成检查项。

表 1-3 安全治理功能说明

功能模块	功能详情
安全治理	• 提供安全遵从包 提供安全治理模板，包含法规标准条款原文、扫描策略、自评估检查项以及专家的改进建议，覆盖 PCI DSS、ISO27701、ISO27001、隐私等法规标准。用户可以订阅、取消订阅安全遵从包，查看合规评估与治理结果。 • 合规策略扫描 Policy as Code，将安全遵从包内的法规标准条款代码化，周期性、自动化扫描云上资产的合规情况，可视化看板呈现风险，提供专家改进建议。 • 自评估检查项 将安全遵从包内的法规标准条款转化成检查项，租户可根据检查项完成自身业务的合规评估，查看历史评估结果，进行证据上传和下载，根据专家改进建议进行治理。 • 合规结果可视 可视化呈现合规评估结果与安全治理情况，包括租户订阅的法规、标准条款遵从概况，各安全遵从包状态，各策略扫描概况。

安全态势

支持通过安全态势即时查看安全态势、定期订阅安全运营报告，了解安全运营核心关注指标。

表 1-4 安全态势功能介绍

功能模块		功能详情
态势总览	安全评分	根据分析检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
	安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
	安全趋势	呈现最近 7 天整体资产安全健康得分的趋势图。
安全报告		通过创建分析报告，及时掌握资产的安全状况数据。
任务中心		集中呈现当前需要进行处理的任务。

资产管理

态势感知（专业版）支持对云上资产全面自动盘点，也可灵活纳管云外各种资产，点清所有资产，并呈现资产实时安全状态。

表 1-5 资产管理功能说明

功能模块	功能详情
资产管理	同步所有资源的安全状态统计信息，支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题。

风险预防

风险预防提供基线检查和漏洞管理功能，帮助您的云安全配置达到各类权威安全标准；知晓全局的漏洞分布。

功能模块	功能详情
基线检查	通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。

功能模块	功能详情
漏洞管理	通过自动同步主机安全服务（Host Security Service，HSS）漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。
策略管理	支持统一管理应急策略。

威胁运营

威胁运营提供丰富的威胁检测模型，帮助您从海量的安全日志中，发现威胁、生成告警；同时，提供丰富的安全响应剧本，帮助您对告警进行自动研判、处置，并对安全防线和安全配置自动加固。

表 1-6 威胁运营功能介绍

功能模块		功能详情
事件管理		集中呈现事件详情，支持人工转事件、自动化转事件。
告警管理		通过集成各云服务告警，包含 HSS、WAF、DDoS 等，集中呈现告警信息。
情报管理		支持接入各云服务情报，同时也可以基于告警和事件自定义规则提取指标。
智能建模		支持构建告警模型。
安全分析	查询与分析	• 检索分析：支持数据的快捷检索分析，支持安全调查场景安全数据的快速筛留、筛除等操作，快速定位关键数据。 • 筛选统计：支持数据字段快速分析统计，并基于分析结果进行数据的快速筛选；时序数据支持默认时间分区统计，快速识别数据量的变化趋势，支持基于时间分区的快速筛选；支持分析、统计、排序等丰富统计分析函数，支撑快速构建安全分析模型。 • 可视化：支持数据可视化分析，直观反映业务结构性和趋势性特征，并基于此构建自定义分析报告和分析指标。
	数据监控	支持数据流量端到端的监控管理。
	数据消费	• 提供数据消费和生产的流式通信接口，提供数据管道集成 SDK，支持租户利用 SDK 进行系统集成，支持客户自定义数据的生产和消费。 • 提供 Logstash 开源采集软件插件，支持利用开源生态进行数据消费和生产。

安全编排

安全编排支持剧本管理、流程管理、数据类管理（安全实体对象）和资产连接管理等。同时，可以自定义剧本和流程等。

通过安全编排可以对安全响应剧本进行拖拽式的灵活编排，动态适配您的业务需求。也可以对安全运营的对象、交互的页面进行灵活扩展和定义。

表 1-7 安全编排功能介绍

功能模块	功能详情
运营对象	集中对数据类、数据类类型、分类映射等运营对象进行管理。
剧本编排	支持对剧本、流程、资产连接、实例的全生命周期管理。
页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。
插件管理	支持将安全编排流程中使用的插件进行统一管理。

数据采集

通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

表 1-8 数据采集功能说明

功能模块	功能详情
数据采集	使用 Logstash 通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

数据集成

通过集成云原生安全产品，进行联动操作或数据对接。集成后，可以检索并分析所有收集到的日志。

表 1-9 数据集成功能说明

功能模块	功能详情
数据集成	云内置采集系统，支持一键集成存储、管理与监管、安全等多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

1.3 产品优势

见微知著的指标脉络与态势呈现

您可以通过安全态势即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

云原生的资产盘点与风险预防

云上资产自动盘点，云安全配置自动检查，支持定位到资产，指导并辅助自动加固，帮助您告别黑资产、错配置的焦虑。同时避免传统的外挂式安全方案引入的隐式通道或安全设备漏洞。

智能高效的威胁检测与响应处置

专注于快速找到真正的威胁。通过每天对数十亿安全日志进行分析，利用多年沉淀经验，内置模型和研判剧本来降低合法事件的干扰。通过威胁及资产画像，与威胁告警环环关联，还原整个攻击链，配置自动化处置剧本进行响应，简化操作、提升安全性，提升了处理告警和事件的效率。

灵活的环境集成与作战协同

可通过配置连接到所有安全服务，进行数据对接或者联动操作；也可以定义您自己的模型、研判/处置剧本，以最佳适配您的安全需求。通过工作空间，还可以实现大型组织协同作战、MSSP（Managed Security Service Provider）托管等。

1.4 应用场景

云安全的理念是“三分建设，七分运营”，态势感知（专业版）的应用场景即是占了七分的安全运营。主要有以下几个应用场景：

日常安全运营

日常过程中，基于安全运营中关注的要素，对各个安全目标，执行各安全运营流程剧本，从而发现并消减风险，并对流程进行持续改进，避免风险再次发生。

重大保障

重大节日、假日、活动、会议期间，进行高强度 7*24 的安全保障，侧重于防攻击，保障业务可用性不因安全攻击受影响。

防护演练

国家机关单位、地方政府、企业组织的攻防演练中，进行高强度的安全防守保障，侧重于防入侵，保障不因入侵失分被问责（通报、批评等）。

安全评估

重大保障及防护演练前，信息全面的脆弱性盘点，包括白盒方式的基线评估、黑盒方式的攻击面、攻击路径探测。

1.5 计费说明

计费项

态势感知**专业版**按选购的资产配额数计费。

表 1-10 计费项说明

计费项	计费说明
资产配额	按购买的资产配额数计费。
按包周期购买计费	提供包月和包年的购买模式。
按需购买计费	即开即停，按小时结算。

计费模式

安全云脑的计费模式为包周期和按需计费。

- 包周期（包年/包月）
- 按需计费：按小时结算，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

变更配置

- 变更资产配额

  当您的资产数量增加，可在当前计费模式内增加资产配额数，不支持减少配额数。
- 退订

  若购买安全云脑后，需停止使用，请执行退订操作。

须知

不支持部分配额购买专业版。

续费

- 包周期购买的版本到期后，您可以单击“已购资源”页面中对应 region 栏的“续费”，跳转至续费管理页面完成续费，延长使用期。

  为避免版本到期未及时续费，导致安全风险，建议开通自动续费。开通自动续费后，系统将根据配置自动续费，无需手动操作。
- 按需计费是按小时计费，请确保账户余额充足，及时为账户充值。在账户余额充足的前提下，将持续为您提供防护服务，不影响使用。

到期与欠费

- 到期

  若包周期版本到期后，未及时续费，会根据“客户等级”和“订购方式”定义不同的保留期时长，保留期内专业版服务可继续使用。若保留期到期后，仍未及时续费，专业版会变为基础版。
- 欠费

  当您的账户欠费后，可查看欠费详情，此时账户将进入欠费状态，需要在约定时间内支付欠款。为避免相关服务不被停止，请及时为账户充值。

1.6 与其他云服务的关系

本章节主要介绍安全云脑与其他云服务之间的关系。

与安全服务的关系

安全云脑从主机安全（Host Security Service，HSS）、Web 应用防火墙（Web Application Firewall，WAF）等安全防护服务中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能 AI 分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

与弹性云服务器的关系

安全云脑为弹性云服务器（Elastic Cloud Server，ECS）提供资产安全管理服务，结合 HSS 主机防护状态，全方位呈现当前 ECS 安全风险态势，并提供相应防护建议。

1.7 基本概念

本节介绍态势感知（专业版）基本概念。

安全风险

安全风险是对资产安全状况的综合评估，反映了一段时间内资产遭受的安全风险。安全风险通常体现为一个量化的数值，便于用户理解目前资产的安全状况，数值大小并不代表资产的安全或危险，仅作为资产遭受攻击严重程度的参考。

威胁告警

广义的威胁告警是指由于自然因素、人为因素或软硬件本身的原因，对信息系统造成危害的事件，或对社会造成负面影响的威胁。对于态势感知（专业版）来讲，威胁告警泛指根据大数据分析检测出的，对用户资产产生威胁的安全事件。

工作空间

工作空间（Workspace）属于态势感知（专业版）顶层工作台，单个工作空间可绑定普通项目、企业项目和 Region，可支撑不同场景下的工作空间运营模式。

数据空间

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一载均衡策略。

数据管道

数据传输消息主题和存储索引组合为数据管道。

分类和映射

分类和映射是指对云服务告警进行类型匹配和字段映射。

安全编排

安全编排（Security Orchestration）是将企业和组织在安全运营过程中涉及的不同系统或者一个系统内部不同组件的安全功能通过可编程接口（API）封装后形成的安全能力（即应用）和人工检查点按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。

安全编排是将安全运营相关的工具/技术、流程和人员等各种能力整合到一起的一种协同工作方式。

生产者

是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。

订阅器

用于订阅态势感知（专业版）管道消息，一个管道可由多个订阅器进行订阅，态势感知（专业版）通过订阅器进行消息分发。

消费者

是用来接收并处理数据的运行实体，负责通过订阅器把态势感知（专业版）管道中的消息进行消费并处理。

消息队列

是数据存储和传输的实际容器。

威胁检测模型

是一种被训练的 AI 智能识别算法模型。能针对特定威胁，自动化的完成数据汇聚、分析和报警，这种检测模式具备较好的泛化能力，防躲避能力强，可在不同业务系统中发挥同等效果，应对复杂的新型攻击。

2 服务委托授权

操作场景

云服务委托可将相关云服务的操作权限委托给态势感知（专业版），让态势感知（专业版）以您的身份使用这些云服务，代替您进行一些任务调度、资源运维等工作。

当您**首次**使用态势感知（专业版）时，需要先进行委托授权，才能正常访问。

前提条件

已购买态势感知（专业版）。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

图 2-1 工作空间页面

步骤 4 在空间管理页面上方单击“服务委托授权-当前租户”，右侧弹出授权页面。

图 2-2 服务委托授权

步骤 5 在授权页面中，默认已勾选所需全部权限，请勾选权限下方的“同意授权”，并单击“确认”。

----结束

3 购买态势感知（专业版）

3.1 选择计费模式

态势感知（专业版）提供包年/包月、按需计费两种计费模式，以满足不同场景下的用户需求。

包周期计费

包年/包月的计费模式也称为包周期计费模式，是一种预付费方式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

适用于包周期的资源：资产配额，主要为主机配额。

按需计费

按需计费是按小时付费，是一种后付费方式，可以随时开通/取消。系统会根据资源的实际使用情况（按态势感知（专业版）服务的实际使用时长计费）每小时出账单，并从账户余额里扣款。

适用于按需的资源：资产配额，主要为主机配额。

3.2 购买专业版

操作场景

态势感知（专业版）专业版支持包周期和按需方式进行购买，本章节介绍如何购买专业版。

包周期方式

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在总览页面中，单击购买按钮，进入购买态势感知（专业版）页面。

步骤 4 （可选）首次购买需要进行访问授权。在弹出的访问授权页面中，勾选同意授权并单击“确认”。

步骤 5 在购买态势感知（专业版）页面，配置购买参数。

表 3-1 包周期购买专业版参数说明

参数名称	说明
计费模式	此处选择“包周期”，按配置周期计费。
区域	选择您所在的区域。
版本	选择“专业版”。
主机配额	主机配额是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 **说明** • 主机配额最大限制为 10000 台。 • 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。
购买时长	选择“购买时长”。 **说明** 选择 1 月时，支持自动续费，当服务期满时，系统会自动按照购买周期进行续费。

步骤 6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤 7 确认订单详情无误后，单击“去支付”。

步骤 8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

按需方式

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在总览页面中，单击购买按钮，进入购买态势感知（专业版）页面。

步骤 4 （可选）首次购买需要进行访问授权。在弹出的访问授权页面中，勾选同意授权并单击“确认”。

步骤 5 在购买态势感知（专业版）页面，配置购买参数。

表 3-2 按需购买专业版参数说明

参数名称	说明
计费模式	此处选择“按需”，按小时计费。从开通开始到取消结束，按实际防护时长（小时）计费。
区域	选择您所在的区域。
版本	选择“专业版”。
主机配额	主机配额是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 说明 ● 主机配额最大限制为 10000 台。 ● 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。

步骤 6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤 7 确认订单详情无误后，单击“确认开通”。

步骤 8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

生效条件

付款成功后，您可以在管理控制台“已购资源”页面查看当前购买的态势感知（专业版）版本。

3.3 增加配额

操作场景

购买态势感知（专业版）资产配额完成后，当用户资产数量增加，或需对不同资产有不同使用时长需求，可参考本章节扩充“主机配额”，并配置使用时长。

约束与限制

- 主机配额是授权检测主机的数量。主机配额最大限制为 10000 台。
- 在购买态势感知（专业版）时，选择的最大配额需等于或大于当前账户下主机总数量，且不支持减少。若购买的最大配额小于主机数量，可能会造成未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源页面后，在待购买态势感知（专业版）专业版所在 region 栏中，单击“增加配额”。

步骤 4 在购买态势感知（专业版）页面，配置购买参数。

1. “当前配置”：显示已选择 region 态势感知（专业版）版本信息，无需配置。
2. “升级方式”：选择“增加配额”。
3. “主机配额”：配置主机配额。

表 3-3 主机配额参数说明

参数	说明
主机配额	主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 **说明** ● 主机配额最大限制为 10000 台。 ● 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。

步骤 5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤 6 确认订单详情无误后，单击“去支付”。

步骤 7 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

3.4 续费

操作场景

态势感知（专业版）续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不可变更版本规格，即不能改变“主机配额”。

续费操作仅针对**包周期**版本规格。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期版本到期时，用户需通过续费延长使用期。

- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源页面后，在待续费态势感知（专业版）版本所在 region 栏中，单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤 4 在态势感知（专业版）实例所在行，单击“续费”，跳转至“续费”页面。

步骤 5 配置“续费时长”，如选择“一年”。

步骤 6 （可选）设置并勾选“统一到期时间”。默认将统一到期时间设置为每月 1 号 23:59:59 GMT+08:00。

步骤 7 单击“去支付”，跳转至支付页面，完成付款。

步骤 8 返回续费管理页面，可查看态势感知（专业版）已续费成功。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本的资产配额、增值包、安全编排将自动续费，延长使用周期。

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。

3.5 退订

操作场景

若用户不再使用态势感知（专业版）防护功能或增值包，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购 5 天内的资源，支持每年 10 次 5 天无理由“退订”；使用超过 5 天的资源，“退订”需要收取手续费。
- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

退订包周期计费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对包周期购买的资产配额、或增值包，单击“退订”，进入“退订管理”列表页面。

步骤 5 在需要退订的实例所在行，单击“操作”列中的“退订资源”，进入“退订资源”页面。

步骤 6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤 7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

4 安全总览

4.1 总览

态势感知（专业版）“总览”页面实时呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全，帮助您全量了解资产的安全情况，包括资产的安全评估结果、安全监控和安全趋势等信息。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“总览”，进入态势感知（专业版）总览页面。

步骤 4 在总览页面查看您的资产安全总览情况，并进行相关操作。“总览”分为以下几个板块：

- 安全评分
- 安全监控
- 安全趋势

各个板块数据统计周期及更新频率如下表所示：

表 4-1 总览

参数名称	统计周期	更新频率	说明
安全评分	实时	• 每天 2:00 自动更新 • 随手动单击“重新检测”更新而更新	根据是否开启各安全服务防护、未处理的配置问题等级及个数、未处理的漏洞等级及个数、未处理的威胁事件等级及个数等计算而来，具体评分详细信息请参见 4.2 安全评分。

参数名称	统计周期	更新频率	说明
威胁告警	近 7 天	每 5 分钟	本账号态势感知（专业版）下全部工作空间告警管理中的告警总和。
漏洞	近 7 天	每 5 分钟	本账号态势感知（专业版）下全部工作空间漏洞管理中的漏洞总和。
合规检查	实时	每 5 分钟	本账号态势感知（专业版）下全部工作空间基线检查中的问题总和。
安全趋势	近 7 天	每 5 分钟	近 7 天的安全评分数据。

----结束

安全评分

“安全评分”板块根据态势感知（专业版）的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。

图 4-2 安全评分

- 安全评分每天凌晨 2:00 自动更新，也支持通过单击“重新检测”来进行实时更新。
- 分值范围为 0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见 4.2 安全评分。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。资产安全风险修复后，也可以直接单击“重新检测”，重新检测资产并进行评分。

说明

资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

- 安全评分显示为历史扫描结果，**非实时**数据，如需获取最新数据及评分，可单击“重新检测”，获取最近的数据。

安全监控

“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

图 4-3 安全监控

表 4-2 安全监控参数说明

参数名称	参数说明
威胁告警	呈现**近 7 天内**本账号所有工作空间内未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 • 单击威胁告警模块，系统将列表实时呈现**近 7 天内** TOP5 的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 列表呈现近 7 天 TOP5 的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 若列表显示内容为空，表示近 7 天无威胁告警事件。

参数名称	参数说明
漏洞	展示您本账号所有工作空间内资产中 TOP5 漏洞类型，以及**近 7 天内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 高危：即高危风险，表示资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 中危：即中危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“漏洞类型 Top5”栏，系统将列表呈现 TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的 TOP 等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 仅当主机中 Agent 版本为 2.0 时，才会在“漏洞类型 Top5”中显示对应数据。如未显示数据或需要查看 TOP5 漏洞类型，请将主机将 Agent1.0 升级至 Agent2.0。 • 单击漏洞模块中的“实时监控最新漏洞风险事件 Top5”栏，系统将列表实时呈现**近 7 天内** TOP5 的漏洞事件，可快速查看漏洞详情。 – 列表呈现当日最新 TOP5 漏洞事件详情，包括漏洞名称、漏洞等级、资产名称、漏洞发现时间。 – 若列表显示内容为空，表示当日无漏洞事件。
合规检查	展示您本账号所有工作空间内资产中存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了不合规配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常配置，建议您立即查看合规检查事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常配置，建议您及时查看该合规检查项目的详情。 • 单击合规检查异常模块，系统将列表实时呈现 TOP5 的合规检查异常事件，可快速查看合规检查详情。 – 列表呈现最近一次合规检查中 TOP 的合规异常事件详情，包括合规检查项目名称、等级、受影响资产数量、发现时间。 – 若列表显示内容为空，表示近 30 天无合规异常事件。

安全趋势

“安全趋势”板块展示**近 7 天内**您的整体资产安全健康得分的趋势图。更新频率为每 5 分钟更新一次。

图 4-4 安全趋势

4.2 安全评分

操作场景

态势感知（专业版）实时呈现您云上资产的整体安全评估状况，并根据态势感知（专业版）的威胁检测能力，评估整体资产安全健康得分。

安全评分每天凌晨 2:00 自动更新，也支持通过在页面中单击“重新检测”来进行实时更新。

本章节将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

安全分值

态势感知（专业版）根据威胁检测能力，评估整体资产安全健康得分。

- 风险等级包括“无风险”、“提示”、“低危”、“中危”、“高危”和“致命”。
- 分值范围为 0～100，分值越大表示风险越小，资产更安全。
- 分值从 0 开始，每隔 20 取值范围对应不同的风险等级，例如分值范围 40~60 对应风险等级为“中危”。
- 分值环形图不同色块表示不同威胁等级，例如黄色对应“中危”。
- 资产风险修复，并手动刷新告警事件状态后，安全评分可以通过手动单击“重新检测”进行更新。

说明

资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

表 4-3 安全分值表

风险等级	安全分值	分值说明
无风险	100 分	恭喜您，您的资产当前安全状况良好。
提示	80≤分值<100	您的资产存在少量的安全隐患，建议您及时加固安全防护体系。
低危	60≤分值<80	您的资产存在较多的安全隐患，建议您及时加固安全防护体系。
中危	40≤分值<60	您的资产防御黑客入侵的能力较弱，建议您立即加固安全防护体系。
高危	20≤分值<40	您的资产存在较高的黑客入侵和病毒感染的风险，建议您立即处理。
致命	0≤分值<20	您的资产很可能遭受到黑客入侵和病毒感染的威胁，建议您立即处理。

安全评分扣分项

安全评分扣分项及其分值情况如表 4-4 所示。

表 4-4 安全评分扣分项

分类	扣分项	单项扣分值	处理建议	最高扣分上限
安全服务启用	未开启安全相关服务	-	开启安全相关服务	30
合规检查	存在未处理的致命不合规项	10	按照合规修复建议指导进行合规问题修复，修复后重新触发扫描任务，自动刷新评分。	20
	存在未处理的高危不合规项	5		
	存在未处理的中危不合规项	2		
	存在未处理的低危不合规项	0.1		
漏洞	存在未处理的致命漏洞	10	按照漏洞修复建议指导进行漏洞修	20

分类	扣分项	单项扣分值	处理建议	最高扣分上限
	存在未处理的高危漏洞	5	复，修复后重新触发漏洞扫描任务，自动刷新评分。	
	存在未处理的中危漏洞	2		
	存在未处理的低危漏洞	0.1		
威胁告警	存在未处理的致命告警事件	10	按照威胁事件处置指导建议进行修复，修复后自动刷新评分。	30
	存在未处理的高危告警事件	5		
	存在未处理的中危告警事件	2		
	存在未处理的低危告警事件	0.1		

5 工作空间

5.1 工作空间概述

本章节将介绍工作空间的定义、类型和基本操作等内容。

什么是工作空间？

工作空间（Workspace）属于态势感知（专业版）顶层工作台。

- 空间管理：

  单个工作空间可绑定普通项目，可支撑不同场景下的工作空间运营模式。
- 空间托管：
  - 工作空间数据委托：单租所有工作空间按照租户实际运营汇聚到某一个工作空间做集中安全运营，跨租汇聚安全运营。
  - 工作空间委托：跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。

什么是数据空间？

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一载均衡策略。

什么是数据管道？

数据传输消息主题和存储索引组合为数据管道。

工作空间通用规则

- 单账号单 Region 内最多创建 5 个工作空间。
- 一个工作空间中最多可创建 5 个数据空间。
- 一个数据空间中最多可创建 20 个数据管道。

5.2 新增工作空间

操作场景

工作空间（Workspace）属于态势感知（专业版）顶层工作台，单个工作空间可绑定普通项目、企业项目，可支撑不同场景下的工作空间运营模式。

在态势感知（专业版）前，需要创建工作空间，它可以将资源划分为各个不同的工作场景，避免资源冗余查找不便，影响日常使用。

本章节介绍如何新增工作空间。

约束与限制

单账号单 Region 内最多创建 5 个工作空间。

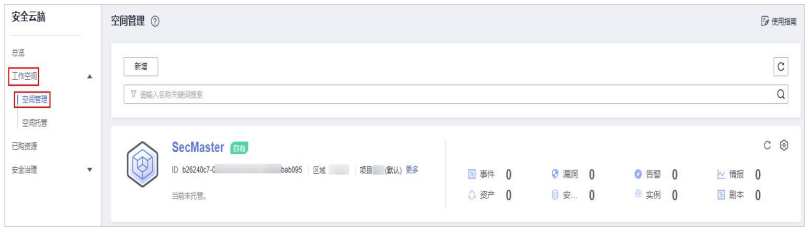
操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

图 5-1 工作空间页面



步骤 4 在工作空间管理页面中，单击“新增”，系统从右侧弹出新增工作空间页面。

步骤 5 配置新建工作空间参数，参数说明如下表所示：

表 5-1 新增工作空间

参数名称	参数说明
区域	选择待新增工作空间所在区域。

参数名称	参数说明
企业项目	可选参数，在下拉列表中选择您所在的企业项目。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。 说明 “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
工作空间名称	自定义工作空间的名称。命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 64 个字符。
标签	可选参数，添加该工作空间的标签，用于标识工作空间，方便您对工作空间进行分类和跟踪。
描述	可选参数，设置该工作空间的备注信息。

步骤 6 单击“确定”，完成工作空间的新增。

----结束

5.3 空间管理

5.3.1 查看工作空间详情

操作场景

本章节将介绍用户通过管理控制台查看工作空间的信息，包括名称、类型和创建时间等。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

图 5-2 工作空间页面

步骤 4 在工作空间界面，查看已有工作空间的信息。

当工作空间较多时，可以通过搜索功能，选择搜索条件并在搜索框中输入关键词，单击，即可快速查询指定工作空间。

图 5-3 工作空间详情

表 5-2 工作空间参数说明

参数名称	参数说明
名称	工作空间的名称。
类型	工作空间的类型。
ID	工作空间的 ID。
区域	工作空间所属区域。
项目	工作空间所属的项目。
更多	单击“更多”可查看工作空间详细信息。
托管状态	工作空间是否托管。
事件	该工作空间中的事件数量。
漏洞	该工作空间中的漏洞数量。
告警	该工作空间中的告警数量。
情报	该工作空间中的情报数量。
资产	该工作空间中已有资产的数量。
安全分析	该工作空间中已有数据空间数量。
实例	该工作空间中已有实例的数量。
剧本	该工作空间中已有剧本的数量。

步骤 5 如需查看某个工作空间的详细信息，可单击待查看工作空间右侧的，进入工作空间基本信息页面查看详细信息。

图 5-4 工作空间基本信息

----结束

5.3.2 编辑工作空间

操作场景

工作空间新增成功后，您可以对工作空间的基本信息（**名称**、**标签**和**描述**）进行修改。

该任务指导您如何编辑工作空间。

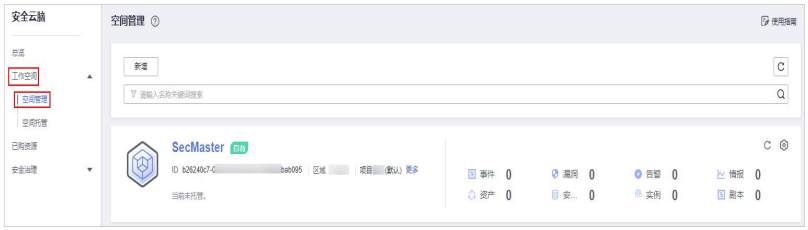
操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

图 5-5 工作空间页面



步骤 4 单击待编辑工作空间右侧的，进入工作空间详情页面。

图 5-6 工作空间详情页面入口

步骤 5 在工作空间的“基本信息”页签中，单击“编辑”。

步骤 6 编辑工作空间名称、标签或描述后，单击“保存”。

----结束

5.3.3 删除工作空间

操作场景

如果不再需要某个工作空间，可以参照本章节进行删除。

工作空间删除后，相关的资产会存在风险，且会影响资产的风险预防和处理，安全性能降低，删除后不可恢复，请谨慎操作。

约束与限制

- 删除时，工作空间内运行的剧本、流程、引擎等将立即停止。
- 选择永久删除，工作空间内的所有内容将永久删除无法恢复。

删除工作空间

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，进入态势感知（专业版）工作空间页面。

图 5-7 工作空间页面

步骤 4 单击待删除工作空间右侧的⚙，进入工作空间详情页面。

图 5-8 工作空间详情页面入口

步骤 5 在工作空间的“基本信息”页签中，单击“删除”。

步骤 6 在弹出的删除工作空间页面中，确认无误后，勾选“永久删除工作空间”，并在“确认删除”中输入工作空间名称，并单击“删除”。

⚠ 注意

- 删除时，工作空间内运行的剧本、流程、引擎等将立即停止。
- 选择永久删除，工作空间内的所有内容将永久删除无法恢复。

----结束

5.4 空间托管

5.4.1 概述

空间托管是指跨账号安全运营，可实现 Workspace 委托集中安全运营查看统一资产风险、告警和事件等。

表 5-3 空间托管流程

操作步骤		说明
1	5.4.2 创建托管视图	创建托管视图管理托管任务。
2	5.4.3 创建托管	态势感知（专业版）支持将项目中的工作空间托管给其他用户，托管后，可实现 Workspace 委托集中安全运营查看统一资产风险、告警和事件等。
3	5.4.4 托管授权	由于托管是将本项目中的工作空间托管给其他用户，因此，需要双重授权。 1. 创建委托后，需要先在已有账号中，接收授权，同意将工作空间托管给其他用户。 2. 然后在目标账号的“工作空间 > 空间托管 > 我纳管的”菜单下进行托管授权，统一接收托管。 授权后，被托管空间将挂载到托管账号下的空间中，进行统一管理。

约束与限制

- 单账号单 Region 内最多创建 1 个空间托管视图。
- 单账号单 Region 空间托管视图（包含的纳管工作空间数）中的工作空间数 ≤ 100 个。
- 跨账号跨 Region 空间托管视图（包含的纳管工作空间数）中的工作空间数 ≤ 10 个。
- 单账号创建账号委托 ≤ 50 个。

5.4.2 创建托管视图

操作场景

创建托管前，需先创建托管视图。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

图 5-9 空间托管页面

步骤 4 在“托管视图”页签中，单击“创建托管视图”，右侧弹出创建托管视图页面。

步骤 5 配置托管视图参数。

表 5-4 创建托管视图参数说明

参数名称	参数说明
托管视图名称	设置托管视图名称。
绑定空间名称	选择需要绑定的工作空间。
描述	自定义托管视图描述信息。

步骤 6 单击“确定”。

创建成功后，可以在“空间管理”或“空间托管”页面中查看已创建的托管视图。

----结束

相关操作

- 编辑托管视图
  a. 在待编辑托管视图所在行“操作”列，单击“编辑”。
  b. 在弹出的编辑托管视图中，修改托管视图参数后，单击“确定”。
- 删除托管视图
  a. 在待删除视图所在行“操作”列，单击“删除”。
  b. 在弹出确认框中，单击“确认”。

5.4.3 创建托管

操作场景

态势感知（专业版）支持将项目中的工作空间托管给其他用户，托管后，可实现Workspace 委托集中安全运营查看统一资产风险、告警和事件等。

前提条件

- 接收托管方已创建托管视图，具体操作请参见 5.4.2 创建托管视图。
- 托管方需要已授权云服务关联委托权限。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

图 5-10 空间托管页面

步骤 4 单击页面右上角“创建托管”，右侧弹出创建托管页面。

步骤 5 配置托管参数。

表 5-5 创建托管参数说明

参数名称		参数说明
发起方式		空间托管的发起方式默认为当前租户。
托管方	托管空间	选择托管工作空间。
受托管方	租户	输入受托管方用户的账号名称。获取方式如下： 1. 已登录管理控制台，并将鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，默认进入 API 凭证页面。 2. 在 API 凭证页面中，获取“账号名”。
	托管视图	选择已有的托管视图。
托管信息	托管名称	设置托管名称。
	托管时长	选择托管时长。
	托管策略	选择托管策略。
	描述	自定义托管描述信息。

步骤 6 单击“确认”。

----结束

后续处理

托管创建后，需进行托管授权，详细操作请参见 5.4.4 托管授权。

5.4.4 托管授权

操作场景

托管创建完成后，需要到目标工作空间所属账号中进行授权。授权后，被托管空间将挂载到托管账号下的空间中，进行统一管理。

前提条件

已创建托管，详细操作请参见 5.4.3 创建托管。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

图 5-11 空间托管页面

步骤 4 在托管页面中，选择“我纳管的”页签，并在目标托管任务所在行“操作”列，单击“接收”。

步骤 5 在弹出的确认框中，单击“确认”。

----结束

后续处理

授权后，可以在“工作空间 > 空间管理”页面中查看已创建的托管视图，单击视图名称，进入后，可以查看被托管空间的详细信息。

5.4.5 管理托管

操作场景

空间托管页面中，可以管理托管视图、我纳管的和纳管我的。

- 托管视图：查看已创建的托管视图及其详细信息。
- 我纳管的：列表呈现有哪些工作空间托管在我创建的托管视图中。
- 纳管我的：列表呈现我的工作空间被哪些托管视图纳管着。

托管视图

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

图 5-12 空间托管页面

步骤 4 在托管页面中，选择“托管视图”页签，进入托管视图页面。

步骤 5 在托管视图页面中，可以查看和管理托管视图。

- 查看托管视图

表 5-6 查看托管视图

参数名称	参数说明
托管视图名称	托管视图的名称。
区域	托管视图所在的区域。
绑定空间名称/ID	托管视图绑定的工作空间的名称和 ID 信息。 单击绑定工作空间名称，可以快速进入该工作空间。
纳管空间数量	托管视图中绑定的工作空间数量。
创建时间	托管视图的创建时间。
描述	托管视图的描述信息。
操作	可以对托管视图进行编辑、删除操作。

- 编辑托管视图
  a. 在待编辑托管视图所在行“操作”列，单击“编辑”。
  b. 在弹出的编辑托管视图中，修改托管视图参数后，单击“确定”。
- 删除托管视图
  a. 在待删除视图所在行“操作”列，单击“删除”。
  如果需要删除多个视图，可以在列表中勾选需要删除的视图，并单击列表上方“批量删除”。
  b. 在弹出确认框中，单击“确认”。

----结束

我纳管的

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

图 5-13 空间托管页面

步骤 4 在托管页面中，选择“我纳管的”页签，进入我纳管的页面。

步骤 5 在我纳管的页面中，可以查看和管理我纳管的任务。

- 查看我纳管的

表 5-7 查看我纳管的

参数名称	参数说明
托管名称	托管视图的名称。
名称/ID	被我的托管视图纳管的工作空间的名称和 ID。
发起方式	托管任务的发起方式。
托管状态	托管任务的托管状态。
选中状态	托管任务的选中状态。
托管时长	托管任务的时长。
托管时间	托管任务的开始时间。
托管策略	托管任务使用的策略。
操作	可以对我纳管的任务进行接收、删除操作。

- 接收：接收托管。
  a. 在待接收拖管所在行“操作”列，单击“接收”。
     如果需要接收多个拖管关系，可以在列表中勾选需要接收的拖管关系，并单击列表上方“批量接收”。
  b. 在弹出确认框中，单击“确认”。
- 拒绝：拒绝托管关系。
  a. 在待拒绝拖管所在行“操作”列，单击“拒绝”。

如果需要拒绝多个拖管关系，可以在列表中勾选需要拒绝的拖管关系，并单击列表上方“批量拒绝”。

b. 在弹出确认框中，单击“确认”。

- 解除：解除托管关系。
  a. 在待解除拖管所在行“操作”列，单击“更多 > 解除”。
     如果需要解除多个托管关系，可以在列表中勾选需要解除的拖管关系，并单击列表上方“批量解除”。
  b. 在弹出确认框中，单击“确认”。
- 删除：删除托管任务。
  a. 在待删除拖管所在行“操作”列，单击“更多 > 删除”。
     如果需要删除多个拖管，可以在列表中勾选需要删除的拖管，并单击列表上方“批量删除”。
  b. 在弹出确认框中，单击“确认”。

----结束

纳管我的

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间托管”，进入空间托管管理页面。

图 5-14 空间托管页面

步骤 4 在托管页面中，选择“纳管我的”页签，进入纳管我的页面。

步骤 5 在纳管我的页面中，可以查看和管理纳管我的。

- 查看纳管我的

表 5-8 查看我纳管的

参数名称	参数说明
托管名称	托管视图的名称。
名称/ID	我方工作空间的名称和 ID 信息。

参数名称	参数说明
受托管方	工作空间的受托管方信息。
发起方式	托管任务的发起方式。
托管视图名称	托管任务所属的托管视图的名称。
托管时长	托管任务的时长。
托管状态	托管任务的托管状态。
托管时间	托管任务的开始时间。
托管策略	托管任务的策略。
操作	可以对托管关系进行修改、删除等操作。

- 修改：修改已接收的托管任务。
  a. 在待修改拖管所在行“操作”列，单击“修改”。
  b. 在弹出编辑页面中修改托管信息。
  c. 单击“确认”。
- 撤回：撤回已接收的托管任务。
  a. 在待撤回拖管所在行“操作”列，单击“撤回”。
     如果需要撤回多个解除关系，可以在列表中勾选需要撤回的拖管关系，并单击列表上方“批量撤回”。
  b. 在弹出确认框中，单击“确认”。
- 重申：如果受纳管方拒绝了托管，可发起再次申请操作。
  a. 在待解除拖管所在行“操作”列，单击“更多 > 重申”。
  b. 在弹出确认框中，单击“确认”。
- 解除：解除托管关系。
  a. 在待解除拖管所在行“操作”列，单击“更多 > 解除”。
     如果需要解除多个托管关系，可以在列表中勾选需要解除的拖管关系，并单击列表上方“批量解除”。
  b. 在弹出确认框中，单击“确认”。
- 删除：删除托管任务。
  a. 在待删除拖管所在行“操作”列，单击“更多 > 删除”。
     如果需要删除多个拖管，可以在列表中勾选需要删除的拖管，并单击列表上方“批量删除”。
  b. 在弹出确认框中，单击“确认”。

----结束

6 查看已购资源

操作场景

在态势感知（专业版）的已购资源中可统一呈现当前账号已经申请的资源，方便统一管理已购资源。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源管理页面。

步骤 4 在已购资源页面查看详细信息。

- 总览：
  - 已开通区域/总区域：当前账号已开通云脑的区域。
  - 可升级：当前账号的所有已购版本中，可以升级的资源数量。
  - 将到期版本：即将到期的规格及增值包数量。
  - 总配额：当前账号已购买的总配额数量。
- 各区域具体购买态势感知（专业版）资源的详细情况。

----结束

7 安全治理

7.1 概述

什么是安全治理？

安全治理是态势感知（专业版）中的一个自动化合规评估和安全治理功能，以“云服务网络安全与合规标准”（Cloud Service Cybersecurity & Compliance Standard，3CS）为基座，将全球安全合规经验服务化，开放 PCI DSS、ISO27701、ISO27001 等安全治理模板，将合规语言 IT 化实现自动化扫描，可视化呈现合规状态，一键生成合规遵从性报告，帮助用户快速实现云上业务的安全遵从，提升租户获得法规及行业标准认证的效率。

功能特性

安全治理为您提供安全治理模板与合规策略扫描服务，将安全遵从包内的法规标准条款转化成检查项。

- 提供安全遵从包

  提供安全治理模板，包含法规标准条款原文、扫描策略、自评估检查项以及专家的改进建议，覆盖 PCI DSS、ISO27701、ISO27001、隐私等法规标准。用户可以订阅、取消订阅安全遵从包，查看合规评估与治理结果。

- 合规策略扫描

  Policy as Code，将安全遵从包内的法规标准条款代码化，周期性、自动化扫描云上资产的合规情况，可视化看板呈现风险，提供专家改进建议。

- 自评估检查项

  将安全遵从包内的法规标准条款转化成检查项，租户可根据检查项完成自身业务的合规评估，查看历史评估结果，进行证据上传和下载，根据专家改进建议进行治理。

- 合规结果可视

  可视化呈现合规评估结果与安全治理情况，包括租户订阅的法规、标准条款遵从概况，各安全遵从包状态，各策略扫描概况。

功能优势

- 全球合规治理经验服务化

  安全治理以“云服务网络安全与合规标准”（Cloud Service Cybersecurity & Compliance Standard，3CS）为基座，将全球安全合规经验服务化，开放安全治理模板，将法规条款、标准要求转化为业务语言、IT 语言，帮助客户识别自身合规状态。

- 提升获得法规及行业标准认证的效率

  安全治理开放 PCI DSS、ISO27701、ISO27001 等安全治理模板，内含合规策略和自评估检查项；合规策略将自动化、持续性扫描租户云上资产的合规状态，自评估检查项将帮助租户快速梳理业务情况；并且安全治理提供证据链管理功能，支持一键导出报表，可极大提升租户获得法规及行业标准认证的效率。

- 高效实施安全治理动作

  安全治理通过数据看板将所有的合规情况集中展示，向用户显示当前的安全性与合规性状态。租户可以轻松发现识别潜在问题，并根据专家建议采取必要的安全治理动作。

7.2 安全遵从包规格说明

安全治理提供安全遵从包，您可以根据不同遵从包的判定指引来选择所需的安全遵从包。

- 安全标准遵从包

安全标准遵从包

当前可选择的安全标准遵从包如表 7-1 所示，用户依据**判定指引**选择并订阅安全遵从包。

表 7-1 安全标准遵从包一览

遵从包名称	描述	适用区域	分类	领域	判定指引

遵从包名称	描述	适用区域	分类	领域	判定指引
PCI DSS 安全遵从包	该遵从包依据广受国际认可的数据安全标准-支付卡行业数据安全标准 (PCI DSS 3.2.1 版，2018 年 5 月)，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评数据安全管理情况，并结合 PCI DSS 给出了数据安全方面的改进建议，帮助企业提升数据安全水平。	全球	行业标准	数据安全	1. 您是否作为参与支付卡处理的实体，包括商户、处理商、收单机构、发卡机构和服务提供商？ 2. 您是否存储、处理或传输持卡人数据（主账户信息（PAN，一般为银行卡号）、持卡人姓名、银行卡有效期、业务码）或敏感验证数据（全磁道数据、信用卡安全码、PIN）？ 3. 您是否期望对您在数据安全方面的风险进行识别，并获知如何采取措施降低风险？ 若以上任一回答为是，建议您订阅该遵从包。
ISO 27001 安全遵从包	该遵从包依据国际上公认的 ISO 27001 信息安全管理体系要求（2013 版），提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评信息安全管理情况，并给出了信息安全方面的改进建议，帮助企业提升信息安全水平。	全球	国际标准	信息安全	ISO 27001 为组织建立、实施、运行、保持和持续改进信息安全管理体系规定了要求，是一项具有普适性的信息安全标准。 如您期望对您在信息安全方面的风险进行识别，并获知如何采取措施降低风险，建议您订阅该遵从包。

遵从包名称	描述	适用区域	分类	领域	判定指引
ISO 27701 安全遵从包	该遵从包依据国际上公认的 ISO 27701 隐私信息管理要求和指南（2019 版），提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评隐私信息管理情况，并给出了隐私保护方面的改进建议，帮助企业贯彻隐私保护的责任，提升隐私保护及信息安全水平。	全球	国际标准	隐私保护	1. 您是否涉及处理（包括收集、使用、传输、存储、删除等）个人可识别信息（简称“PII”，如姓名、电话号码、电子邮箱、身份证件信息等，在本遵从包中也称作“个人数据”）？ 2. 您是否作为 PII 控制者（决定 PII 处理目的和方法的隐私利益相关方，在本遵从包中也称作“数据控制者”）和/或 PII 处理者（代表 PII 控制者，并按照 PII 控制者的指示对 PII 进行处理的隐私利益相关方，在本遵从包中也称作“数据处理者”）的角色？ 3. 您是否期望对您在隐私保护方面的风险进行识别，并获知如何采取措施降低风险？ 若以上任一回答为是，建议您订阅该遵从包。

遵从包名称	描述	适用区域	分类	领域	判定指引
等保 2.0 标准四级安全遵从包	该遵从包依据国家标准 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》中四级的安全要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评网络安全管理情况，并给出了网络安全等级保护的改进建议，帮助企业建设网络安全体系，提升网络安全水平。	中国	国家标准	网络安全	1. 您是否涉及网络安全等级保护工作的作用对象，主要包括基础信息网络（为信息流通、信息系统运行等起基础支撑作用的信息网络，包括电信网、广播电视传输网、互联网、业务专网等网络设备设施）、信息系统（例如工业控制系统、云计算平台、物联网、使用移动互联技术的信息系统以及其他信息系统）和大数据等？ 2. 您是否期望对网络实施分级保护措施，在网络安全保护方面的风险进行识别，并获知如何采取措施降低风险？ 若以上任一回答为是，建议您订阅该遵从包。
等保 2.0 标准三级安全遵从包	该遵从包依据国家标准 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》中三级的安全要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评网络安全管理情况，并给出了网络安全等级保护的改进建议，帮助企业建设网络安全体系，提升网络安全水平。	中国	国家标准	网络安全	1. 您是否涉及网络安全等级保护工作的作用对象，主要包括基础信息网络（为信息流通、信息系统运行等起基础支撑作用的信息网络，包括电信网、广播电视传输网、互联网、业务专网等网络设备设施）、信息系统（例如工业控制系统、云计算平台、物联网、使用移动互联技术的信息系统以及其他信息系统）和大数据等？ 2. 您是否期望对网络实施分级保护措施，在网络安全保护方面的风险进行识别，并获知如何采取措施降低风险？ 若以上任一回答为是，建议您订阅该遵从包。

7.3 使用流程

安全治理功能的使用流程如表 7-2 所示。

图 7-2 使用流程

表 7-2 使用流程

子流程	说明
7.4 服务授权	使用安全治理功能前，需要获取访问云服务资源的权限，授权后，才能通过策略扫描帮您快速识别云上资产的安全遵从情况。
7.5 订阅安全遵从包	态势感知（专业版）提供有不同的安全遵从包，您可以选择所需的安全遵从包。
7.6 用户自评估	订阅安全遵从包后，您可以遵从包的条款进行自评估，以便识别业务遵从情况。
查看结果	策略扫描或自评估后，您可以查看安全治理情况： • 7.7 安全合规总览：查看法规、标准条款遵从概况、各安全遵从包状态、策略扫描概况。 • 7.8 查看治理结果：查看各个安全遵从包整体遵从情况和各条款的详细信息。 • 7.9 查看策略扫描结果：查看策略扫描结果及其详细信息。

7.4 服务授权

操作场景

使用安全治理功能前，需要获取访问云服务资源的权限，授权后，才能通过策略扫描帮您快速识别云上资产的安全遵从情况。

本章节将介绍如何授权访问用户云上资产。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 7-3 进入订阅列表页面

步骤 4 在订阅列表页面中，单击流程引导“服务授权”中的“授权”按钮，弹出服务授权确认框。

步骤 5 在弹出服务授权确认框中，单击“同意授权”，完成授权。

----结束

7.5 订阅安全遵从包

操作场景

安全遵从包是指开放的安全治理模板，包含法规标准条款原文、扫描策略、自评估检查项以及专家的改进建议，覆盖 PCI DSS、ISO27701、ISO27001、隐私等法规标准。

本章节将介绍如何订阅安全遵从包。

前提条件

已完成服务授权。如未授权，请先进行服务授权操作，详细操作请参见 7.4 服务授权。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 7-4 进入订阅列表页面

步骤 4 在订阅列表页面中单击“订阅安全遵从包”，进入订阅安全遵从包页面。

如果是首次订阅，请单击流程引导“订阅安全遵从包”中的“订阅”按钮，进入订阅安全遵从包页面。

步骤 5 在订阅安全遵从包页面中，选择需要订阅的安全遵从包，单击右下角的“确认订阅”。

步骤 6 在弹出的订阅成功确认框中单击“返回”，可以返回订阅列表页面，查看已订阅的安全遵从包的详细信息。

如果需要立即进行自评估，可以在弹出的订阅成功确认框中单击“自评估”，进行评估。详细操作请参见 7.6 用户自评估。

----结束

7.6 用户自评估

操作场景

订阅安全遵从包后，用户可以依据国际标准进行自评估。

前提条件

已订阅安全遵从包，详细操作请参见 7.5 订阅安全遵从包。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 7-5 进入订阅列表页面

步骤 4 单击待自评估遵从包名称左侧的 按钮，展开遵从包信息。展开后，在租户自评估栏操作列单击“自评”，进入自评估页面。

图 7-6 自评估

步骤 5 在租户自评估页面，对每个检查项进行自评。

图 7-7 自评估界面

- 如需上传附件，可单击评估项目的“查看附件 > 附件上传”，上传相关的凭据信息。
- 租户自评的过程中，单击评估项目右侧的“参考指导”，可查看该检查项的基本信息、相关的条款以及历史记录。

步骤 6 评估完成后，单击右下角的“提交”。

----结束

7.7 安全合规总览

操作场景

订阅安全遵从包后，在合规总览界面可查看当前已订阅的安全遵从包的法规、标准条款遵从概况和策略扫描概况。

前提条件

已订阅安全遵从包，详细操作请参见 7.5 订阅安全遵从包。

查看法规、标准条款遵从概况

步骤 1 登录管理控制台。

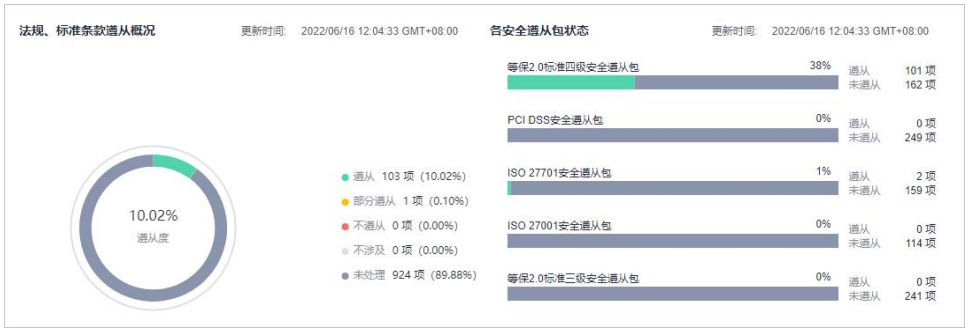
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 合规总览”，进入合规总览页面。

图 7-8 进入合规总览页面

步骤 4 在合规总览页面中，查看“法规、标准条款遵从概况”。

图 7-9 法规、标准条款遵从概况



----结束

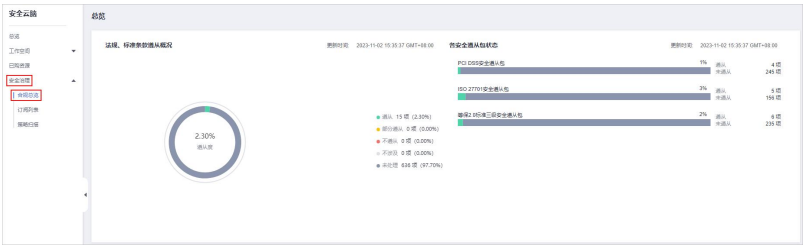
查看策略扫描概况

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

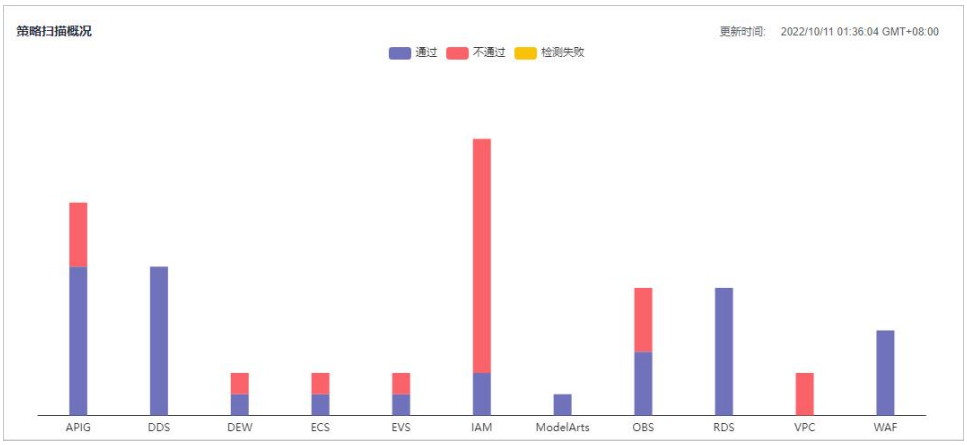
步骤 3 在左侧导航栏选择“安全治理 > 合规总览”，进入合规总览页面。

图 7-10 进入合规总览页面



步骤 4 在合规总览页面中，查看“策略扫描概况”。

图 7-11 策略扫描概况



----结束

7.8 查看治理结果

操作场景

订阅安全遵从包后，态势感知（专业版）将自动依据安全遵从包进行扫描。扫描后，可查看整体遵从情况，并查看改进建议。

前提条件

已订阅安全遵从包，详细操作请参见 7.5 订阅安全遵从包。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 7-12 进入订阅列表页面

步骤 4 在订阅列表页面中，单击待查看结果安全遵从包所在行“操作”列的“治理结果”，进入治理结果页面。

图 7-13 治理结果

步骤 5 查看治理结果。

图 7-14 治理结果界面

- 查看当前订阅的安全遵从包的整体遵从情况。
- 如需查看某条款的详细信息，在左侧目录树中选中该条款，右侧将展示该条款的详细内容，包括条款内容、遵从状态、改进建议等内容。

  如需查看该条款的基本信息和历史记录，可单击该条款名称，右侧将弹出该条款的详细信息。
- 如需对指定法规进行自评估，请参照以下步骤进行处理：

  a. 在左边目录树选择需要自评估的条款。

  图 7-15 选择条款

  b. 单击“租户自评估”检查项的名字，进入单个检查项的操作页面，单击“编辑”按钮，填写遵从状态和自评备注。

  如果有相关的凭据，可单击“附件上传”。

  图 7-16 自评估

  c. 完成自评估后单击右上角的“提交”，完成该条款下单个检查项的评估。

----结束

7.9 查看策略扫描结果

操作场景

在策略扫描界面可查看已授权云服务的已订阅安全遵从包的总体扫描情况和各个云服务扫描情况。

说明

策略扫描将在每日凌晨 1:30 自动扫描一次并生成扫描结果。

前提条件

已订阅安全遵从包，详细操作请参见 7.5 订阅安全遵从包。

操作步骤

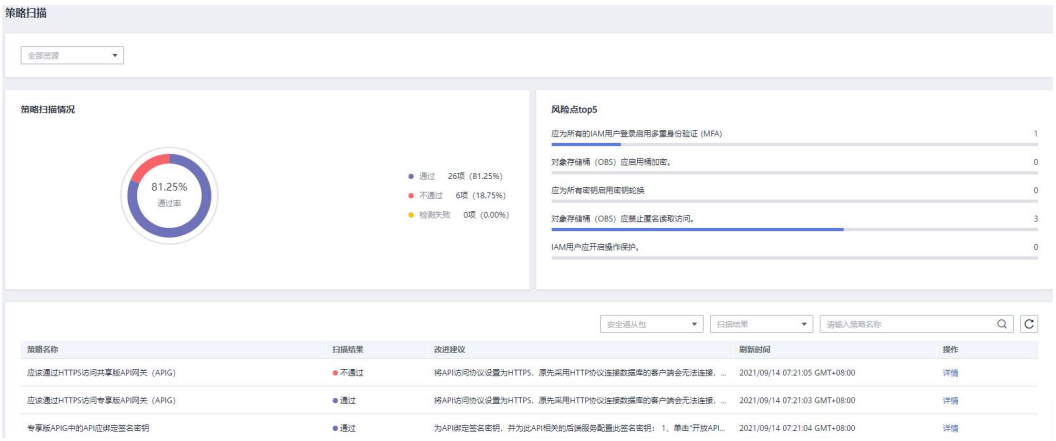
步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 策略扫描”，进入策略扫描页面。

步骤 4 查看策略扫描结果。

图 7-17 策略扫描



- 默认展示所有资源的所有策略扫描情况。
  - 策略扫描情况：所有资源的所有策略扫描情况率、通过、不通过以及检测失败情况。
  - 风险点 TOP5：策略扫描时，不通过的策略 TOP5。

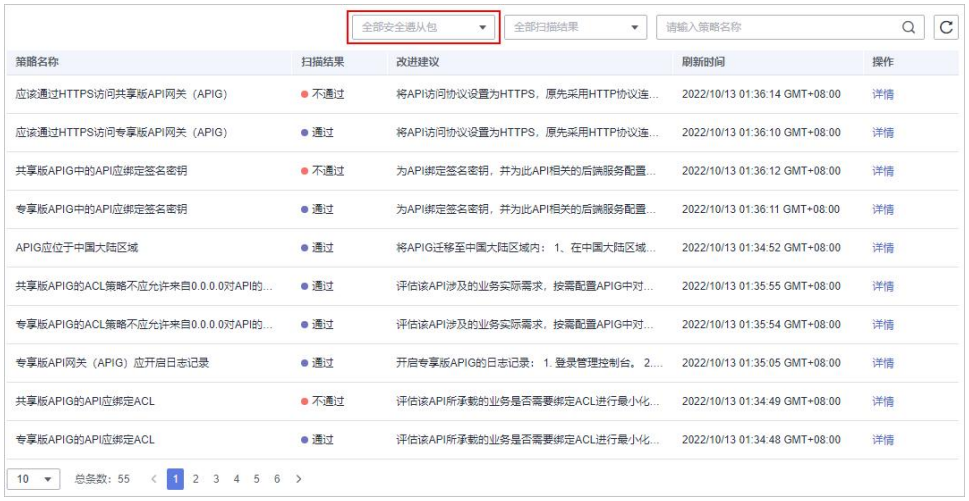
- 如需查看某个资源的所有策略扫描情况，可在上方筛选框中，选择对应资源。

  图 7-18 选择资源

- 如需查看某个策略的所有资源扫描情况，可在表格上方，选择对应遵从包。还支持通过扫描结果、策略名称进行筛选。

  图 7-19 选择遵从包

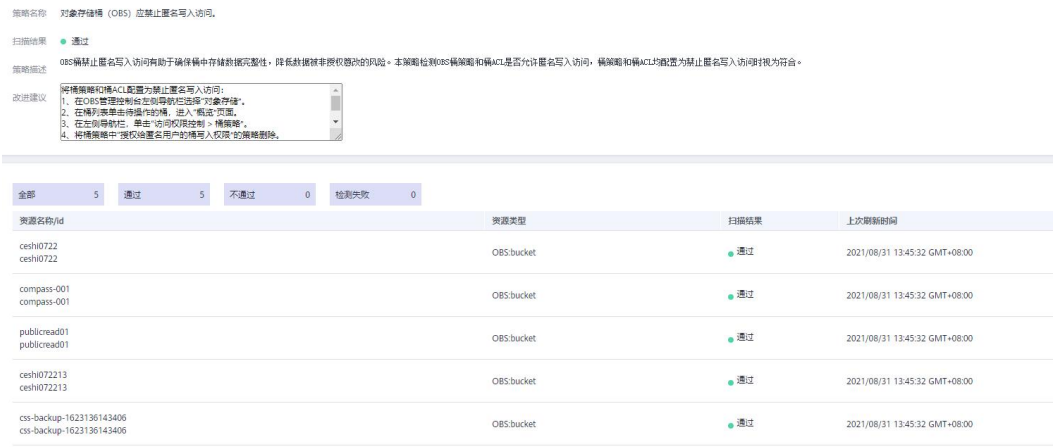
  

- 如需查看某个资源的某个策略扫描情况，可先在上方筛选框中，选择对应资源，再在表格上方，选择对应遵从包。

图 7-20 具体筛选

步骤 5 在下方策略表格中，单击具体策略“操作”列的“详情”，可进入到相应策略扫描结果界面，查看具体改进建议，如图 7-21 所示。

图 7-21 策略扫描详情



说明

每天凌晨 1:30 自动扫描一次并生成扫描结果。

----结束

7.10 下载安全合规报表

操作场景

安全治理提供安全合规报表的功能，支持下载当前资源的合规情况。

前提条件

已订阅安全遵从包，详细操作请参见 7.5 订阅安全遵从包。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 7-22 进入订阅列表页面

步骤 4 在订阅列表页面中，单击待下载报表订阅安全遵从包所在行“操作”列的“下载报表”。

系统将下载指定合规的报表到本地路径。

----结束

7.11 取消订阅安全遵从包

操作场景

当您需要更换或取消当前订阅的安全遵从包时，可在订阅列表删除该安全遵从包。

前提条件

已订阅安全遵从包，详细操作请参见 7.5 订阅安全遵从包。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 7-23 进入订阅列表页面

步骤 4 在订阅列表页面中，单击待取消订阅安全遵从包所在行“操作”列的“取消订阅”。

步骤 5 在弹出的确认框中，单击“确认”。

说明

删除后，对该安全遵从包的处理结果将清空，且不可恢复，请谨慎操作。

----结束

8 安全态势

8.1 态势总览

“态势总览”页面实时呈现当前工作空间中资源的整体安全评估状况，帮助您全量了解资产的安全情况，包括资产的安全评估结果、安全监控和安全趋势等信息。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-1 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全态势 > 态势总览”，进入态势总览页面。

步骤 5 在态势总览页面查看您的资产安全总览情况，并进行相关操作。“态势总览”分为以下几个板块：

- 安全评分
- 安全监控
- 安全趋势

各个板块数据统计周期及更新频率如下表所示：

表 8-1 态势总览

参数名称	统计周期	更新频率	说明
安全评分	实时	• 每天 2:00 自动更新 • 随当手动单击“重新检测”更新而更新	根据是否开启各安全服务防护、未处理的配置问题等级及个数、未处理的漏洞等级及个数、未处理的威胁事件等级及个数等计算而来，具体评分详细信息请参见安全分值和扣分项说明。
威胁告警	近 7 天	每 5 分钟	当前工作空间内，“威胁运营 > 告警管理”中的告警总和。
漏洞	近 7 天	每 5 分钟	当前工作空间内，“风险预防 > 漏洞管理”中的漏洞总和。
合规检查	实时	每 5 分钟	当前工作空间内，“风险预防 > 基线检查”中的问题总和。
安全趋势	近 7 天	每 5 分钟	近 7 天的安全评分数据。

----结束

安全评分

“安全评分”板块根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。

图 8-2 安全评分

- 安全评分每天凌晨 2:00 自动更新，也支持通过单击“重新检测”来进行实时更新。
- 分值范围为 0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见安全分值和扣分项说明。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 单击“立即处理”，系统右侧弹出“安全风险处理”页面，您可根据该页面的提示，参考对应的帮助文档或直接对风险进行处理。
  - 安全风险处理页面中包含所有需要您尽快处理的安全风险和威胁，分为“威胁告警”、“漏洞”、“合规检查”三大类别。

- “安全风险处理”页面中显示的数据为最近/最新检测后的数据结果，“告警管理”、“漏洞管理”、“基线检查”页面（单击“前往处理”，进入该页面）显示的是所有检测时间的各类数据详情，因此，安全风险处理页面的数据总数≤告警管理或漏洞管理页面的数据总数。
- **处理安全风险：**
  i. 在“安全评分”栏中，单击“立即处理”，系统右侧弹出“安全风险处理”页面。
  ii. 在“安全风险处理”页面中，单击“前往处理”，进入“告警管理”、“漏洞管理”或“基线检查”页面。
  iii. 对风险告警、漏洞或基线检查项目进行处理。

- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。资产安全风险修复后，也可以直接单击“重新检测”，重新检测资产并进行评分。

说明

资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

- 安全评分显示为历史扫描结果，**非实时**数据，如需获取最新数据及评分，可单击“重新检测”，获取最近的数据。

安全分值和扣分项说明

态势感知（专业版）实时呈现您资产的整体安全评估状况，并根据态势感知（专业版）的威胁检测能力，评估整体资产安全健康得分。

此处将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

- 安全分值

  根据态势感知（专业版）的威胁检测能力，评估整体资产安全健康得分。
  - 风险等级包括“无风险”、“提示”、“低危”、“中危”、“高危”和“致命”。
  - 分值范围为 0～100，分值越大表示风险越小，资产更安全。
  - 分值从 0 开始，每隔 20 取值范围对应不同的风险等级，例如分值范围 40~60 对应风险等级为“中危”。
  - 分值环形图不同色块表示不同威胁等级，例如黄色对应“中危”。
  - 资产风险修复，并手动刷新告警事件状态后，安全评分可以通过手动单击“重新检测”进行更新。

说明

资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

表 8-2 安全分值表

风险等级	安全分值	分值说明
无风险	100 分	恭喜您，您的资产当前安全状况良好。
提示	80≤分值<100	您的资产存在少量的安全隐患，建议您及时加固安全防护体系。

风险等级	安全分值	分值说明
低危	60≤分值<80	您的资产存在较多的安全隐患，建议您及时加固安全防护体系。
中危	40≤分值<60	您的资产防御黑客入侵的能力较弱，建议您立即加固安全防护体系。
高危	20≤分值<40	您的资产存在较高的黑客入侵和病毒感染的风险，建议您立即处理。
致命	0≤分值<20	您的资产很可能遭受到黑客入侵和病毒感染的威胁，建议您立即处理。

- 安全评分扣分项

  安全评分扣分项及其分值情况如表 8-3 所示。

表 8-3 安全评分扣分项

分类	扣分项	单项扣分值	处理建议	最高扣分上限
安全服务启用	未开启安全相关服务	-	开启安全相关服务	30
合规检查	存在未处理的致命不合规项	10	按照合规修复建议指导进行合规问题修复，修复后重新触发扫描任务，自动刷新评分。	20
	存在未处理的高危不合规项	5		
	存在未处理的中危不合规项	2		
	存在未处理的低危不合规项	0.1		
漏洞	存在未处理的致命漏洞	10	按照漏洞修复建议指导进行漏洞修复，修复后重新触发漏洞扫描任务，自动刷新评分。	20
	存在未处理的高危漏洞	5		
	存在未处理的中危漏洞	2		
	存在未处理的低危漏洞	0.1		
威胁告警	存在未处理的致命告警事件	10	按照威胁事件处置指导建议进行修	30

分类	扣分项	单项扣分值	处理建议	最高扣分上限
	存在未处理的高危告警事件	5	复，修复后自动刷新评分。	
	存在未处理的中危告警事件	2		
	存在未处理的低危告警事件	0.1		

安全监控

“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

图 8-3 安全监控

表 8-4 安全监控参数说明

参数名称	参数说明

参数名称	参数说明
威胁告警	呈现最**近 7 天内**当前工作空间中未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 • 单击威胁告警模块，系统将列表实时呈现**近 7 天内** TOP5 的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 列表呈现近 7 天 TOP5 的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 若列表显示内容为空，表示近 7 天无威胁告警事件。 – 单击“查看更多”，可跳转到“告警管理”页面，查看更多的威胁告警信息，并可自定义过滤条件查询告警信息。

参数名称	参数说明
漏洞	展示当前工作空间中您资产中 TOP5 漏洞类型，以及**近 7 天内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 高危：即高危风险，表示资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 中危：即中危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“漏洞类型 Top5”栏，系统将列表呈现 TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的 TOP 等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 仅当主机中 Agent 版本为 2.0 时，才会在“漏洞类型 Top5”中显示对应数据。如未显示数据或需要查看 TOP5 漏洞类型，请将主机将 Agent1.0 升级至 Agent2.0。 • 单击漏洞模块中的“实时监控最新漏洞风险事件 Top5”栏，系统将列表实时呈现**近 7 天内** TOP5 的漏洞事件，可快速查看漏洞详情。 – 列表呈现当日最新 TOP5 漏洞事件详情，包括漏洞名称、漏洞等级、资产名称、漏洞发现时间。 – 若列表显示内容为空，表示当日无漏洞事件。 – 单击“查看更多”，可跳转到“漏洞管理”页面，查看更多的漏洞信息，并可自定义过滤条件查询漏洞信息。

参数名称	参数说明
合规检查	展示当前工作空间中您资产中存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。统计信息更新频率为每 5 分钟更新一次。 • 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看合规检查事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该合规检查项目的详情。 • 单击合规检查异常模块，系统将列表实时呈现**近 30 天内** TOP5 的合规检查异常事件，可快速查看合规检查详情。 – 列表呈现最近一次合规检查中 TOP 的合规异常事件详情，包括合规检查项目名称、等级、受影响资产数量、发现时间。 – 若列表显示内容为空，表示近 30 天无合规异常事件。 – 单击“查看更多”，可跳转到“基线检查”页面，查看更多的合规异常信息，并可自定义过滤条件查询合规检查信息。

安全趋势

“安全趋势”板块展示**近 7 天**内您的整体资产安全健康得分的趋势图。更新频率为每 5 分钟更新一次。

图 8-4 安全趋势

8.2 安全报告

8.2.1 创建/复制安全报告

操作场景

态势感知（专业版）提供安全报告功能。您可以通过创建安全报告，及时掌握资产的安全状况数据。

本章节主要介绍如何新建安全报告，以及通过复制已创建的报告快速创建报告。

创建安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-5 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 8-6 进入安全报告页面

步骤 5 在安全报告页面中单击 + 按钮，进入配置报告基本信息页面。

步骤 6 配置报告基本信息。

表 8-5 报告基本信息参数说明

参数名称	参数说明
报告名称	自定义报告名称。

参数名称	参数说明
报告类型	选择报告类型。 • 日报：默认统计前一天 00:00~24:00 的安全信息。 • 周报：默认统计上一周安全信息，上周一 00:00 到上周日 24:00。 • 月报：默认统计上一月安全信息，上月第一天 00:00 到上月最后一天 24:00。 • 自定义：自定义选择时间范围。
统计周期	根据您选择的“报告类型”显示安全报告统计周期。 当“报告类型”选择“日报”或“月报”时，系统会根据您选择的“报告类型”显示安全报告统计周期。
报告发送时间	当“报告类型”选择为“日报”或“月报”时，需要设置报告发送时间。 • 日报：设置为每天报告的发送时间点，默认发送前一天 00:00:00~23:59:59 的安全信息报告。 • 月报：设置为每月报告的发送时间点，默认发送前一个月整月的安全信息报告。
报告发送频次	当“报告类型”选择“自定义”时，需要选择安全报告的发送频次。
发送规则	当“报告类型”选择“自定义”时，需要设置报告的发送时间以及统计范围。 最多可添加 5 个发送规则。
邮件标题	设置报告发送邮件的标题信息。
报告接收人邮箱	添加接收人邮箱地址。 • 最多可添加 100 个邮箱地址。 • 有多个邮箱地址，请使用英文逗号隔开。例如：test01@example.com,test02@example.com
（可选）抄送	添加抄送人邮箱地址。 • 最多可添加 100 个邮箱地址。 • 有多个邮箱地址，请使用英文逗号隔开。例如：test03@example.com,test04@example.com
（可选）备注	自定义安全报告的备注信息。

步骤 7 单击右上角“下一步：报告选择”，进入报告选择页面。

步骤 8 在“报告选择”页面的左侧已有报告布局中，选择已有报告布局。选择完成后，可以在右侧页面中预览报告样式。

如果前一步基本信息配置中选择的“报告类型”为“日报”时，此处请选择日报布局；如果选择的是“月报”，此处请选择月报布局。

全屏查看报告：单击右侧预览页面左上角的，可以全屏查看安全报告。

步骤 9 单击右下角“完成”，返回安全报告管理页面，即可查看创建的安全报告。

----结束

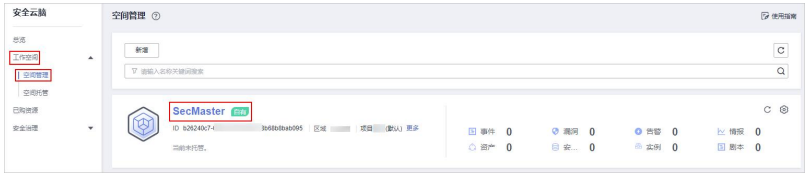
复制安全报告

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-7 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 8-8 进入安全报告页面

步骤 5 在已创建的目标安全报告模块，单击“复制”，跳转到报告基本信息配置页面。

步骤 6 修改报告基本信息。

步骤 7 单击右上角“下一步：报告选择”，进入报告选择配置页面，修改报告内容。

全屏查看报告：单击右侧预览页面左上角的，可以全屏查看安全报告。

步骤 8 单击右上角“完成”，返回安全报告管理页面，即可查看复制的安全报告。

----结束

8.2.2 查看安全报告

操作场景

本章节介绍如何查看已创建的安全报告及其展示的信息。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-9 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 8-10 进入安全报告页面

步骤 5 选择目标报告，单击报告图标，跳转到报告详情页面。

在报告详情页面，可以预览当前安全报告的详细信息。

当报告较多时，可以通过搜索功能，选择报告的“类型”或“启用状态”，单击，即可快速查询指定报告。

----结束

模板**日报**展示内容

表 8-6 模板日报展示内容

参数模块	参数说明
统计周期	日报默认统计周期为前一天 00:00:00~23:59:59。
安全评分	根据您的态势感知（专业版）的威胁检测能力，评估前一天 00:00:00~23:59:59 整体资产安全健康得分，可以快速了解资产的整体安全状况。
基线检查	展示**最近一次**基线检查的统计情况，包含以下信息： • 当前基线检查项目总数量 • 最近一次基线检查合规检查项目数量 • 最近一次基线检查不合规检查项所占的比例
安全漏洞	展示接入云服务**前一天**的漏洞统计情况，包含以下信息： • 漏洞总数量 • 未修复漏洞数量
策略覆盖	展示当前安全产品覆盖情况，包含以下信息： • 受安全产品保护的实例数量（=受保护 ECS 数量+受保护 WAF 实例数量） • 主机安全覆盖率（=受保护 ECS 数量/全部 ECS 数量） • 当前受保护云主机数量 • 当前受保护网站数量
资产安全	展示当前资产安全情况，包含以下信息： • 当前资产总数量 • 当前存在风险的资产数量
安全分析	展示**前一天**安全分析统计情况，包含以下信息： • 前一天安全日志总流量 • 安全日志模型数量
安全响应	展示**前一天**安全响应情况，包含以下信息： • 前一天处置的安全告警数量 • 前一天确认的入侵事件数量 • 前一天运行的自动化响应剧本数量 • 前一天自动化剧本闭环率 • 前一天的 MTTR 平均时间 • 前一天确认高风险入侵事件数量

参数模块	参数说明
资产风险	展示**前一天**资产安全状况，包含以下信息： • 前一天受攻击资产数量 • 前一天未防护资产数 • 前一天脆弱性资产数 • 截止昨天为止的**近 7 天**的资产变化趋势 • 前一天资产防护率
威胁态势	展示**前一天**资产的威胁态势情况，包含以下信息： • 前一天 DDoS 攻击次数 • 前一天网络攻击次数 • 前一天应用攻击次数 • 前一天主机攻击次数 • 前一天 DDoS 巡检情况 • 前一天网络主机攻击变化趋势 • 前一天 WAF 巡检情况 • 前一天 TOP5 网络攻击类型统计情况 • 前一天 TOP5 应用攻击类型统计情况 • 前一天 TOP5 主机攻击类型统计情况 • 前一天 TOP5 应用攻击源分布情况 • 前一天 TOP5 应用攻击目的分布情况 • 前一天 TOP5 主机告警分布情况 • 前一天 TOP5 网络攻击源分布情况 • 前一天主机安全巡检情况
日志分析	展示**前一天**日志分析的情况，包含以下信息： • 前一天日志源数量 • 前一天日志索引数量 • 前一天日志接收总数 • 前一天日志存储总量 • 截至昨天为止的**近 7 天**的日志变化趋势 • 截至昨天为止的**近 7 天**的 TOP5 日志源接入流量统计情况 • 前一天 TOP10 模型检测告警统计数量

参数模块	参数说明
安全响应	展示**前一天**安全响应的情况，包含以下信息： • 前一天已处理告警数量 • 前一天已处理事件数量 • 前一天已处理漏洞数量 • 前一天已处理基线数量 • 前一天威胁告警分布情况及数量 • 前一天 TOP5 入侵事件分布情况及数量 • 前一天 TOP5 应急响应统计情况 • 前一天 TOP20 威胁告警处理情况
外部安全热点	展示**前一天**外部安全热点的情况。

8.2.3 下载安全报告

操作场景

态势感知（专业版）创建并生成报告后，可以将报告下载至本地。

本章节将介绍如何下载报告至本地。

约束与限制

使用内置报告布局暂不支持下载至本地，仅支持通过创建报告时配置的发送信息来发送报告。

操作步骤

步骤 1 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 2 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-11 进入目标工作空间管理页面

步骤 3 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 8-12 进入安全报告页面

步骤 4 在已创建的目标安全报告模块，单击“编辑”，进入报告基本信息配置页面。

创建/复制安全报告时，也可以下载报告，具体操作请参见 8.2.1 创建/复制安全报告。

步骤 5 单击右上角“下一步：报告选择”，进入报告选择配置页面。

步骤 6 在报告选择页面，单击右侧预览页面左上角的 。

如需修改报告数据周期，可以在右侧预览页面右上角进行编辑。

步骤 7 在弹出的下载对话框中，选择报告格式，并单击“确定”。

系统将自动下载对应格式的报告到本地。

----结束

8.2.4 管理安全报告

操作场景

本章节介绍如何管理安全报告，包括启用、停用、编辑、删除操作。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-13 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 8-14 进入安全报告页面

步骤 5 管理安全报告。

表 8-7 管理安全报告

操作名称	执行步骤
启用/停用安全报告	在安全报告页面中，单击目标报告模块中的未启用或启用按钮。 • 安全报告状态更新为启用，则表示启用成功。 • 安全报告状态更新为未启用，则表示停用成功。
编辑安全报告	1. 在安全报告页面中，单击目标报告模块中的“编辑”，跳转到报告基本信息配置页面。 2. （可选）编辑报告基本信息。 3. 单击“下一步：报告选择”，跳转到报告选择页面。 4. （可选）勾选报告布局。 5. 单击右上角“完成”，返回安全报告管理页面。
删除安全报告	1. 在安全报告页面中，单击目标报告中的“删除”，弹出删除报告确认窗口。 2. 单击“确认”，返回安全报告管理页面。

----结束

8.3 任务中心

8.3.1 查看待办任务

操作场景

待办列表呈现当前需要您进行处理的任务，本章节主要介绍如何查看待办任务列表。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-15 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全态势 > 任务中心”，默认进入我的待办页面。

步骤 5 在待办任务列表中查看待办任务详情。

当待办任务较多时，可以通过搜索功能，选择待办任务的“创建人”、“任务名称”或“备注”，并在搜索框中输入关键词，单击 🔍，即可快速查询指定待办任务。

表 8-8 待办任务参数说明

参数名称	参数说明
任务名称	该条任务的名称。
业务类型	任务属于的类型。 • 流程发布 • 剧本发布 • 剧本-节点审核
关联对象	对应的剧本/流程名称。
创建人	创建任务的用户。
审核人	该剧本/流程的审核人员。
备注	任务的备注信息。
创建时间	该剧本/流程的创建时间。
更新时间	该剧本/流程的最近一次更新时间。
操作	对待办任务进行审批操作。

----结束

8.3.2 处理待办任务

操作场景

当剧本/流程任务执行到某一节点时，任务暂停需人工处理，剧本/流程任务才能继续执行。

本章节主要介绍如何处理待办任务。

前提条件

已触发剧本/流程任务，且任务流程需人工处理。

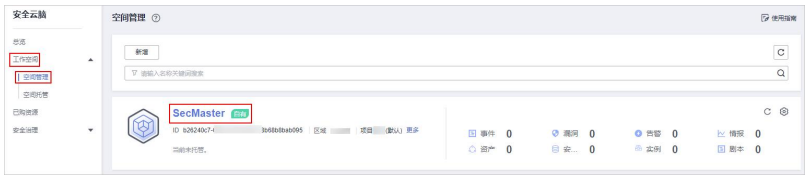
操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-16 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“安全态势 > 任务中心”，默认进入我的待办页面。

步骤 5 在目标待办任务所在行“操作”列，单击“审批”。

不同业务类型，审批方式不同：

- 剧本发布：右侧弹出“剧本发布”界面，填写“审核意见”，并根据页面提示进行审批。
- 流程发布：右侧弹出“流程发布”界面，填写“审核意见”，并根据页面提示进行审批。
- 剧本-节点审核：右侧弹出“剧本-节点审核”界面，可选择“继续执行”或“终止”。

----结束

8.3.3 查看已处理任务

操作场景

已处理列表呈现当前您已处理的任务，本章节主要介绍如何已处理的任务列表。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 8-17 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全态势 > 任务中心”，进入任务中心后，选择“我已处理”页签，进入已处理任务页面。

步骤 5 在已处理任务列表中查看已处理任务详情。

当待办任务较多时，可以通过搜索功能，选择待办任务相关属性，并在搜索框中输入关键词，单击 🔍，即可快速查询指定任务。

表 8-9 已处理任务参数说明

参数名称	参数说明
任务名称	该条任务的名称。
业务类型	任务属于的类型。 • 流程发布 • 剧本发布 • 剧本-节点审核
关联对象	对应的剧本/流程名称。
创建人	创建任务的用户。
备注	该条任务的备注信息。
审核人	该剧本/流程的审核人员。

参数名称	参数说明
审核意见	该条任务的审核意见。
描述	该条任务的描述信息。
创建时间	该剧本/流程的创建时间。
更新时间	该剧本/流程的最近一次更新时间。

----结束

9 资产管理

9.1 资产管理概述

态势感知（专业版）支持对云上资产全面自动盘点，也可灵活纳管云外各种资产，点清所有资产，并呈现资产实时安全状态。

在资产管理中，可以查看当前工作空间所在 region 中所有资源的安全状态统计信息，包括资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题并提供解决方案。

9.2 设置资产订阅

操作场景

态势感知（专业版）只有在开启资产订阅设置的工作空间才能同步资产相关信息。订阅后，资产信息将在每天晚上进行更新。

本章节介绍如何订阅资产。

说明

仅支持订阅和同步云上资产。同时，不建议同一个区域的资产订阅至多个工作空间。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 9-1 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，单击页面右上角“资产订阅设置”，右侧弹出订阅资产设置页面。

步骤 6 在订阅资产设置页面中，在需要订阅资产所在的 region 所在行“是否开通”列开启订阅。

步骤 7 单击页面右下角的“确认”。

订阅后，资产信息将在每天晚上进行更新。

----结束

9.3 查看资产信息

操作场景

在资产管理页面，可以查看资产的名称、类型、防护状态等信息。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 9-2 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面查看资产的详细信息。

- 如需查看指定类型资产信息，如主机资产，请选择“主机资产”页签进行查看。

- 当资产较多时，可以通过搜索功能，选择搜索类型并输入关键字后单击，即可快速查询指定资产。
- 页面最多可查看 9999 条资产信息。

----结束

9.4 导入/导出资产

操作场景

态势感知（专业版）支持导入云外各种资产，导入后，可以呈现资产的安全状态。同时，还可以将资产信息导出。

本章节介绍如何导入/导出资产。

约束与限制

- 仅支持导入.xlsx 格式的文件，且单次导入文件大小不超过 5MB。
- 最多支持导出 9999 条资产信息。

导入资产

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 9-3 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，选择对应资产页签。

步骤 6 在资产列表左上方，单击“导入”，弹出导入资产对话框。

步骤 7 在导入资产对话框中，单击“下载模板”，并根据模板填写要求填写待导入资产信息。

步骤 8 待导入资产文件信息填写完成后，在导入资产对话框中，单击“添加文件”，并选择你需要导入的 Excel 文件。

步骤 9 选择完成后，单击“确定”，完成导入。

----结束

导出资产

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 9-4 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，选择对应资产页签，进入对应资产页面。

步骤 6 在对应资产页面，勾选您需要导出的资产，并单击列表右上角的 ，弹出导出对话框。

步骤 7 在导出资产对话框中，配置参数。

表 9-1 导出资产

参数名称	参数说明
导出格式	默认导出 excel 格式的资产列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 8 单击“确定”。

系统将自动下载资产 excel 表格到本地。

----结束

9.5 删除资产

操作场景

如果不再需要在态势感知（专业版）资产管理页面展示某个/某些云下导入的资产的信息，可以删除资产。

约束与限制

仅支持删除云下导入的资产。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 9-5 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

步骤 5 在资产管理页面中，选择对应资产页签，进入对应资产页面。

步骤 6 在对应资产页面，勾选您需要删除的资产，并单击列表上方的“批量删除”。

系统将删除已勾选资产。

----结束

10 风险预防

10.1 基线检查

10.1.1 基线检查概述

态势感知（专业版）的基线检查功能支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

针对云服务关键配置项，您可以从“安全上云合规检查 1.0”、“等保 2.0 三级要求”、“护网检查”三大风险类别，了解云服务风险配置的所在范围和风险配置数目。

使用流程

表 10-1 使用流程

序号	操作项	说明
1	（可选）10.1.2 新增自定义基线检查计划	态势感知（专业版）将使用默认检查计划对所有资产进行检查。 • 默认检查计划：默认每隔 3 天检查一次，每次在 00:00~06:00 对您账号下当前区域的所有资产进行检查。 • 自定义基线检查计划：根据您的需求自定义检查规范和检查时间。
2	10.1.3 立即执行基线检查	基线检查功能支持定期自动检查和立即检查。 • 定期自动检查：根据系统默认基线检查计划或您自定义的基线检查计划，定时自动执行基线检查。 • 立即检查：如果您新增或修改了自定义的基线检查计划，您可以在基线检查页面选择该基线检查计划，立即执行基线检查，实时查看服务器中是否存在对应的基线风险。

序号	操作项	说明
3	10.1.5 查看基线检查结果	基线检查完后，可以查看基线检查结果，解基线检查项影响的资产、基线项目详情等信息。
4	10.1.6 处理基线检查结果	基线检查完后，可以根据修复建议对风险项目进行处理。

10.1.2 新增自定义基线检查计划

操作场景

态势感知（专业版）支持根据基线检查计划检查您的资产是否存在风险，默认每隔 3 天，每次在 00:00~06:00 对您账号下当前 region 所有资产自动执行基线检查。另外，您还可以自定义自动检测周期及时间。

本文档将介绍如何新增自定义基线检查计划。

约束与限制

- 同一个检查规范只能属于一个检查计划。

创建检查计划

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-2 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，在基线检查页面，单击“设置检查计划”，进入检测设置页面。

图 10-3 进入基线检查计划配置页面

步骤 5 在检测设置页面中，选择待创建计划所在的区域，并单击“创建计划”，系统右侧弹出新建检查计划页面。

步骤 6 配置检查计划。

1. 填写基本信息，具体参数配置如表 10-2 所示。

表 10-2 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。
检查时间	选择检测周期和检查触发时间。 • 检测周期：每隔 1 天、3 天、7 天、15 天、30 天检查一次 • 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00

2. 选择检查规范。

   选择需要检测的基线检查项目。

步骤 7 单击“确定”。

检查计划创建完成后，态势感知（专业版）会在指定的时间执行云服务基线扫描，扫描结果可以在“风险预防 > 基线检查”中查看。

----结束

相关操作

基线检查计划创建后，您可以查看检查计划、对检查计划进行编辑或删除。

- 查看已有检查计划
  a. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。
  b. 在检测设置页面中，查看已有的基线检查计划。
- 编辑检查计划

  仅支持修改用户自定义创建的检查计划。
  a. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

b. 在目标计划所在框的右上角单击“编辑”，系统右侧弹出编辑检查计划页面。

c. 编辑需要修改的计划参数后，单击“确定”。

- 删除检查计划

  仅支持删除用户自定义创建的检查计划。

  a. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

  b. 在目标计划所在框的右上角单击“删除”。

  c. 在弹出的对话框中，单击“确认”。

10.1.3 立即执行基线检查

操作场景

为了解最新的云服务基线配置状态，您需要执行扫描任务，扫描结束后才能获取云服务基线的风险配置。基线检查功能支持定期自动检查和立即检查。

- 定期自动检查：根据态势感知（专业版）提供的默认基线检查计划或您自定义的基线检查计划，定时自动执行基线检查。
- 立即检查：支持立即检查所有检查规范或某个检查计划，实时查看是否存在基线风险。

本章节介绍如何**立即**执行基线检查。

约束与限制

- “立即检查”任务在 10 分钟内仅能执行一次。
- 手动立即执行“定期自动检查任务”在 10 分钟内仅能执行一次。

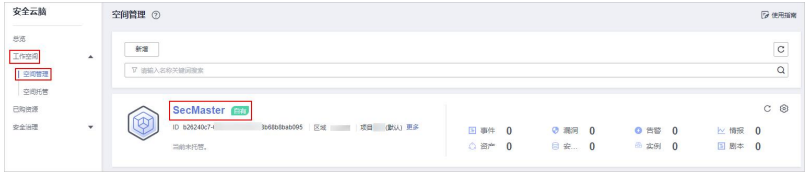
立即检查所有检查规范

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-4 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，并在基线检查页面右上角单击“立即检查”。

步骤 5 在弹出的确认框中，单击“确认”。

刷新页面，查看“最近检查时间”，即可确认是否为最新的扫描结果。

----结束

立即执行某个检查计划

本部分将介绍如何立即执行某个检查计划，配置后，系统将立即执行已选择的基线检查计划。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-5 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

步骤 5 在待执行立即手动检查的检查计划所在栏的上方单击“立即检查”。

系统将立即执行已选择的基线检查计划。

----结束

10.1.4 执行手动检查

操作场景

基线检查的一些检查项目为手动检查项，需要您在线下执行检查后，再在控制台上反馈检查结果，以便计算检查项合格率。

本章节介绍手动检查项目执行检查的操作。

约束与限制

反馈结果有效期为 7 天，7 天后请重新手动检查。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-6 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面。

图 10-7 进入基线检查页面

步骤 5 在“检查规范”页签中，单击待反馈结果检查项目所在行“操作”列的“反馈结果”。

步骤 6 在弹出提示框中，选择反馈结果，并单击“确定”。

说明

反馈结果有效期为 7 天，7 天后请重新手动检查。

----结束

10.1.5 查看基线检查结果

操作场景

本章节介绍如何查看基线检查详情、结果，您可以了解基线检查项影响的资产、基线项目详情等信息。

操作步骤

查看某工作空间中所有检查项的检查结果。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-8 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面。

图 10-9 进入基线检查页面

步骤 5 查看检查结果总数据。

在基线检查页面，查看当前工作空间检测到的基线检查结果汇总数据。

图 10-10 检查结果总数据

- 检查规范数：最近一次执行基线检查的检查规范数/检查规范总数。
- 检查项：最近一次执行基线检查中所有的检查项数目。
- 检查项合格率：最近一次执行基线检查的基线合格率。

  整体合格率=合格检查项数量/检查项总数。合格率的统计范围为全部规范的全部检查项目。

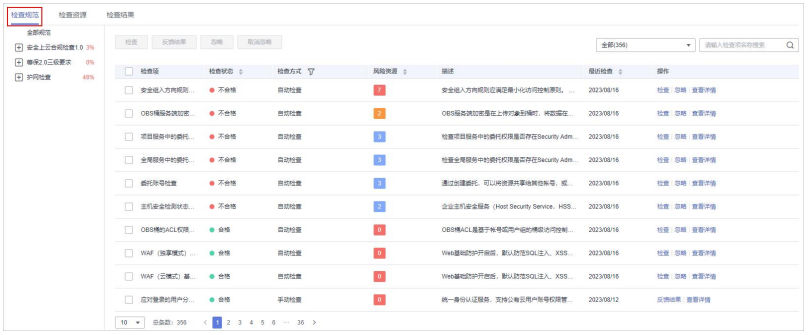
  检查项结果分为合格、不合格、检查失败和待检查几种。
- 风险资源分布：最近一次执行基线检查的风险资源分布情况以及风险资源的数量。

风险等级分为：致命、高危、中危、低危、提示几个级别。

步骤 6 查看检查规范的检测结果。

1. 在基线检查的“检查规范”页签中，系统将显示当前区域所有检查规范及其详细信息。

图 10-11 全部检查规范



基线检查规范页面会展示所有基线检查规范的列表，包括检查项、检查状态、检查分类、风险资源、描述，以及最近检查时间等信息。

说明

您也可在基线检查规范列表中，选择某个基线检查规范，查看该规范对应的基线检查项目列表。

2. 如需查看某个基线检查项目详情，可以在待查看检查项目所在行的“操作”列，单击“查看详情”，系统进入检查项目详情页面。

   在检查项目详情页面，查看检查项目的详细描述、检查提示和检查结果等详细信息。

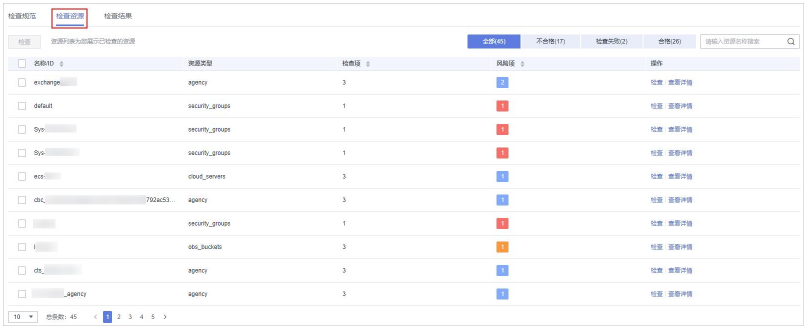
步骤 7 查看资源的检查结果。

资料列表只展示已检查的资源。

1. 选择“检查资源”页签，系统将显示当前区域所有检查资源以及其详细信息。

   检查资源页面会展示所有检查资源的列表，包括资源名称、资源类型、检查项，以及风险项等信息。

图 10-12 全部检查资源



2. 如需查看某个资源的检查详情，待查看资源所在行的“操作”列，单击“查看详情”，进入资源详情页面。

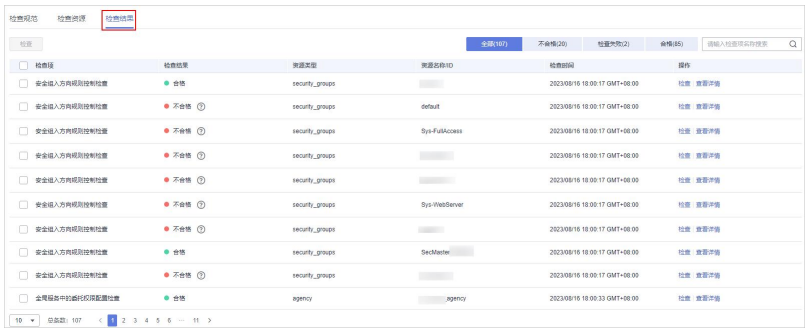
   在资源详情页面，查看资源的检查项、检查状态、检查方式、最近检查时间等详细信息。

步骤 8 查看检查结果清单。

选择“检查结果”页签，系统将显示当前区域所有检查结果以及其详细信息。

检查结果页面会展示所有检查结果的列表，包括检查项、检查结果、资源类型、资源名称，以及最近检查时间等信息。

图 10-13 全部检查结果



----结束

10.1.6 处理基线检查结果

操作场景

本章节介绍如何处理检查结果，请根据您的需要进行选择：

- 修复风险项：根据检测结果修复风险检查项目。
- 反馈结果：基线检查项目中的手动检查项，您在线下执行检查后，需要在控制台上反馈检查结果，以便计算检查项合格率。
- 忽略检查项：如果您对某个检查项有其他检查要求（例如，“会话超时策略检查”检查项中检查会话时限是否设置为 15 分钟，而您的需求为会话时限是否设置为 20 分钟）或不需要对某检查项进行检查，可以执行忽略操作。

前提条件

- 已扫描云服务基线。

修复风险项

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-14 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面。

图 10-15 进入基线检查页面

步骤 5 在“检查规范”页签中，选择子检查项，查看子检查项风险状态。

步骤 6 在子检查项所在行的“操作”列，单击“查看详情”，系统进入检查项目详情页面。

步骤 7 查看风险详细信息，并根据“检查结果”和“帮助指导”，修复风险点。

表 10-3 子检查项信息说明

参数名称	参数说明
检查状态	呈现当前检查项的检查状态。 • 合格，提示当前子检查项配置合理，全部合格。 • 不合格，提示当前子检查项配置可能不合理，并列表呈现检查结果。
最近检查	最近一次执行当前检查项的时间。
检查方式	当前检查项的检查方式。
风险等级	当前检查项出现问题所属的级别。
影响	当前检查项如果有问题将会带来的安全影响。
规范与分类	当前检查项所属的规范以及分类。
描述	当前检查项的具体检查内容。

参数名称	参数说明
检查过程	当前检查项的具体检查过程。
相关资料	子检查项涉及云服务配置手册指导。 单击引导链接，可直接跳转至详细手册指导页面。
检查资源	执行当前检查项所属的资源。 检查结果呈现检查合格和不合格两种。 • 合格，提示当前子检查项配置合理，全部合格。 • 不合格，提示当前子检查项配置可能不合理，并列表呈现检查结果，单击“操作”列引导，可直接跳转至配置项管理页面，进行安全风险修复。

步骤 8 修复所有存在风险的配置后，可单击“检查”，确认风险项是否已修复。

----结束

反馈结果

态势感知（专业版）的基线检查项目中的手动检查项，您在线下执行检查后，需要在控制台上反馈检查结果，以便计算检查项合格率。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-16 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面。

图 10-17 进入基线检查页面

步骤 5 在“检查规范”页签中，单击待反馈结果检查项目所在行“操作”列的“反馈结果”。

步骤 6 在弹出提示框中，选择反馈结果，并单击“确定”。

说明

反馈结果有效期为 7 天，7 天后请重新手动检查。

----结束

忽略检查项

如果您对某个检查项有其他检查要求（例如，态势感知（专业版）的“会话超时策略检查”检查项中检查会话时限是否设置为 15 分钟，而您的需求为会话时限是否设置为 20 分钟）或不需要对某检查项进行检查，可以执行忽略操作。

忽略后，再次检查时，将不再对已忽略检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-18 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面。

图 10-19 进入基线检查页面

步骤 5 在“检查规范”页签中，单击待忽略子检查项“操作”的“忽略”。

如果需要批量忽略检查项，可以勾选所有需要忽略的检查项，然后在列表左上角，单击“忽略”。

步骤 6 在弹出的确认框中，单击“确定”。

说明

- 忽略后，再次执行检查时，将不再对已忽略检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。
- 忽略后，如需再次检查该检查项目，在待取消忽略子检查项的“操作”列单击“取消忽略”，并在弹出的确认框单击“确定”。

----结束

10.2 漏洞管理

10.2.1 漏洞管理概述

背景介绍

态势感知（专业版）通过集成主机安全服务（Host Security Service，HSS）漏洞扫描数据，集中呈现云上资产漏洞风险，帮助用户及时发现资产安全短板，修复危险漏洞。

主机漏洞

态势感知（专业版）支持实时呈现主机漏洞扫描检测信息，支持查看漏洞详情，并提供相应漏洞修复建议。

主机漏洞共支持以下漏洞项的检测：

表 10-4 主机漏洞检测项说明

检测项	说明
Linux 软件漏洞检测	通过与漏洞库进行比对，检测出系统和软件（例如：SSH、OpenSSL、Apache、Mysql 等）是否存在的漏洞，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。

检测项	说明
Windows 系统漏洞检测	通过订阅微软官方更新，判断服务器上的补丁是否已经更新，并推送微软官方补丁，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。
Web-CMS 漏洞检测	通过对 Web 目录和文件进行检测，识别出 Web-CMS 漏洞，将存在风险的结果上报至管理控制台，并为您提供漏洞告警。
应用漏洞	通过检测服务器上运行的软件及依赖包发现是否存在漏洞，将存在风险的漏洞上报至控制台，并为您提供漏洞告警。

集成后，态势感知（专业版）中漏洞的危险等级和 HSS 中漏洞危险等级的对应关系如下：

表 10-5 漏洞危险等级对应关系

HSS 中漏洞等级	对应的态势感知（专业版）中的漏洞等级
低危（Low）	低危（Low）
中危（Medium）	中危（Medium）
高危（High）	中危（Medium）
致命（Critical）	高危（High）

10.2.2 查看漏洞详情

操作场景

本章节介绍如何查看 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞的详细信息。

前提条件

- 已接入 HSS 产品日志并已开启自动转告警设置，详细操作请参见 13.2 数据集成。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-20 进入目标工作空间管理页面

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理页面，查看漏洞统计情况。

图 10-21 漏洞统计

- **漏洞类型分布**：呈现漏洞整体数量，及各类型漏洞分布情况。
- **漏洞 TOP5 排行**：漏洞编号页签中，呈现漏洞编号数量 TOP5 的漏洞及受影响资产数量；漏洞类型页签中，呈现漏洞类型数量 TOP5 的漏洞、漏洞危险程度及受影响资产。
- **风险资产 TOP5 排行**：呈现 TOP5 的风险资产。

步骤 6 在漏洞管理界面，选择“Linux 漏洞”、“Windows 漏洞”、“Web-CMS 漏洞”、“应用漏洞”任意一个页签，进入对应漏洞管理页面。

当漏洞较多时，可以通过搜索功能，选择漏洞的“漏洞名称”、“漏洞编号”、“等级”或者“是否处理”，并在搜索框中输入关键词，单击，即可快速查询指定漏洞。

页面最多可查看 9999 条漏洞信息。

表 10-6 漏洞参数说明

参数名称	参数说明
漏洞名称	扫描出的漏洞名称。 单击漏洞名称，可查看该漏洞的简介、相关漏洞库信息。
等级	漏洞的危险程度。
ID	漏洞 ID。
影响资产	受某个漏洞影响的资产总数。
漏洞编号	漏洞对应的编号。

参数名称	参数说明
最近扫描时间	最近一次扫描的时间。
是否处理	该漏洞是否已处理。

步骤 7 如需查看某个漏洞的详细信息，可单击漏洞名称，在右侧弹出的详情页面进行查看。

----结束

10.2.3 修复漏洞

操作场景

本章节介绍如何修复漏洞。

不同类型漏洞修复方式不同，请根据漏洞类型选择对应修复方法。漏洞修复方法建议如下：

表 10-7 漏洞修复方法建议

漏洞类型	修复方式建议
Linux 软件漏洞	可以使用以下方式进行处理： • 使用态势感知（专业版）控制台上的“修复”功能进行修复。 • 根据界面提供的修复建议进行手动修复。 修复完成后，可通过“验证”功能，快速验证漏洞是否修复成功。
Windows 系统漏洞	
Web-CMS 漏洞	根据界面提供的修复建议进行手动修复。
应用漏洞	

⚠ 注意

- 执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云服务器备份（CSBS）为 ECS 创建备份。然后，使用空闲主机搭建环境充分测试，确认不影响业务正常运行后，再对主机执行漏洞修复。
- 在线修复主机漏洞时，需要连接 Internet，通过外部镜像源提供漏洞修复服务。但是，如果主机无法访问 Internet，或者外部镜像源提供的服务不稳定时，可以使用镜像源进行漏洞修复。

  为了保证漏洞修复成功，请在执行在线升级漏洞前，确认主机中已配置的对应操作系统的镜像源。

通过控制台修复漏洞

仅 Linux 软件漏洞和 Windows 系统漏洞支持使用控制台的漏洞修复功能。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-22 进入目标工作空间管理页面

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择“Linux 漏洞”、“Windows 漏洞”任意一个页签，进入对应漏洞管理页面。

步骤 6 在漏洞列表中，单击目标漏洞名称，右侧弹出漏洞信息页面。

步骤 7 在漏洞信息页面中，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“修复”，系统提示修复操作触发成功。

如需批量修复，可以勾选所有需要修复的资产，然后在列表左上角，单击“批量修复”。

步骤 8 漏洞修复完成后，若修复成功，修复状态将变更为“修复成功”。若修复失败，修复状态将变更为“修复失败”。

说明

“Linux 系统 Kernel 类的漏洞”修复完成后需要手动重启，否则系统仍可能为您推送漏洞消息。

----结束

手动修复系统软件漏洞

- **漏洞修复命令**

  进入到漏洞的基本信息页，可根据修复建议修复已经被识别出的漏洞，漏洞修复命令可参见表 10-8。

  说明

  - “Windows 系统漏洞”和“Linux 系统 Kernel 类的漏洞”修复完成后需要手动重启，否则系统仍可能为您推送漏洞消息。
  - 不同的漏洞请根据修复建议依次进行修复。
  - 若同一主机上的多个软件包存在同一漏洞，您只需修复一次即可。

表 10-8 漏洞修复命令

操作系统	修复命令
CentOS/Fedora /Euler/Redhat/Oracle	**yum update** *软件名称*
Debian/Ubuntu	**apt-get update && apt-get install** *软件名称 --only-upgrade*
Gentoo	请参见漏洞修复建议。

- **漏洞修复方案**

  漏洞修复有可能影响业务的稳定性，为了防止在修复漏洞过程影响当前业务，建议参考以下两种方案，选择其中一种执行漏洞修复：

  - **方案一：创建新的虚拟机执行漏洞修复**
    i. 为需要修复漏洞的 ECS 主机创建镜像。
    ii. 使用该镜像创建新的 ECS 主机。
    iii. 在新启动的主机上执行漏洞修复并验证修复结果。
    iv. 确认修复完成之后将业务切换到新主机。
    v. 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。
  - **方案二：在当前主机执行修复**
    i. 为需要修复漏洞的 ECS 主机创建备份。
    ii. 在当前主机上直接进行漏洞修复。
    iii. 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态。

说明

- 方案一适用于第一次对主机漏洞执行修复，且不确定漏洞修复的影响。
- 方案二适用于已经有同类主机执行过修复，漏洞修复方案已经比较成熟可靠的场景。

修复验证

漏洞修复后，建议您立即进行验证。

表 10-9 修复验证

验证方式	操作方法

验证方式	操作方法
手动验证	• 通过漏洞详情页面的“验证”，进行一键验证。 • 执行以下命令查看软件升级结果，确保软件已升级为最新版本。 – CentOS/Fedora /Euler/Redhat/Oracle 操作系统：**rpm -qa | grep** *软件名称* – Debian/Ubuntu 操作系统：**dpkg -l | grep** *软件名称* – Gentoo 操作系统：**emerge --search** *软件名称*
自动验证	若您未进行手动验证，HSS 每日凌晨进行全量检测，您修复后需要等到次日凌晨检测后才能查看修复效果。

10.2.4 导入/导出漏洞

操作场景

本章节介绍如何导入、导出漏洞。

- 导入漏洞
- 导出漏洞

约束与限制

- 仅支持导入.xlsx 格式的文件，且文件大小不超过 5MB。
- 态势感知（专业版）最多支持导出 9999 条漏洞信息。

导入漏洞

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-23 进入目标工作空间管理页面

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择“Linux 漏洞”、“Windows 漏洞”、“Web-CMS 漏洞”、“应用漏洞”任意一个页签，进入对应漏洞管理页面。

步骤 6 在漏洞管理页面中，单击漏洞管理列表上方的“导入”，弹出导入对话框。

步骤 7 在导入漏洞对话框中，单击“下载模板”，并根据模板填写要求填写待导入漏洞信息。

步骤 8 待导入漏洞文件填写完成后，在导入漏洞对话框中，单击“添加文件”，并选择你需要导入的 Excel 文件。

步骤 9 选择完成后，单击“确认”，完成导入。

----结束

导出漏洞

最多支持导出 9999 条漏洞信息。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-24 进入目标工作空间管理页面

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择“Linux 漏洞”、“Windows 漏洞”、“Web-CMS 漏洞”、“应用漏洞”任意一个页签，进入对应漏洞管理页面。

步骤 6 在漏洞管理页面中，单击漏洞管理列表右上方的 ，弹出导出漏洞对话框。

步骤 7 在导出漏洞对话框中，配置漏洞参数。

表 10-10 导出漏洞

参数名称	参数说明
导出格式	默认导出 excel 格式的漏洞列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 8 单击“确定”。

系统将自动下载漏洞 excel 表格到本地。

----结束

10.2.5 忽略/取消忽略漏洞

操作场景

某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某些漏洞无害，可以忽略该漏洞，无需修复。忽略后，将不会对该漏洞进行告警。

本章节介绍如何忽略和取消忽略某个漏洞。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-25 进入目标工作空间管理页面

步骤 4 在态势感知（专业版）管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

步骤 5 在漏洞管理界面，选择“Linux 漏洞”、“Windows 漏洞”、“Web-CMS 漏洞”、“应用漏洞”任意一个页签，进入对应漏洞管理页面。

步骤 6 在漏洞列表中，单击目标漏洞名称，右侧弹出漏洞信息页面。

步骤 7 对目标漏洞进行忽略或取消忽略操作。

- 忽略

  在漏洞信息页面中，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“更多 > 忽略”。

- 取消忽略

  a. 在漏洞信息页面中，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“更多 > 取消忽略”，弹出取消忽略确认框。

  b. 在确认框中，确认无误后，单击“确认”。

----结束

10.3 策略管理

10.3.1 策略管理概述

态势感知（专业版）的策略管理功能可以简化您在多个账户和资源上的管理和维护任务，以实现各种保护，包括 WAF、CFW、VPC 安全组。

支持统一展示所有策略信息、人工管理七层防线策略、查看人工/自动化拦截记录等操作。

约束与限制

- 应急策略目前仅支持 CFW/WAF/VPC 安全组的黑名单策略。
- 单用户单工作空间内容最多新增 500 条应急策略。
- 将 IP 或 IP 地址段配置为黑名单后，来自该 IP 或 IP 地址段的访问，CFW 将不会做任何检测，直接拦截。

10.3.2 新增/编辑应急策略

操作场景

目前，支持在态势感知（专业版）中创建 CFW/WAF/VPC 安全组的黑名单策略。

本章节介绍如何新增/编辑应急策略。

约束与限制

- 单用户单工作空间内容最多新增 500 条应急策略。
- 将 IP 或 IP 地址段配置为黑名单后，来自该 IP 或 IP 地址段的访问，CFW 将不会做任何检测，直接拦截。
- 应急策略新增成功后，**不支持**修改阻断对象（即新增时设置的 IP 地址或 IP 地址段）。

新增应急策略

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-26 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

步骤 5 在应急策略管理页面中，单击“新增”，右侧弹出新增应急策略页面。

步骤 6 在新增策略页面中，配置策略信息。

表 10-11 新增应急策略

参数名称	参数说明
阻断对象	输入需要阻断的单个（或多个）IP 地址或 IP 地址段，如有多个 IP 地址或地址段，请使用英文逗号隔开。 填写示例： • 单个 IP 地址：192.168.0.0 • IP 地址段：192.168.0.0/12
标签	自定义应急策略的标签。
操作连接	选择该策略的操作连接。
阻断老化	确认是否老化该条阻断。 • 如果选择是，请设置策略老化时间，如设置为 180 天，即该策略在设置后的 180 天内有效，180 天后将不再继续阻断设置的 IP 地址或 IP 地址段。 • 如果选择否，则该策略将一直有效，阻断设置的 IP 地址或 IP 地址段。
原因描述	自定义该策略的描述信息。

步骤 7 单击“确定”。

----结束

编辑应急策略

说明

应急策略新增成功后，**不支持**修改阻断对象（即新增时设置的 IP 地址或 IP 地址段）。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-27 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

步骤 5 在应急策略管理页面中，单击待修改策略所在行“操作”列的“编辑”，右侧弹出编辑应急策略页面。

步骤 6 在编辑策略页面中，修改策略信息。

表 10-12 编辑应急策略

参数名称	参数说明
阻断对象	应急策略新增成功后，**不支持修改**。
标签	自定义应急策略的标签。
操作连接	选择该策略的操作连接。
阻断老化	确认是否老化该条阻断。 • 如果选择是，请设置策略老化时间，如设置为 180 天，即该策略在设置后的 180 天内有效，180 天后将不再继续阻断设置的 IP 地址或 IP 地址段。 • 如果选择否，则该策略将一直有效，阻断设置的 IP 地址或 IP 地址段。
原因描述	自定义该策略的描述信息。

步骤 7 单击“确定”。

----结束

10.3.3 查看应急策略

操作场景

本章节介绍如何查看已有应急策略。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-28 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

步骤 5 在应急策略管理页面上方中，查看应急策略统计情况。

- 策略下发数量：策略下发到各个云产品的数量统计情况。
- 操作连接 TOP3：策略封堵的操作链接 TOP3 统计情况及其封堵个数。
- 阻断区域 TOP5：策略封堵对象所在的区域 TOP 统计及其分布情况。

步骤 6 在策略列表中，查看应急策略的相关信息，参数说明下所示：

表 10-13 查看应急策略

参数名称	参数说明
阻断对象	阻断的单个（或多个）IP 地址或 IP 地址段。
标签	策略的标签信息。
策略下发数量	策略在产品中下发的数量。
阻断类型	策略所属的阻断类型。
创建人	策略的创建人信息。
原因描述	策略的描述信息。

参数名称	参数说明
创建时间	策略的创建时间。
操作	对策略进行编辑、删除等操作。

步骤 7 如需查看某个应急策略的详细信息，可以选中需查看的策略，并单击页面下方“已选择：xxx”，将显示目标策略的详细信息。

在详细信息页面中，可以对策略进行阻断、取消阻断、删除操作，还可以查看策略的历史记录。

----结束

10.3.4 删除应急策略

操作场景

本章节介绍删除/批量删除应急策略。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-29 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

步骤 5 在应急策略管理页面中，单击待删除策略所在行“操作”列的“删除”。

如果需要删除多条策略，可以在策略列表中勾选需要删除的策略，并单击列表上方“批量删除”。

步骤 6 在弹出的删除确认框中，确认无误后单击“确定”。

----结束

10.3.5 批量阻断/批量取消阻断

操作场景

新增阻断时将设置某个 IP 地址或 IP 地址段，如果该阻断也适用于其他操作连接，可以进行批量阻断操作。同时，配置阻断时将设置某个 IP 地址或 IP 地址段，如果该阻断已不适用，可以进行批量取消阻断操作。

本章节介绍如何执行批量阻断、批量取消阻断操作。

约束与限制

将 IP 或 IP 地址段配置为黑名单后，来自该 IP 或 IP 地址段的访问，CFW 将不会做任何检测，直接拦截。

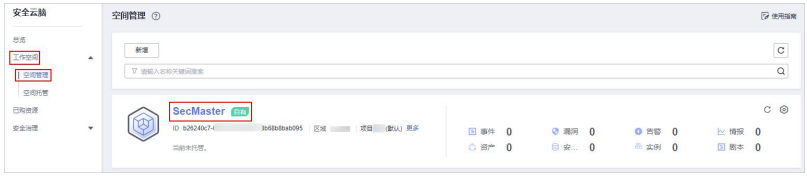
批量阻断

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-30 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

步骤 5 在应急策略管理页面中，单击待阻断策略所在行“操作”列的“批量阻断”。

步骤 6 在弹出的批量阻断对话框中，输入阻断原因，并单击“确定”。

----结束

批量取消阻断

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-31 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

步骤 5 在应急策略管理页面中，单击待取消阻断策略所在行“操作”列的“批量取消阻断”。

步骤 6 在弹出的取消阻断对话框中，输入取消阻断原因，并单击“确定”。

----结束

11 威胁运营

11.1 事件管理

11.1.1 查看事件信息

操作场景

通过查看事件列表，您可以了解近 360 天的事件的统计信息列表，列表内容包括事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如事件名称、事件等级和发生时间等，快速查询到相应事件的统计信息。

本章节主要介绍如何查看事件信息。

操作步骤

步骤 1 登录管理控制台。

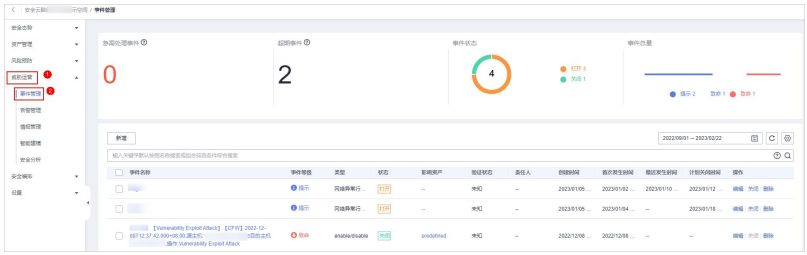
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-1 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 11-2 事件管理页面



步骤 5 在事件管理页面上方，查看事件统计情况。

图 11-3 事件统计情况

- **急需处理事件**：呈现事件等级为致命或高危，且状态为非关闭的事件总数。
- **超期事件**：呈现已超过事件设置的计划关闭时间，且还未关闭的事件总数。
- **事件状态**：呈现“打开”、“阻塞”、“关闭”状态的事件总数及对应状态下事件数量。
- **事件数量**：当前工作空间内的事件总数，以及各个等级对应的事件数量。

步骤 6 在事件列表中，查看事件详细信息。

页面最多可查看 9999 条事件信息。

表 11-1 事件参数说明

参数	说明
事件名称	事件名称。
事件 ID	事件对应的 ID。
事件等级	事件严重等级，分为以下等级：提示、低危、中危、高危、致命。
类型	事件类型。
状态	事件状态，分为以下状态：打开、阻塞、关闭。
影响资产	受此事件影响的资产。
验证状态	此事件的验证状态，即事件的准确性。分为以下状态：未知、确认、误报。
责任人	此事件的主要责任人。
创建时间	此事件的创建时间。

参数	说明
首次发生时间	此事件首次发生时间。
最近发生时间	此事件最近一次发生的具体时间。
计划关闭时间	此事件的计划关闭时间。
描述	事件的描述信息。
数据源产品名称	事件来源产品的名称。
标签	事件的标签信息
操作	可对事件进行编辑、关闭等操作。

步骤 7 如需查看某个事件详概览，可单击告警名称，页面右侧将展示事件的概览信息。

- 在事件概览页面可以查看事件的处置建议、基本信息和关联信息（包括关联的威胁指标、告警、事件、攻击信息等）。
- 如果需要查看事件详情，可以在事件概览页面右下角单击“事件详情”，进入事件详情页面。

  在详情页面除了可以查看概览页面的信息外，还可以查看事件的时间线和攻击信息。例如：事件首次发生时间、检测时间、攻击进程 ID 等。
- 在事件概览/详情页面可以在事件等级和状态的下拉箭头中修改事件等级、状态。
- 在事件概览/详情页面可以关联或取消关联告警、事件、情报，还可以查看受影响资产相关信息。

----结束

11.1.2 新增/编辑事件

操作场景

本章节主要介绍如何新增事件，以及如何对已有的事件进行编辑。

新增事件

步骤 1 登录管理控制台。

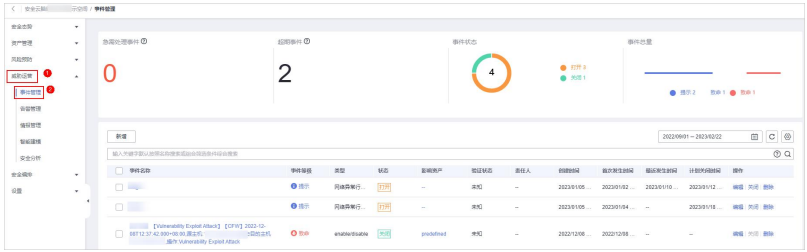
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-4 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 11-5 事件管理页面



步骤 5 在事件管理页面单击“新增”，并在右侧弹出的新增事件管理页面中配置参数，参数说明如表 11-2 所示。

表 11-2 新增事件参数说明

参数名称		参数说明
基础信息	事件名称	自定义事件名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 255 个字符。
	事件类型	选择事件类型。
	（可选）业务 ID	填写事件对应的业务 ID。
	事件等级	选择严重等级，可选择以下等级：提示、低危、中危、高危、致命。
	状态	选择事件状态，可选择以下状态：打开、阻塞、关闭。
	数据源产品名称	选择数据源产品的名称。
	数据源类型	选择数据源所属类型。
	（可选）责任人	选择事件的主要责任人。

参数名称		参数说明
时间线	首次发生时间	该事件首次发生时间。
	（可选）最近发现时间	该事件最近一次发生的具体时间。
	（可选）计划关闭时间	选择事件计划关闭时间。
其他	（可选）验证状态	选择事件的验证状态，标识事件的准确性。可选择以下状态：未知、确认、误报。
	（可选）阶段	选择您的事件阶段。 • 准备：准备资源处理事件。 • 检测与分析：检测与分析事件发生原因。 • 控制、清除、恢复：进行事件问题处理。 • 事件后活动：事件处理完成后的后续活动。
	（可选）模拟调试项	选择是否开启模拟调试功能。
	（可选）标签	填写事件的标签。
	描述	事件描述信息，输入规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 1024 个字符。

步骤 6 单击“确认”，完成事件创建。

----结束

编辑事件

步骤 1 登录管理控制台。

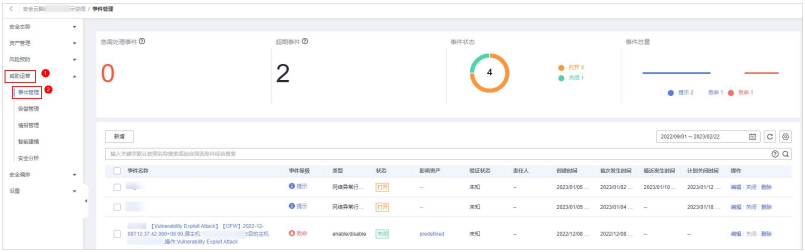
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-6 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 11-7 事件管理页面



步骤 5 在事件管理列表中，单击目标事件所在行“操作”列的“编辑”，右侧弹出编辑事件页面。

步骤 6 在弹出的“编辑”页面中，编辑事件参数。

表 11-3 编辑事件参数说明

参数名称		参数说明
基础信息	事件名称	自定义事件名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 255 个字符。
	事件类型	选择事件类型。
	（可选）业务 ID	填写事件对应的业务 ID。
	事件等级	选择严重等级，可选择以下等级：提示、低危、中危、高危、致命。
	状态	选择事件状态，可选择以下状态：打开、阻塞、关闭。
	数据源产品名称	选择数据源产品的名称，**不支持修改**。
	数据源类型	选择数据源所属类型，**不支持修改**。
	（可选）责任人	选择事件的主要责任人。

参数名称		参数说明
时间线	首次发生时间	该事件首次发生时间。
	（可选）最近发现时间	该事件最近一次发生的具体时间。
	（可选）计划关闭时间	选择事件计划关闭时间。
其他	（可选）验证状态	选择事件的验证状态，标识事件的准确性。可选择以下状态：未知、确认、误报。
	（可选）阶段	选择您的事件阶段。 • 准备：准备资源处理事件。 • 检测与分析：检测与分析事件发生原因。 • 控制、清除、恢复：进行事件问题处理。 • 事件后活动：事件处理完成后的后续活动。
	（可选）模拟调试项	选择是否开启模拟调试功能，**不支持修改**。
	（可选）标签	填写事件的标签。
	描述	事件描述信息，输入规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 1024 个字符。

步骤 7 单击“确认”，完成事件编辑。

----结束

11.1.3 导入/导出事件

操作场景

本章节主要介绍如何导入、导出事件。

约束与限制

- 仅支持导入.xlsx 格式的文件，且文件大小不超过 5MB。
- 最多支持导出 9999 条事件信息。

导入事件

步骤 1 登录管理控制台。

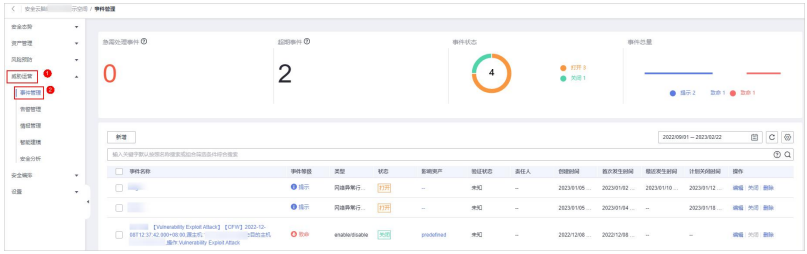
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-8 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 11-9 事件管理页面



步骤 5 在事件管理页面中，单击事件表格左上角的“导入”。

步骤 6 在弹出的“导入”对话框中，单击“下载模板”，并根据模板填写要求填写待导入事件信息。

步骤 7 待导入事件文件填写完成后，在导入事件对话框中，单击“添加文件”，选择你需要导入的 Excel 文件。

步骤 8 选择完成后，单击“确定”，完成导入。

----结束

导出事件

步骤 1 登录管理控制台。

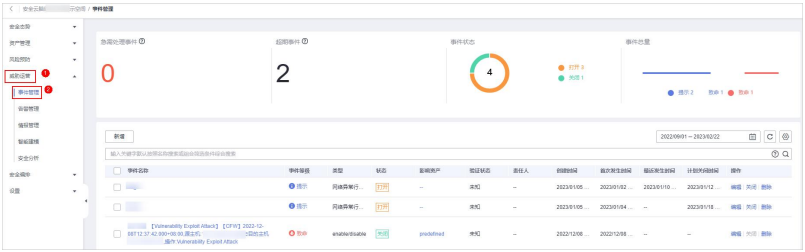
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-10 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 11-11 事件管理页面



步骤 5 在事件管理页面，勾选您需要导出的事件，并单击列表右上角的，弹出导出对话框。

步骤 6 在导出事件对话框中，配置参数。

表 11-4 导出事件

参数名称	参数说明
导出格式	默认导出 excel 格式的事件列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 7 单击“确定”。

系统将自动下载事件 excel 表格到本地。

----结束

11.1.4 关闭/删除事件

操作场景

本章节主要介绍如何执行关闭/删除事件操作。

操作步骤

步骤 1 登录管理控制台。

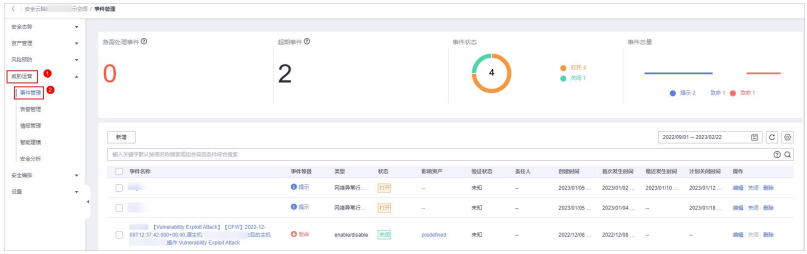
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-12 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 11-13 事件管理页面



步骤 5 在事件管理页面中，对事件进行关闭或删除操作。

表 11-5 管理事件

参数名称	参数说明
关闭事件	1. 单击目标事件所在行“操作”列的“关闭”，弹出关闭事件确认框。 如果需要关闭多条事件，可以在事件列表中勾选需要关闭的事件，并单击列表上方“批量关闭”。 2. 在关闭确认框中，选择“关闭原因”并填写“关闭评论”后，单击“确认”。
删除事件	1. 在事件管理页面，单击目标事件所在行“操作”列的“删除”，弹出删除事件确认框。 如果需要删除多条事件，可以在事件列表中勾选需要删除的事件，并单击列表上方“批量删除”。 2. 确认无误后，在弹出的确认框中，单击“确认”。 **说明** 事件删除后，不可找回，请谨慎操作。

----结束

11.2 告警管理

11.2.1 查看告警信息

操作场景

通过查看告警列表，您可以了解近 360 天的告警威胁的统计信息列表，列表内容包括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如告警名称、告警等级和发生时间等，快速查询到相应告警事件的统计信息。

本章节主要介绍如何查看告警信息。

操作步骤

步骤 1 登录管理控制台。

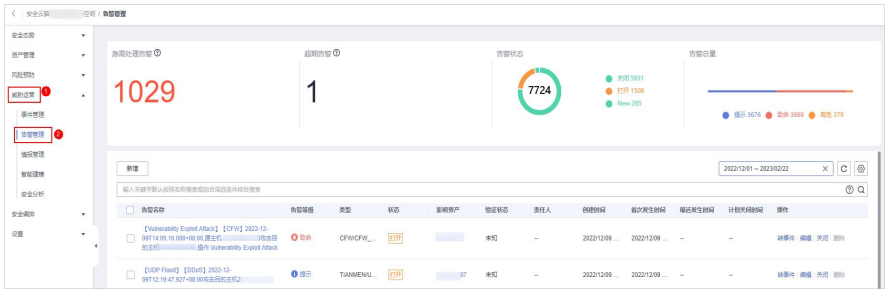
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-14 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-15 告警管理页面



步骤 5 在告警管理页面上方，查看告警统计情况。

图 11-16 告警统计情况

- **急需处理告警**：呈现告警等级为致命或高危，且状态为非关闭的告警总数。
- **超期告警**：呈现已超过告警设置的计划关闭时间，且还未关闭的告警总数。
- **告警状态**：呈现“打开”、“阻塞”、“关闭”状态的告警总数及对应状态下告警数量。
- **告警数量**：呈现当前工作空间内的告警总数，以及各个等级对应的告警数量。

步骤 6 在告警管理列表中，查看告警详细信息，参数说明如表 11-6 所示。

页面最多可查看 9999 条告警信息。

表 11-6 告警参数说明

参数	说明
告警名称	此告警的名称。
告警等级	告警严重等级，分为以下等级：提示、低危、中危、高危、致命。
类型	告警类型。
状态	告警状态，分为以下状态：打开、阻塞、关闭。
影响资产	受此告警影响的资产。 可以将鼠标悬停在影响资产名称上，将显示资产的详细信息。
验证状态	此告警的验证状态，即事件的准确性。分为以下状态：未知、确认、误报。
责任人	此告警的主要责任人。
创建时间	此告警的创建时间。
首次发生时间	此告警首次发生时间。
最近发生时间	此告警最近一次发生的具体时间。
计划关闭时间	此告警的计划关闭时间。
标签	告警的标签信息。
操作	可对告警进行编辑、关闭、删除等操作。

步骤 7 如需查看某个告警概览信息详情，可单击告警名称，页面右侧将展示告警的概览信息。

- 在告警概览页面可以查看告警的处置建议、基本信息和关联信息（包括关联的威胁指标、告警、事件、攻击信息等）。
- 如果需要查看告警详情，可以在告警概览页面右下角单击“告警详情”，进入告警详情页面。

  在详情页面除了可以查看概览页面的信息外，还可以查看告警的时间线和攻击信息。例如：告警首次发生时间、检测时间、攻击进程 ID 等。
- 在告警概览/详情页面可以在告警等级和状态的下拉箭头中修改告警等级、状态。
- 在告警概览/详情页面可以关联或取消关联告警、事件、情报，还可以查看受影响资产相关信息。

----结束

11.2.2 告警转事件或关联事件

操作场景

本章节主要介绍如何将告警转为事件，以及告警如何关联事件。

告警转事件

步骤 1 登录管理控制台。

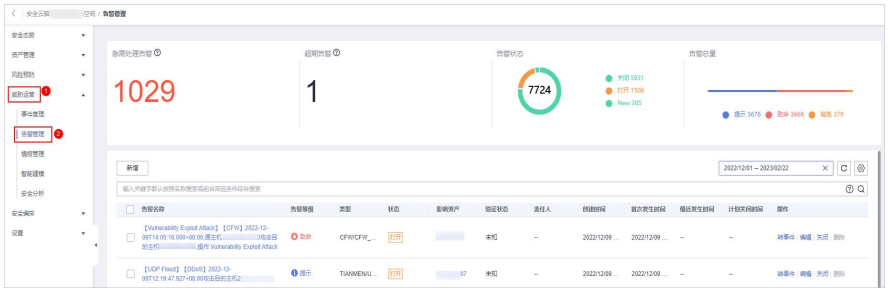
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-17 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-18 告警管理页面



步骤 5 在告警管理列表中，单击目标告警所在行“操作”列的“转事件”，右侧弹出转事件配置页面。

步骤 6 在转事件配置页面中，设置“事件类型”，其他参数保持缺省值即可。

事件名称将自动填入当前告警的名称，可以进行修改。

步骤 7 设置完成后，单击“确认”。

----结束

告警关联事件

步骤 1 登录管理控制台。

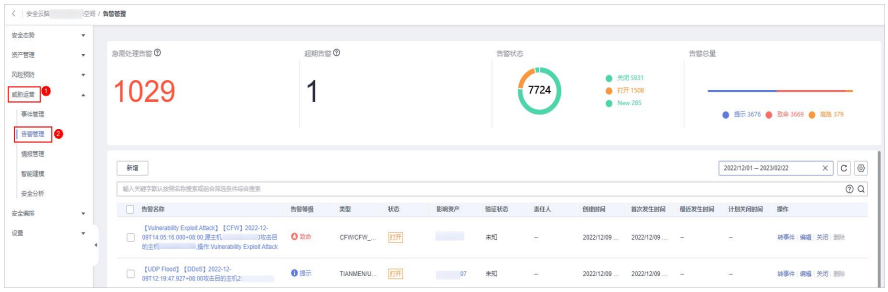
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-19 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-20 告警管理页面



步骤 5 单个告警关联事件。

1. 在告警管理列表中，单击目标告警名称，右侧弹出告警概览页面。
2. 在告警概览页面的“关联信息”栏中，选择“关联事件”页签。
3. 勾选需要关联的事件，并单击页面右下角“确认”。

步骤 6 批量关联事件。

1. 在告警管理列表中，勾选需要关联事件的告警，并单击列表上方的“关联事件”，弹出关联事件对话框。
2. 在关联事件对话框中，勾选需要绑定的事件，并单击“确认”。

----结束

11.2.3 新增/编辑告警

操作场景

本章节主要介绍如何新增告警，以及如何对已有的告警进行编辑。

新增告警

步骤 1 登录管理控制台。

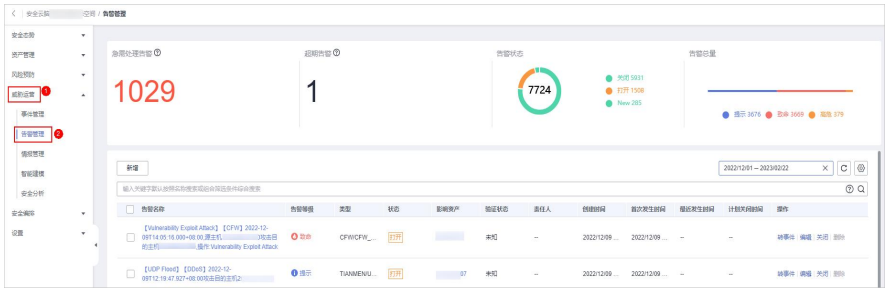
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-21 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-22 告警管理页面



步骤 5 在告警管理页面单击“新增”，并在右侧弹出的新增告警管理页面中配置参数，参数配置说明如表 11-7 所示。

表 11-7 告警参数说明

参数名称		参数说明
基础信息	告警名称	自定义告警名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 255 个字符。
	告警类型	选择告警类型。
	告警等级	选择告警严重等级，可选择以下等级：提示、低危、中危、高危、致命。
	状态	选择告警状态，可选择以下状态：打开、阻塞、关闭。
	（可选）责任人	选择告警的主要责任人。
	数据源产品名称	选择数据源产品的名称。
	数据源类型	选择数据源所属类型。
时间线	首次发生时间	该条告警首次发生时间。
	（可选）最近发现时间	该条告警最近一次发现的具体时间。
	（可选）计划关闭时间	选择告警计划关闭时间。
其他	（可选）标签	填写告警的标签。
	（可选）调试数据	选择是否开启模拟调试功能。

参数名称		参数说明
	（可选）验证状态	选择告警的验证状态，标识事件的准确性。可选择以下状态：未知、确认、误报。
	（可选）阶段	选择您的告警阶段。 • 准备：准备资源处理告警。 • 检测与分析：检测与分析告警发生原因。 • 控制、清除、恢复：进行告警问题处理。 • 事件后活动：告警处理完成后的后续活动。
	描述	填写告警描述信息，填写规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过 1024 个字符。

步骤 6 单击“确认”。

----结束

编辑告警

步骤 1 登录管理控制台。

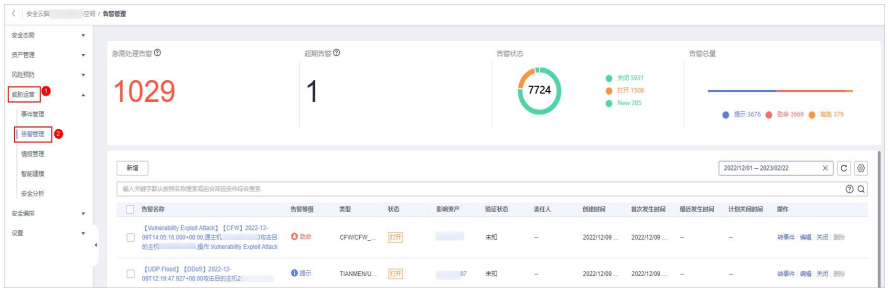
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-23 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-24 告警管理页面



步骤 5 在告警管理列表中，单击目标告警所在行“操作”列的“编辑”，右侧弹出编辑告警页面。

步骤 6 在弹出的编辑告警页面中，编辑告警参数，参数说明如表 11-8 所示。

表 11-8 告警参数说明

参数名称		参数说明
基础信息	告警名称	自定义告警名称，命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 255 个字符。
	告警类型	选择告警类型。
	告警等级	选择告警严重等级，可选择以下等级：提示、低危、中危、高危、致命。
	状态	选择告警状态，可选择以下状态：打开、阻塞、关闭。
	（可选）责任人	选择告警的主要责任人。
	数据源产品名称	选择数据源产品的名称，**不支持修改**。
	数据源类型	选择数据源所属类型，**不支持修改**。
时间线	首次发生时间	该条告警首次发生时间。
	最近发现时间	该条告警最近一次发现的具体时间。
	计划关闭时间	选择告警计划关闭时间。
其他	标签	填写告警的标签。

参数名称		参数说明
	调试数据	选择是否开启模拟调试功能，**不支持修改**。
	验证状态	选择告警的验证状态，标识事件的准确性。可选择以下状态：未知、确认、误报。
	阶段	选择您的告警阶段。 • 准备：准备资源处理告警。 • 检测与分析：检测与分析告警发生原因。 • 控制、清除、恢复：进行告警问题处理。 • 事件后活动：告警处理完成后的后续活动。
	描述	填写告警描述信息，填写规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过 1024 个字符。

步骤 7 单击“确认”，完成告警编辑。

----结束

11.2.4 导入/导出告警

操作场景

本章节主要介绍如何导入、导出告警。

约束与限制

- 仅支持导入.xlsx 格式的文件，且文件大小不超过 5MB。
- 最多支持导出 9999 条告警信息。

导入告警

步骤 1 登录管理控制台。

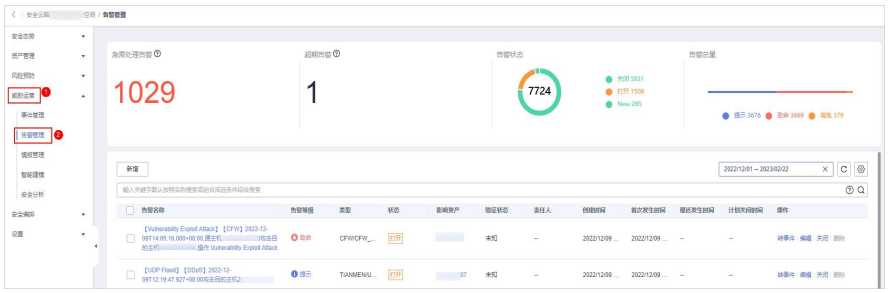
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-25 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-26 告警管理页面



步骤 5 在告警管理页面中，单击告警列表左上角的“导入”。

步骤 6 在弹出的“导入”对话框中，单击“下载模板”，并根据模板填写要求填写待导入告警信息。

步骤 7 待导入告警文件填写完成后，在导入告警对话框中，单击“添加文件”，选择你需要导入的 Excel 文件。

步骤 8 选择完成后，单击“确定”，完成导入。

----结束

导出告警

步骤 1 登录管理控制台。

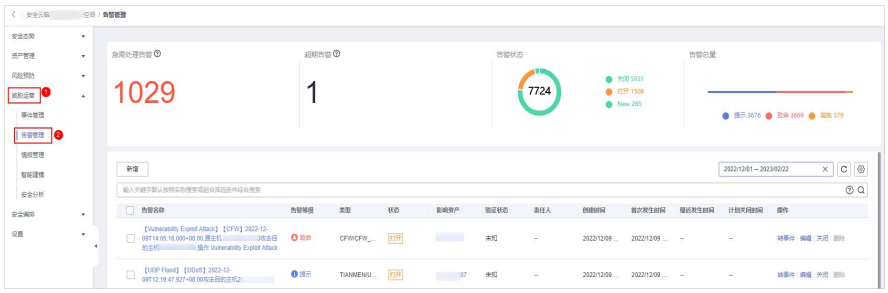
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-27 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-28 告警管理页面



步骤 5 在告警管理列表中，勾选您需要导出的告警，并单击列表右上角的，弹出导出对话框。

步骤 6 在导出告警对话框中，配置参数。

表 11-9 导出告警

参数名称	参数说明
导出格式	默认导出 excel 格式的告警列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 7 单击“确定”。

系统将自动下载告警 excel 表格到本地。

----结束

11.2.5 关闭/删除告警

操作场景

本章节主要介绍如何执行关闭/删除告警操作。

操作步骤

步骤 1 登录管理控制台。

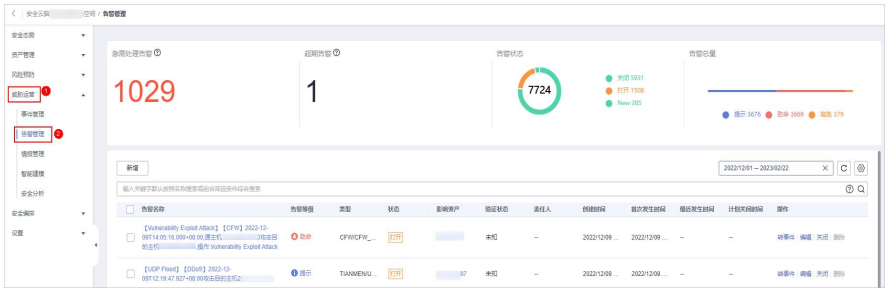
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-29 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 11-30 告警管理页面



步骤 5 在告警管理页面中，对告警进行关闭或删除操作。

表 11-10 管理告警

参数名称	参数说明
关闭告警	1. 单击目标告警所在行“操作”列的“更多 > 关闭”，弹出关闭告警确认框。 如果需要关闭多条告警，可以在告警列表中勾选需要关闭的告警，并单击列表上方“批量关闭”。 2. 在关闭确认框中，选择“关闭原因”并填写“关闭评论”后，单击“确认”。

参数名称	参数说明
删除告警	1. 单击目标告警所在行“操作”列的“更多 > 删除”，弹出删除告警确认框。 如果需要删除多条告警，可以在告警列表中勾选需要删除的告警，并单击列表上方“批量删除”。 2. 在弹出的确认框中，单击“确认”。 说明 告警删除后，不可找回，请谨慎操作。

----结束

11.3 情报管理

11.3.1 新增情报指标

操作场景

情报指标库列表呈现当前您的所有指标信息。

本章节主要介绍如何新建情报指标。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-31 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-32 情报管理页面

步骤 5 在情报管理页面单击“新增”，并在右侧弹出的新增情报管理页面中配置参数。

表 11-11 指标参数说明

参数	说明
指标名称	自定义威胁情报指标名称，命名规则如下： 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。
类型	选择指标类型。
威胁度	选择威胁度等级。 • 黑：表示危险 • 灰：表示一般 • 白：表示安全
数据源产品名称	选择数据源产品的名称。
数据源类型	选择数据源所属类型。
状态	选择指标状态，可选择以下状态：打开、关闭、作废。
（可选）置信度	填选指标的可信度，范围为 80~100。
（可选）责任人	选择该条指标的主要责任人。
（可选）标签	自定义指标的标签。
首次发生时间	选择该条指标首次发生时间。
最近发生时间	选择该条指标最近一次发生的具体时间。
（可选）失效时间	选择该指标的失效时间。
是否失效	选择是否失效该条指标。默认为“否”。
粒度	选择该指标的粒度，可选择以下粒度：首次发现、自产数据、需购买、外网直接查询。

参数	说明
其他参数	根据选择的不同类型，还需要配置对应的参数信息，请根据界面显示进行填写。 例如，当“类型”选择“ipv6”时，还需要配置 IP 地址、邮箱账户、地区等信息。

步骤 6 单击“确认”，完成指标创建。

----结束

11.3.2 关闭情报指标

操作场景

本章节主要介绍如何关闭情报指标。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-33 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-34 情报管理页面

步骤 5 在情报管理页面，单击目标情报所在行“操作”列的“关闭”，弹出关闭情报确认框。

步骤 6 在弹出的关闭情报确认框中，选择“关闭原因”，并填写评论信息。

步骤 7 单击“确认”。

----结束

11.3.3 导入/导出情报指标

操作场景

本章节主要介绍如何导入、导出情报指标。

约束与限制

- 仅支持导入.xlsx 格式的文件，且文件大小不超过 5MB。
- 最多支持导出 9999 条情报指标信息。

导入指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-35 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-36 情报管理页面

步骤 5 在情报管理页面中，单击指标列表左上角的“导入”。

步骤 6 在弹出的“导入”对话框中，单击“下载模板”，并根据模板填写要求填写待导入情报指标信息。

步骤 7 待导入情报指标文件填写完成后，在导入情报指标对话框中，单击“添加文件”，选择你需要导入的 Excel 文件。

步骤 8 选择完成后，单击“确定”，完成导入。

----结束

导出指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-37 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-38 情报管理页面

步骤 5 在情报管理页面中，勾选您需要导出的指标，并单击列表右上角的，弹出导出对话框。

步骤 6 在导出指标对话框中，配置参数。

表 11-12 导出指标

参数名称	参数说明
导出格式	默认导出 excel 格式的指标列表。
自定义导出列	选择导出表格中，需要导出的参数。

步骤 7 单击“确定”。

系统将自动下载指标 excel 表格到本地。

----结束

11.3.4 管理情报指标

操作场景

本章节主要介绍如何执行查看情报指标信息、编辑指标、删除指标等操作。

查看情报指标信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-39 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-40 情报管理页面

步骤 5 在情报管理页面上方，查看威胁情报指标统计情况。

图 11-41 情报指标总览

- **情报类型**：呈现所有类型情报指标总数及对应类型下情报指标数量。
- **超期情报**：呈现已超过威胁情报指标设置的失效时间，且还未关闭的威胁情报指标总数。
- **情报状态**：呈现不同状态的情报指标总数及对应状态下情报指标数量。
- **威胁度**：呈现不同威胁程度对应的情报指标数量。

步骤 6 在情报管理列表中，查看情报详细信息，参数说明如表 11-13 所示。

页面最多可查看 9999 条情报指标信息。

表 11-13 情报参数说明

参数	说明
指标名称	指标名称。
指标 ID	指标对应的 ID。
威胁度	指标对应的威胁度，分为以下威胁度：黑、白、灰。

参数	说明
类型	指标类型。
状态	指标状态，分为以下状态：打开、关闭、作废。
置信度	指标的置信度。
责任人	指标的责任人。
首次发生时间	指标首次发生时间。
创建时间	指标的创建时间。
失效时间	指标的失效时间。
操作	可对指标进行编辑、关闭、删除等操作。

步骤 7 如需查看某个指标详细信息，可单击指标名称，页面右侧将展示指标的详细信息。

----结束

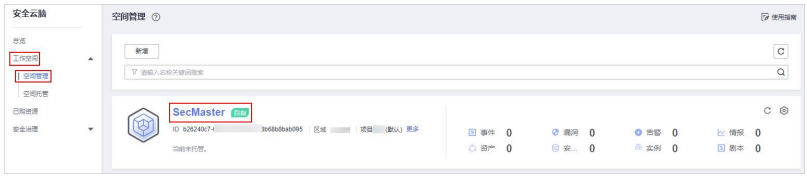
编辑指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-42 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-43 情报管理页面

步骤 5 在情报管理页面中，单击目标情报所在行“操作”列的“编辑”，右侧弹出编辑情报页面。

步骤 6 在弹出的编辑情报指标页面中，编辑指标参数。

表 11-14 指标参数说明

参数	说明
指标名称	自定义威胁情报指标名称，命名规则如下： 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。
类型	选择指标类型。
威胁度	选择威胁度等级。 • 黑：表示危险 • 灰：表示一般 • 白：表示安全
数据源产品名称	选择数据源产品的名称，**不支持修改**。
数据源类型	选择数据源所属类型，**不支持修改**。
状态	选择指标状态，可选择以下状态：打开、关闭、作废。
置信度	填选指标的可信度，范围为 80~100。
责任人	选择该条指标的主要责任人。
标签	自定义指标的标签。
首次发生时间	选择该条指标首次发生时间。
最近发现时间	选择该条指标最近一次发生的具体时间。
失效时间	选择该指标的失效时间。
是否失效	选择是否失效该条指标。默认为“否”。
粒度	选择该指标的粒度，可选择以下粒度：首次发现、自产数据、需购买、外网直接查询。

参数	说明
其他参数	根据选择的不同类型，还需要配置对应的参数信息，请根据界面显示进行填写。 例如，当“类型”选择“ipv6”时，还需要配置 IP 地址、邮箱账户、地区等信息。

步骤 7 单击“确认”。

----结束

删除指标

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-44 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 11-45 情报管理页面

步骤 5 在情报管理页面中，单击目标情报所在行“操作”列的“删除”，弹出删除确认框。

步骤 6 确认无误后，在弹出的确认框中，单击“确认”。

说明

指标删除后，不可找回，请谨慎操作。

----结束

11.4 智能建模

11.4.1 查看已有模型模板

操作场景

态势感知（专业版）支持利用模型对管道中的日志数据进行扫描，如果不在模型设置范围内容，将产生告警提示。模型是基于模板而创建的，因此，需利用已有模板创建模型。

本章节介绍如何查看已有模型模板。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-46 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

图 11-47 模型模板页面

步骤 5 在模型模板页面，查看已有模型模板。

- **模型模板统计**：显示**可用模板**和**活跃模板**数量。

- **严重程度**：显示当前已有模板的严重程度统计情况，包含致命、高危、中危、低危、提示级别。
- 模板列表中，显示当前已有模板的严重程度、名称、模型类型、更新时间和创建时间等信息。
- 如需查看某个模型模板的详细信息，可单击模板所在行“操作”列的“详情”，右侧弹出当前模板详情页面。

  在详情页面中可以查看当前模型模板的描述信息、查询规则、触发条件、查询计划等信息。

----结束

11.4.2 新建/编辑模型

操作场景

态势感知（专业版）支持利用模型对管道中的日志数据进行监控，如果数据信息在模型范围内容，将产生告警提示。

本章节将介绍如何创建并编辑告警模型。

- 使用已有模板创建告警模型
- 自定义新建告警模型
- 编辑模型

约束与限制

- 一个告警模型的运行时间间隔须 ≥ 5 分钟，查询数据的时间范围 ≤ 14 天。

使用已有模板创建告警模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-48 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

图 11-49 模型模板页面

步骤 5 在模型模板列表中，单击目标模型模板所在行“操作”列的“详情”，右侧弹出模板详情页面。

步骤 6 在模型模板详情页面，单击右下角“创建模型”，进入新建告警模型页面。

步骤 7 在新增告警模型页面中，配置告警模型基础信息，参数说明如表 11-15 所示。

表 11-15 告警模型基础配置

参数名称	参数说明
管道名称	选择该告警模型的执行管道。
模型名称	自定义该条告警模型的名称。
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	该告警模型的描述信息。
启用状态	设置该告警模型的启用状态。 •  ：表示启用，默认为此状态。 •  ：表示未启用。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤 8 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 9 设置模型逻辑，参数说明如表 11-16 所示。

表 11-16 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。

参数名称	参数说明
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。

步骤 10 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 11 预览确认无误后，单击页面右下角“确定”。

----结束

自定义新建告警模型

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-50 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模的可用模型页面。

图 11-51 可用模型页面

步骤 5 在可用模型列表左上角单击“新建模型”，进入新建告警模型页面。

步骤 6 在新增告警模型页面中，配置告警模型基础信息，参数说明如表 11-17 所示。

表 11-17 告警模型基础配置

参数名称	参数说明
管道名称	选择该告警模型的执行管道。
模型名称	自定义该条告警模型的名称。
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	该告警模型的描述信息。
启用状态	设置该告警模型的启用状态。 •  ：表示启用，默认为此状态。 •  ：表示未启用。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤 7 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 8 设置模型逻辑，参数说明如表 11-18 所示。

表 11-18 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。 语法参考请参见 11.5.6.1 SQL 语法。
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。 •  ：表示抑制，即生成告警后**停止**运行查询。 •  ：表示不抑制，即生成告警后**不停止**运行查询。

步骤 9 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 10 预览确认无误后，单击页面右下角“确定”。

----结束

编辑模型

仅支持编辑自定义创建的模型。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-52 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模的可用模型页面。

图 11-53 可用模型页面

步骤 5 在可用模型列表中，单击目标模型所在行“操作”列的“编辑”，右侧弹出编辑告警模型页面。

步骤 6 在编辑告警模型页面中，配置告警模型基础信息，参数说明如表 11-19 所示。

表 11-19 告警模型基础配置

参数名称	参数说明
管道名称	选择该告警模型的执行管道。**暂不支持编辑**。
模型名称	自定义该条告警模型的名称。
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。

参数名称	参数说明
描述	该告警模型的描述信息。

步骤 7 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 8 设置模型逻辑，参数说明如表 11-20 所示。

表 11-20 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。

步骤 9 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 10 预览确认无误后，单击页面右下角“确定”。

----结束

11.4.3 查看已有模型

操作场景

本章节将介绍如何查看已新增的模型。

前提条件

已新增模型，详细操作请参见 11.4.2 新建/编辑模型。

操作步骤

步骤 1 登录管理控制台。

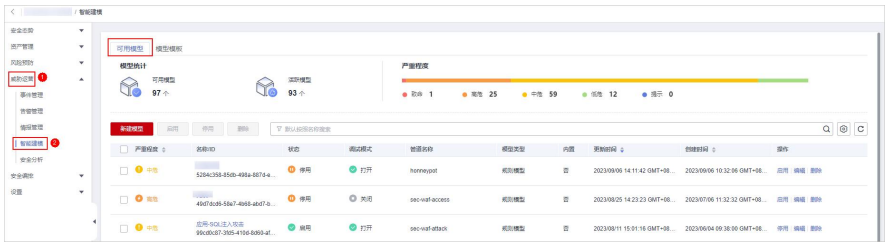
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-54 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模的可用模型页面。

图 11-55 可用模型页面



步骤 5 在可用模型页面，查看已有模型。

- **模型统计**：显示**可用模型**和**活跃模型**数量。

- **严重程度**：显示当前已有模型的严重程度统计情况，包含致命、高危、中危、低危、提示级别。
- 模型列表中，显示当前已有模型的严重程度、名称/ID、管道名称、模型类型、更新时间和创建时间等信息。

----结束

11.4.4 管理模型

操作场景

本章节将介绍如何管理模型，如启用、停用、删除模型等操作。

约束与限制

- 仅支持对自定义创建的模型进行启用、停用、删除操作。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-56 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模的可用模型页面。

图 11-57 可用模型页面

步骤 5 管理模型。

表 11-21 管理模型

参数名称	参数说明
启用模型	在模型列表中，单击目标模型所在行“操作”列的“启用”。 **说明** 如需批量启动模型，可以勾选所有需要启动的模型，然后单击列表左上角的“启用”。 当模型状态更新为启用，则表示启动模型成功。
停用模型	在模型列表中，单击目标模型所在行“操作”列的“停用”。 **说明** 如需批量暂停模型，可以勾选所有需要暂停的模型，然后单击列表左上角的“停用”。 当告警模型状态更新为“停用”，表示停用成功。
删除模型	1. 在模型列表中，单击目标模型所在行“操作”列的“删除”。 **说明** 如需批量删除模型，可以勾选所有需要删除的模型，然后单击列表左上角的“删除”。 2. 在弹出的确认框中，单击“确定”。

----结束

11.5 安全分析

11.5.1 安全分析概述

态势感知（专业版）的安全分析功能是一种云原生安全信息和事件管理（SIEM）解决方案，支持采集多产品的安全日志及告警，并基于预定义和自定义的安全检测规则对多来源的告警及日志进行聚合分析，旨在帮助企业快速发现和响应安全事件，实现对云负载、各类应用及数据的安全保护。

支持接入的云产品和日志

态势感知（专业版）支持集成多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

具体支持接入的云服务日志请参见 13.2.1 支持接入的日志。

约束与限制

- 单次查询分析最多支持返回 500 条结果。
- 一个数据管道内最多创建 50 个快速查询，即最多可以将 50 个查询分析条件保存为快速查询。
- 一个工作空间中最多创建 5 个数据空间；一个数据空间中最多创建 20 个数据管道。

- 一个数据管道内容最多分配 64 个 Shards。
- 一个数据管道内的数据留存时间最长为 180 天。

11.5.2 使用流程

安全分析功能使用具体流程如表 11-22 所示。

表 11-22 使用流程

子流程	说明
5.2 新增工作空间	新增工作空间，用于资源隔离和控制。
13.2 数据集成	配置需要接入的数据。 态势感知（专业版）支持集成存储、管理与监管、安全等多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。
（可选）11.5.10.1 新增数据空间	创建用于存储收集日志数据的数据空间。 通过控制台接入的数据，系统将创建默认数据空间，无需再进行创建。
（可选）11.5.11.1 创建管道	创建用于日志数据的采集、存储和查询的数据管道。 通过控制台接入的数据，系统将创建默认数据管道，无需再进行创建。
11.5.3 配置索引	配置索引条件，缩小查询范围。
11.5.4 查询与分析	对接入的数据进行查询、分析。
11.5.5 下载日志	支持将原始日志或查询分析后的日志下载到本地。
11.5.9.1 图表统计概述	当您执行了查询分析语句后，态势感知（专业版）支持通过图表统计的形式对查询和分析的结果进行可视化展示。 目前支持表格、折线图、柱状图和饼图方式进行展示。

11.5.3 配置索引

安全分析中的索引是一种存储结构，用于对日志数据中的一列或多列进行排序。不同的索引配置，将会产生不同的查询和分析结果，请根据您的需求合理配置索引。

如果您需要使用分析功能，必须配置字段索引。配置字段索引后，您可以指定字段名称和字段值（Key:Value）进行查询，缩小查询范围。例如查询语句 level:error，表示查询 level 字段值包含 error 的日志。

前提条件

已完成数据接入，详细操作请参见 13.2 数据集成。

配置字段索引

步骤 1 登录管理控制台。

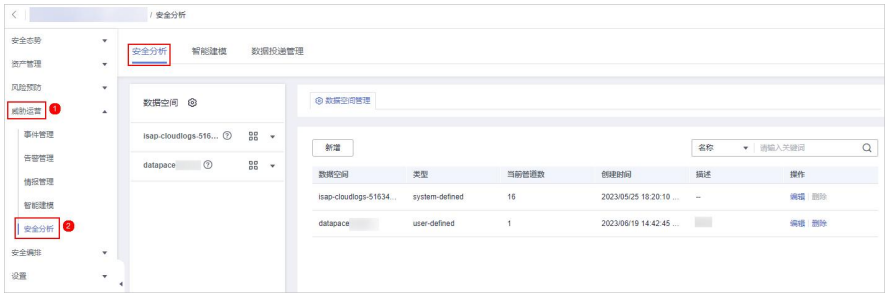
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-58 进入目标工作空间管理页面

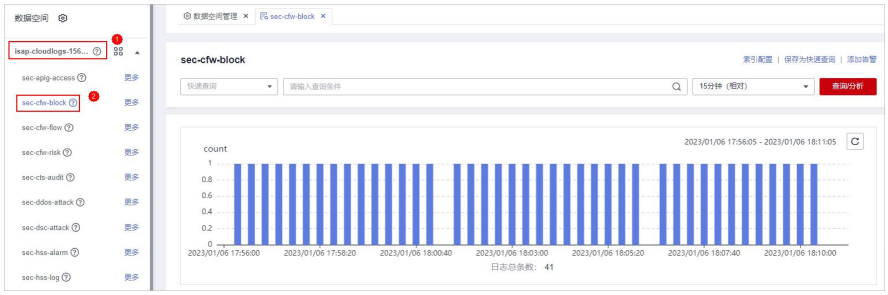
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-59 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-60 管道数据页面



步骤 6 在数据管道检索页面，单击右上角“索引配置”，页面右侧展示索引配置页面。

步骤 7 在索引配置页面中，配置索引参数。

1. 开启索引状态。

   索引状态默认开启，索引状态关闭时，将无法索引和查询采集到的日志。

2. 配置索引参数，参数配置说明如表 11-23 所示。

表 11-23 索引配置参数说明

参数名称	参数说明
字段名称	日志字段名称（key）。
字段类型	日志字段值（value）的数据类型，可选值为 text、keyword、long、integer、double、float、date 和 json。
包含中文	查询时是否区分中英文。当字段类型选择“text”时，需要设置该参数。 • 开启开关后，如果日志中包含中文，则按照中文语法拆分中文内容，按照分词符配置拆分英文内容。 • 关闭开关后，按照分词符配置拆分所有内容。 示例：日志内容为：**user:WAF 日志用户张三**。 • 关闭“包含中文”开关后，按照分词符半角冒号（:）进行拆分，日志会被拆分为 user、WAF 日志用户张三，您可以通过 user 或 WAF 日志用户张先生查找该日志。 • 开启“包含中文”开关后，日志服务后台分词器将日志拆分为 user、WAF、日志、用户和张三，您通过日志或张先生等词都可以查找到该日志。

步骤 8 单击“确定”。

----结束

11.5.4 查询与分析

操作场景

数据收集成功后，您可以在查询分析页面对收集到的日志数据进行实时查询分析。

本章节将介绍如何对日志数据进行查询分析，请根据您的需要选择查询分析方式：

- 输入查询条件进行查询分析
- 使用已有字段进行查询分析
- 操作查询分析结果

前提条件

已完成数据接入，详细操作请参见 13.2 数据集成。

输入查询条件进行查询分析

步骤 1 登录管理控制台。

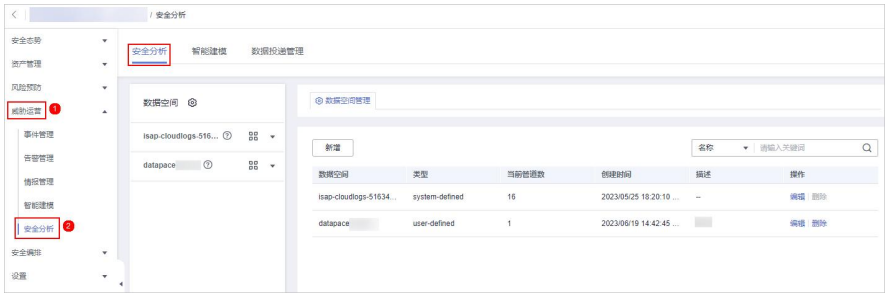
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-61 进入目标工作空间管理页面

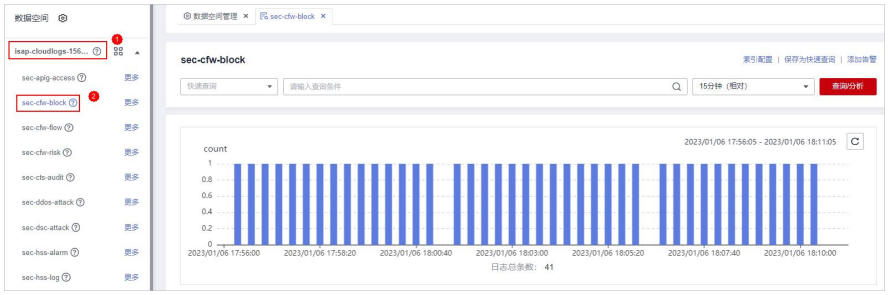
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-62 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-63 管道数据页面



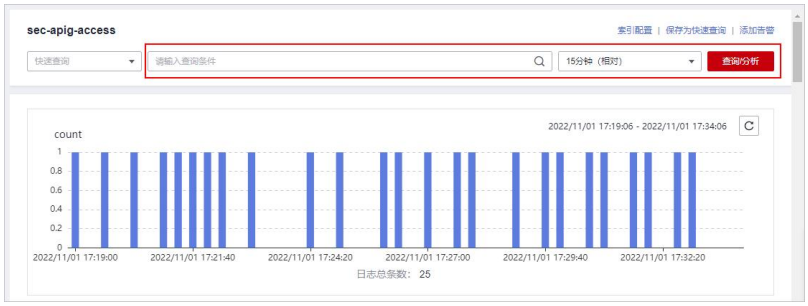
步骤 6 在管道数据检索页面，输入查询分析语句。

查询分析语句由查询语句和分析语句构成，格式为**查询语句|分析语句**，查询分析语句语法详细内容请参见 11.5.6 查询与分析语法。

说明

如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。

图 11-64 查询与分析



步骤 7 单击“15 分钟（相对）”，设置查询时间范围。

您可以选择相对时间（15 分钟、1 小时、24 小时），或自定义查询时间。

步骤 8 单击“查询/分析”，查看查询分析结果。

----结束

使用已有字段进行查询分析

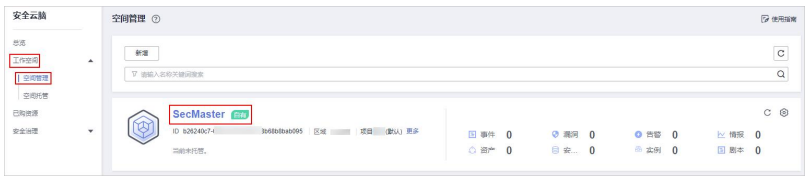
本部分将介绍如何使用已有字段对接入日志进行查询分析。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

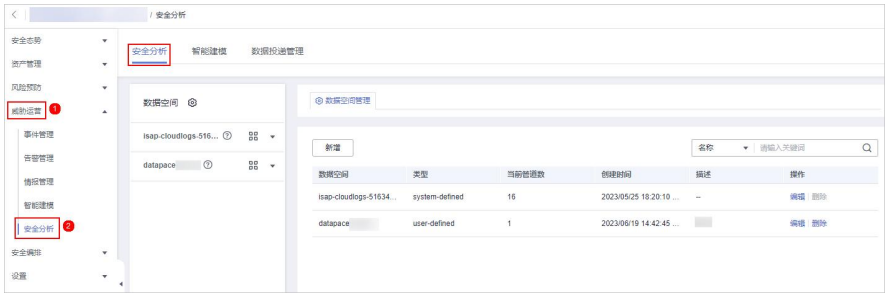
步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-65 进入目标工作空间管理页面



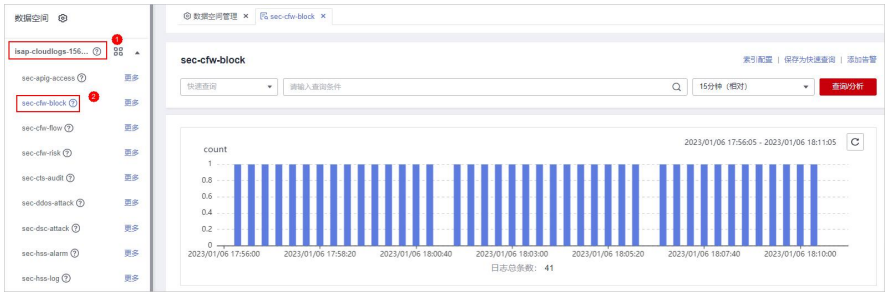
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-66 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击默认数据空间名称，展开数据管道列后，单击管道名称，右侧将显示管道数据的检索页面。

图 11-67 管道数据页面



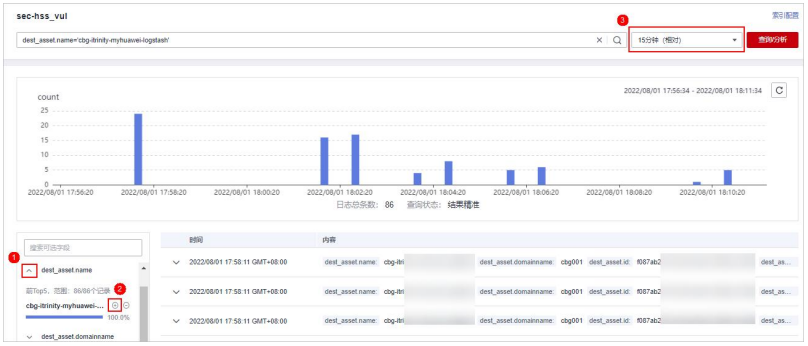
步骤 6 设置查询条件。

说明

如果筛留字段为 text 类型时，默认会使用 MATCH_QUERY 进行分词查询。

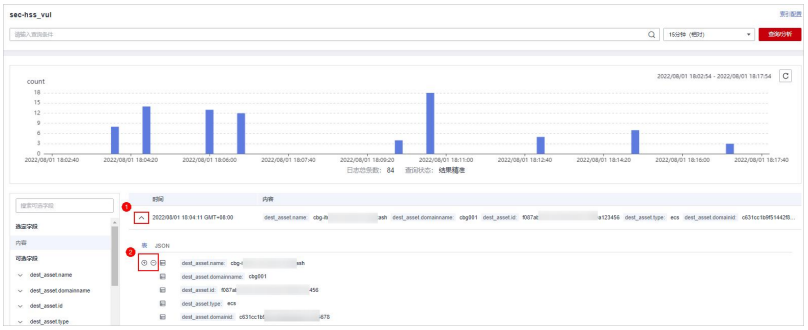
- 单击左侧可选字段前的，并单击待筛选或待排查字段名称后的（筛选某字段值）或（排除某字段值），查询框中将按照已筛选或排查的字段进行查询。

图 11-68 筛选某字段值（一）



- 如果您已展开某时间点的具体日志数据，需要筛选某些字段，可以单击该字段名称前的⊕（筛选某字段值）或⊖（排除某字段值），查询框中将按照已筛选或排查的字段进行查询。

  图 11-69 筛选某字段值（二）

步骤 7 默认查询并显示最近 15 分钟内数据。如果需要查询其他时间段日志数据，则需要设置查询时间，并单击“查询分析”。

----结束

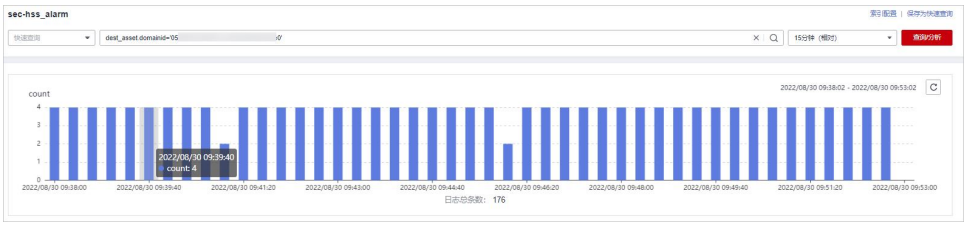
操作查询分析结果

态势感知（专业版）通过**原始日志**、**日志分布直方图**、**图表统计**形式展示查询分析结果。

- **日志分布直方图**

  此处将展示查询到的日志在时间上的分布情况，同时，将鼠标放在柱状图上，可查看该数据块代表的时间和日志命中次数。

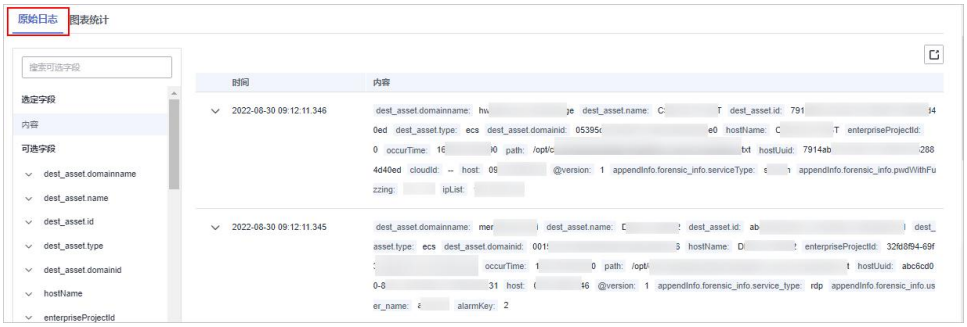
  图 11-70 日志分布直方图

- **原始日志**

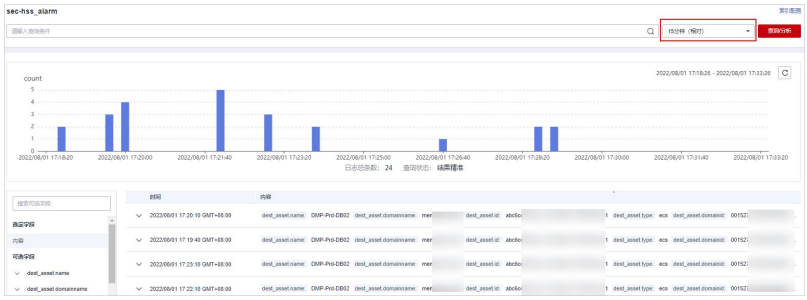
  在“原始日志”页签将展示当前查询结果。

图 11-71 原始日志



- 设置显示日志数据信息：
  - 页面中默认展示最近 15 分钟内的日志数据，如果需要展示其他时间数据，可以在右上角选择展示的时间。

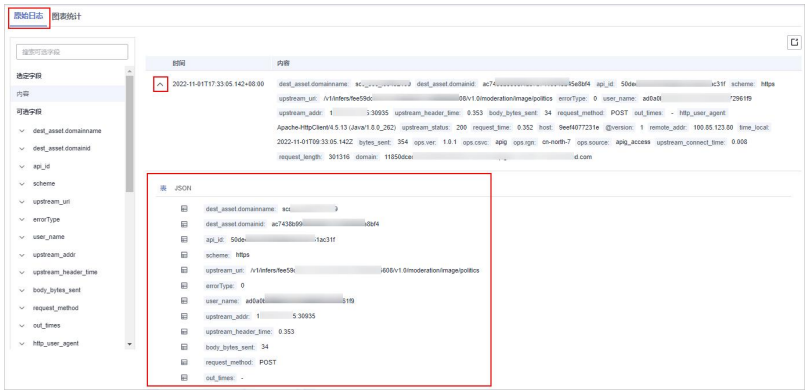
    图 11-72 选择显示时间

  - 如需查看某时间所有字段中的数据，可单击表格中对应时间前方的 展开所有数据，默认展示以表格形式展示数据。

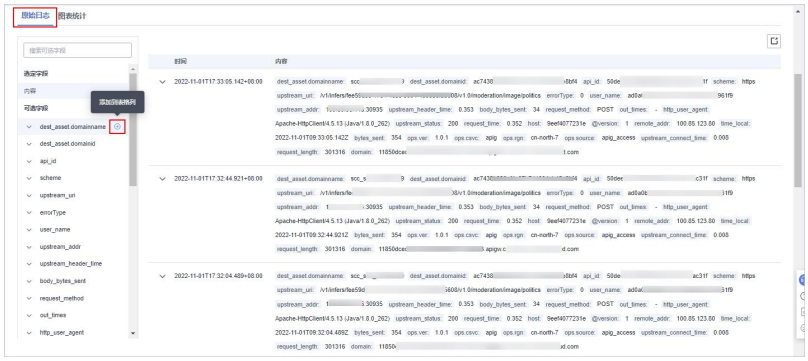
    如需查看 JSON 格式数据，可以选择“JSON”页签，页面将展示 JSON 格式的数据。

    图 11-73 展开显示数据

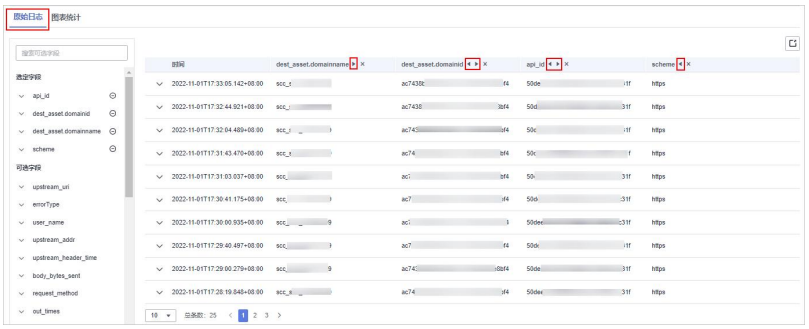
- 如需在列表中展示/筛选某些字段信息，可在右侧可选字段中选择需展示的字段，并单击字段名称后的⊕，该字段将显示在右侧日志数据列表中。

图 11-74 选中显示字段



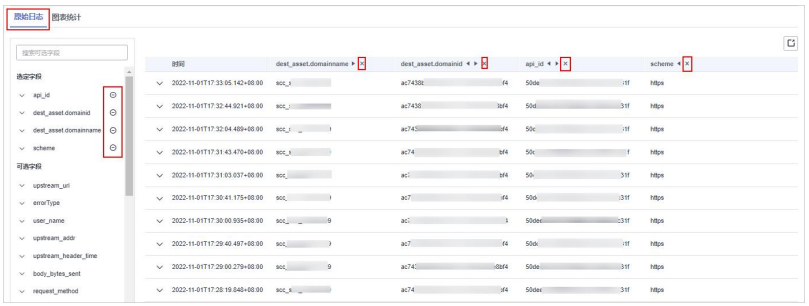
- 字段选中后，如需**调整显示先后顺序**，可在右侧日志数据列表的表头列单击该字段名称后的◀（向左移一列）、▶（向右移一列）按钮来进行调整。

图 11-75 调整顺序



- 字段选中后，如需**取消**，可在右侧日志数据列表的表头列单击该字段名称后的×按钮来进行取消，或左侧在“选定字段”单击该字段名称后的⊖按钮来取消显示。

图 11-76 取消选择



- 导出日志：在原始日志页签，在页面右上方单击图标，系统将自动下载当前原始日志表格到本地。

- **图表统计**

  查询语句查询后，在“图表统计”页签可以查看可视化的查询分析结果。

  图表统计是态势感知（专业版）根据查询分析语句渲染出的结果，提供有表格、线图、柱状图、饼图等多种图表类型，详细信息请参见 11.5.9.1 图表统计概述。

- **告警**

  在查询分析页面右上角单击“添加高警”，可以将查询分析结果设置告警，详细信息请参见 11.5.8 快速添加日志告警模型。

- **快速查询**

  在查询分析页面右上角单击“保存为快速查询”，可以将某一查询分析条件保存为快速查询，详细信息请参见 11.5.7 快速查询。

11.5.5 下载日志

操作场景

态势感知（专业版）支持将原始日志或查询分析日志下载到本地。

前提条件

已完成数据接入，详细操作请参见 13.2 数据集成。

操作步骤

步骤 1 登录管理控制台。

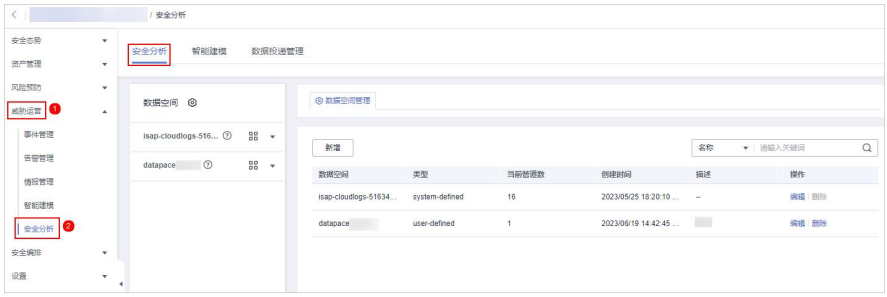
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-77 进入目标工作空间管理页面

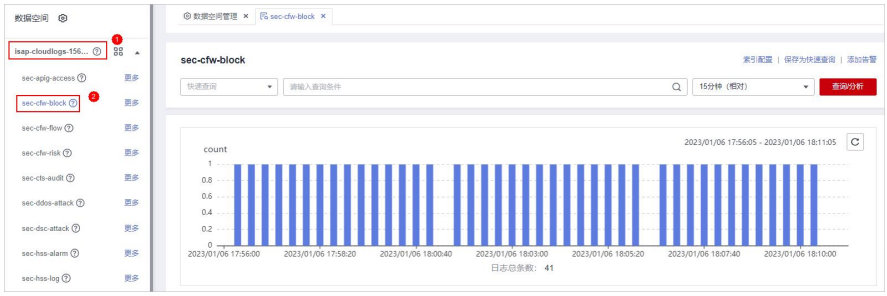
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-78 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-79 管道数据页面



步骤 6 （可选）在管道数据检索页面，输入查询条件，选择时间下拉菜单中选择查询时间，并单击“查询/分析”。

步骤 7 下载日志。

- 下载原始日志：在“原始日志”页签中，单击，系统将下载日志到本地。
- 下载图表日志：在“图表统计”页签中，单击“下载日志”，系统将下载日志到本地。

----结束

11.5.6 查询与分析语法-SQL 语法

11.5.6.1 基本语法

SQL 由查询语句和分析语句组成，以竖线 | 分隔。查询语句可单独使用，分析语句必须与查询语句一起使用。

```
查询语句 | 分析语句
```

表 11-1 基本语法

语句类型	说明

语句类型	说明
11.5.6.1.2 查询语句	查询语句用于指定日志查询时的筛选条件，返回符合条件的日志。通过设置筛选条件，可以帮助您快速、有效地查询到所需日志。
11.5.6.1.3 分析语句	分析语句用于对查询结果进行计算和统计。

11.5.6.2 约束与限制

- 查询语句不支持数学运算，比如：(age + 100) ≤ 1000。
- 聚合函数只支持字段，不支持表达式，比如 avg(log(age))。
- 不支持多表关联。
- 不支持子查询。
- 页面查询只支持返回 500 条。
- GROUP BY 分组上限为 10000 组。

11.5.6.3 查询语句

查询语句用于指定日志查询时的筛选条件，返回符合条件的日志。通过设置筛选条件，可以帮助您快速、有效地查询到所需日志。

本章节将介绍查询语句以及使用示例。

语法

查询语句有两种形式：

- 仅为*，表示不进行筛选，返回全量数据。
- 由一个或多个查询子句组成，子句间通过“NOT”、“AND”、“OR”连接，并支持使用“()”提高括号内查询条件的优先级。

查询子句基本结构如下所示：

```
字段名称 操作符 字段值
```

其中，可使用的操作符如操作符所示。

操作符

表 11-2 操作符说明

操作符	说明
=	查询某字段值**等于**某数值的日志。
<>	查询某字段值**不等于**某数值的日志。

操作符	说明
>	查询某字段值**大于**某数值的日志。
<	查询某字段值**小于**某数值的日志。
>=	查询某字段值**大于或等于**某数值的日志。
<=	查询某字段值**小于或等于**某数值的日志。
IN	查询某字段值**处于某数值范围内**的日志。
BETWEEN	查询某字段值**处于指定的范围内**的日志。
LIKE	全文搜索某字段值的日志。
IS NULL	查询某字段值为 NULL 的日志。
IS NOT NULL	查询某字段值为 NOT NULL 的日志。

示例

表 11-3 普通查询示例

查询需求	查询语句
查询所有日志	*
查询 GET 请求成功（状态码为 200~299）的日志。	request_method = 'GET' AND status BETWEEN 200 AND 299
查询 GET 请求或 POST 请求的日志。	request_method = 'GET' OR request_method = 'POST'
查询非 GET 请求的日志。	NOT request_method = 'GET'
查询 GET 请求或 POST 请求，且请求成功的日志。	(request_method = 'GET' OR request_method = 'POST') AND status BETWEEN 200 AND 299
查询 GET 请求或 POST 请求，且请求失败的日志。	(request_method = 'GET' OR request_method = 'POST') NOT status BETWEEN 200 AND 299
查询 GET 请求成功（状态码为 200~299）且请求时间大于等于 60 秒的日志。	request_method = 'GET' AND status BETWEEN 200 AND 299 AND request_time >= 60
查询请求时间为 60 秒的日志。	request_time = 60

11.5.6.4 分析语句语法

完整的分析语句语法如下：

```
SELECT [DISTINCT] (* | expression) [AS alias] [, ...]
[GROUP BY expression [, ...] [HAVING predicates]]
[ORDER BY expression [ASC | DESC] [, ...]]
[LIMIT size OFFSET offset]
```

11.5.6.5 分析语句-SELECT

指定查询的字段。

使用*查询所有字段

```
SELECT *
```

表 11-4 使用*查询所有字段

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36
13	Nanette	F	Nogal	32838	Quility	VA	Bates	28
18	Dale	M	Orick	4180	null	MD	Adams	32

查询指定字段

```
SELECT firstname, lastname
```

表 11-5 查询指定字段

firstname	lastname
Amber	Duke
Hattie	Bond
Nanette	Bates
Dale	Adams

使用 AS 给字段定义别名

```
SELECT account_number AS num
```

表 11-6 使用 AS 给字段定义别名

num

num
1
16
13
18

使用 DISTINCT 去重

```
SELECT DISTINCT age
```

表 11-7 使用 DISTINCT 去重

age
32
36
28

使用 SQL 函数

函数相关内容请参见函数。

```
SELECT LENGTH(firstname) as len, firstname
```

表 11-8 使用 SQL 函数

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

11.5.6.6 分析语句-GROUP BY

按值分组。

按字段的值分组

```
SELECT age GROUP BY age
```

表 11-9 按字段的值分组

age
28
32
36

按字段别名分组

```
SELECT account_number AS num GROUP BY num
```

表 11-10 按字段别名分组

num
1
16
13
18

按多个字段分组

```
SELECT account_number AS num, age GROUP BY num, age
```

表 11-11 按多个字段分组

num	age
1	32
16	36
13	28
18	32

使用 SQL 函数

函数相关内容请参见函数。

```
SELECT LENGTH(lastname) AS len, COUNT(*) AS count GROUP BY LENGTH(lastname)
```

表 11-12 使用 SQL 函数

len	count

len	count
4	2
5	2

11.5.6.7 分析语句-HAVING

在分组的基础上，结合聚合函数来筛选数据。

```
SELECT age, MAX(balance) GROUP BY age HAVING MIN(balance) > 10000
```

表 11-13 HAVING

age	MAX(balance)
28	32838
32	39225

11.5.6.8 分析语句-ORDER BY

按字段值排序。

使用字段值排序

```
SELECT age ORDER BY age DESC
```

表 11-14 使用字段值排序

age
28
32
32
36

11.5.6.9 分析语句-LIMIT

指定返回数据的条数。

指定返回的条数

```
SELECT * LIMIT 1
```

表 11-15 指定返回的条数

account_number	firstname	gender	city	balance	employer	state	lastname	age
1	Amber	M	Brogan	39225	Pyrami	IL	Duke	32

指定返回的条数和偏移量

```
SELECT * LIMIT 1 OFFSET 1
```

表 11-16 指定返回的条数和偏移量

account_number	firstname	gender	city	balance	employer	state	lastname	age
16	Hattie	M	Dante	5686	Netagy	TN	Bond	36

11.5.6.10 分析语句-函数

数学类

表 11-17 数学类

函数	作用	定义	示例
abs	绝对值	abs(number T) -> T	SELECT abs(0.5) LIMIT 1
add	加法	add(number T, number) -> T	SELECT add(1, 5) LIMIT 1
cbrt	立方根	cbrt(number T) -> T	SELECT cbrt(0.5) LIMIT 1
ceil	向上取整	ceil(number T) -> T	SELECT ceil(0.5) LIMIT 1
divide	除法	divide(number T, number) -> T	SELECT divide(1, 0.5) LIMIT 1
e	自然底数 e	e() -> double	SELECT e() LIMIT 1
exp	自然底数 e 的次幂	exp(number T) -> T	SELECT exp(0.5) LIMIT 1
expm1	自然底数 e 的次幂减一	expm1(number T) -> T	SELECT expm1(0.5) LIMIT 1
floor	向下取整	floor(number T) -> T	SELECT floor(0.5) AS Rounded_Down LIMIT 1

函数	作用	定义	示例
ln	自然对数	ln(number T) -> double	SELECT ln(10) LIMIT 1
log	以 T 为底数的对数	log(number T, number) -> double	SELECT log(10) LIMIT 1
log2	以 2 为底数的对数	log2(number T) -> double	SELECT log2(10) LIMIT 1
log10	以 10 为底数的对数	log10(number T) -> double	SELECT log10(10) LIMIT 1
mod	取余	mod(number T, number) -> T	SELECT modulus(2, 3) LIMIT 1
multiply	乘法	multiply(number T, number) -> number	SELECT multiply(2, 3) LIMIT 1
pi	π	pi() -> double	SELECT pi() LIMIT 1
pow	T 的次幂	pow(number T, number) -> T	SELECT pow(2, 3) LIMIT 1
power	T 的次幂	power(number T) -> T, power(number T, number) -> T	SELECT power(2, 3) LIMIT 1
rand	随机数	rand() -> number, rand(number T) -> T	SELECT rand(5) LIMIT 1
rint	舍弃小数	rint(number T) -> T	SELECT rint(1.5) LIMIT 1
round	四舍五入	round(number T) -> T	SELECT round(1.5) LIMIT 1
sign	符号	sign(number T) -> T	SELECT sign(1.5) LIMIT 1
signum	符号	signum(number T) -> T	SELECT signum(0.5) LIMIT 1
sqrt	平方根	sqrt(number T) -> T	SELECT sqrt(0.5) LIMIT 1
subtract	减法	subtract(number T, number) -> T	SELECT subtract(3, 2) LIMIT 1
/	除法	number / number -> number	SELECT 1 / 100 LIMIT 1
%	取余	number % number -> number	SELECT 1 % 100 LIMIT 1

三角函数

表 11-18 三角函数

函数	作用	定义	示例
acos	反余弦	acos(number T) -> double	SELECT acos(0.5) LIMIT 1
asin	反正弦	asin(number T) -> double	SELECT asin(0.5) LIMIT 1
atan	反正切	atan(number T) -> double	SELECT atan(0.5) LIMIT 1
atan2	T 和 U 相除的结果的反正切	atan2(number T, number U) -> double	SELECT atan2(1, 0.5) LIMIT 1
cos	余弦	cos(number T) -> double	SELECT cos(0.5) LIMIT 1
cosh	双曲余弦	cosh(number T) -> double	SELECT cosh(0.5) LIMIT 1
cot	余切	cot(number T) -> double	SELECT cot(0.5) LIMIT 1
degrees	弧度转换为度	degrees(number T) -> double	SELECT degrees(0.5) LIMIT 1
radians	度转换为弧度	radians(number T) -> double	SELECT radians(0.5) LIMIT 1
sin	正弦	sin(number T) -> double	SELECT sin(0.5) LIMIT 1
sinh	双曲正弦	sinh(number T) -> double	SELECT sinh(0.5) LIMIT 1
tan	正切	tan(number T) -> double	SELECT tan(0.5) LIMIT 1

时间函数

表 11-19 时间函数

函数	作用	定义	示例
curdate	当前日期	curdate() -> date	SELECT curdate() LIMIT 1
date	日期	date(date) -> date	SELECT date() LIMIT 1
date_format	根据格式获取对应日期值	date_format(date, string) -> string	SELECT date_format(date, 'Y') LIMIT 1
day_of_month	月份	day_of_month(date) -> integer	SELECT day_of_month(date) LIMIT 1
day_of_week	周几	day_of_week(date) -> integer	SELECT day_of_week(date) LIMIT 1

函数	作用	定义	示例
day_of_year	当年天数	day_of_year(date) -> integer	SELECT day_of_year(date) LIMIT 1
hour_of_day	当天小时数	hour_of_day(date) -> integer	SELECT hour_of_day(date) LIMIT 1
maketime	生成日期	maketime(integer, integer, integer) -> time	SELECT maketime(11, 30, 00) LIMIT 1
minute_of_hour	当前小时分钟数	minute_of_hour(date) -> integer	SELECT minute_of_hour(date) LIMIT 1
minute_of_day	当天分钟数	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
monthname	月份名称	monthname(date) -> string	SELECT monthname(date) LIMIT 1
now	当前时间	now() -> time	SELECT now() LIMIT 1
second_of_minute	秒数	minute_of_day(date) -> integer	SELECT minute_of_day(date) LIMIT 1
timestamp	日期	timestamp(date) -> date	SELECT timestamp(date) LIMIT 1
year	年份	year(date) -> integer	SELECT year(date) LIMIT 1

文本函数

表 11-20 文本函数

函数	作用	定义	示例
ascii	第一个字符的 ASCII 值	ascii(string T) -> integer	SELECT ascii('t') LIMIT 1
concat_ws	连接字符串	concat_ws(separator, string, string) -> string	SELECT concat_ws('-', 'Tutorial', 'is', 'fun!') LIMIT 1
left	从左往右取字符串	left(string T, integer) -> T	SELECT left('hello', 2) LIMIT 1
length	长度	length(string) -> integer	SELECT length('hello') LIMIT 1
locate	查找字符串	locate(string, string) -> integer	SELECT locate('o', 'hello') LIMIT 1
replace	替换字符串	replace(string T, string, string) -> T	SELECT replace('hello', 'l', 'x') LIMIT 1

函数	作用	定义	示例
right	从右往左取字符串	right(string T, integer) -> T	SELECT right('hello', 1) LIMIT 1
rtrim	去除右侧空字符串	rtrim(string T) -> T	SELECT rtrim('hello ') LIMIT 1
substring	取子字符串	substring(string T, integer, integer) -> T	SELECT substring('hello', 2,5) LIMIT 1
trim	去除两侧空字符串	trim(string T) -> T	SELECT trim(' hello ') LIMIT 1
upper	全部转为大写	upper(string T) -> T	SELECT upper('helloworld') LIMIT 1

其他

表 11-21 其他

函数	作用	定义	示例
if	if 判断	if(boolean, object, object) -> object	SELECT if(false, 0, 1) LIMIT 1 , SELECT if(true, 0, 1) LIMIT 1
ifnull	字段为 null 时，填充默认值	ifnull(object, object) -> object	SELECT ifnull('hello', 1) LIMIT 1 , SELECT ifnull(null, 1) LIMIT 1
isnull	字段是否为 null，是返回 1，否返回 0	isnull(object) -> integer	SELECT isnull(null) LIMIT 1 , SELECT isnull(1) LIMIT 1

11.5.6.11 分析语句-聚合函数

表 11-22 聚合函数

函数	作用	定义	示例
avg	求平均	avg(number T) -> T	SELECT avg(age) LIMIT 1
sum	求和	sum(number T) -> T	SELECT sum(age) LIMIT 1
min	最小值	min(number T) -> T	SELECT min(age) LIMIT 1
max	最大值	max(number T) -> T	SELECT max(age) LIMIT 1

函数	作用	定义	示例
count	次数	count(field) -> integer , count(*) -> integer , count(1) -> integer	SELECT count(age) LIMIT 1 , SELECT count(*) LIMIT 1 , SELECT count(1) LIMIT 1

11.5.7 快速查询

操作场景

快速查询为态势感知（专业版）提供的用于保存查询分析操作的功能。您可以将某个常用的查询分析语句另存为快速查询，以便后续直接使用，快速执行查询分析操作。

本章节将介绍如何创建快速查询。

前提条件

已配置索引，详细操作请参见 11.5.3 配置索引。

创建快速查询

步骤 1 登录管理控制台。

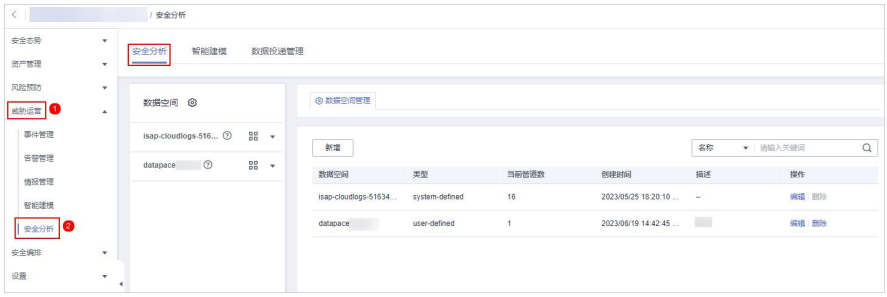
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-80 进入目标工作空间管理页面

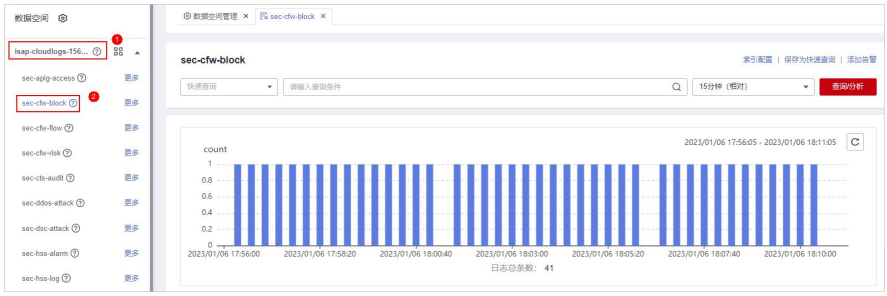
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-81 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-82 管道数据页面



步骤 6 输入查询分析语句，设置时间范围，并单击“查询分析”。

更多查询分析详细操作请参见 11.5.4 查询与分析。

步骤 7 单击页面右上角“保存为快速查询”，在右侧页面中配置查询参数。

表 11-23 快速查询参数配置

参数名称	参数说明
查询名称	设置快速查询的名称。
查询语句	系统自动生成步骤 6 中输入的查询语句。

步骤 8 单击“确定”。

创建快速查询后，您可以在管道数据的查询分析页面中，单击快速查询搜索框中的，并选择目标快速查询名称，即可使用快速查询。

----结束

11.5.8 快速添加日志告警模型

操作场景

态势感知（专业版）支持将查询分析结果设置告警模型，并在满足条件时触发告警。

本章节将接入如何快速为日志设置告警模型。

前提条件

已完成数据接入，详细操作请参见 13.2 数据集成。

操作步骤

步骤 1 登录管理控制台。

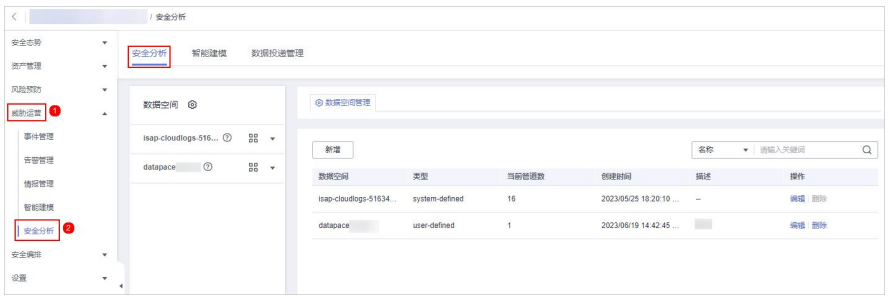
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-83 进入目标工作空间管理页面

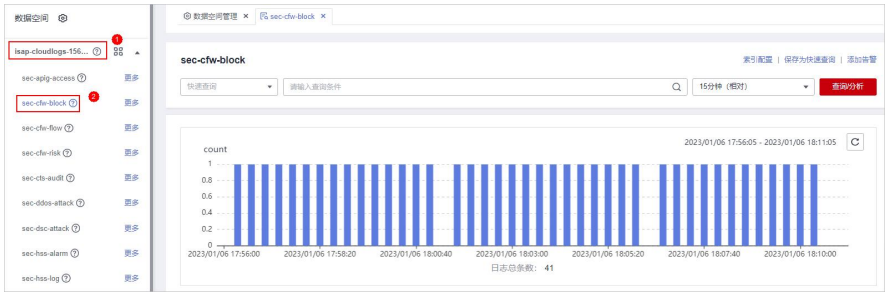
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-84 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-85 管道数据页面

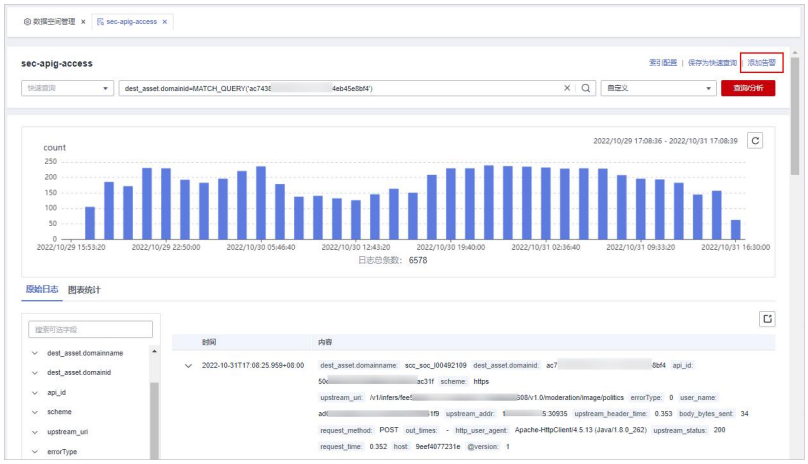


步骤 6 输入查询分析语句，设置时间范围，并单击“查询分析”，显示查询分析结果。

更多查询分析详细操作请参见 11.5.4 查询与分析。

步骤 7 单击页面右上角“添加告警”，进入新建告警模型页面。

图 11-86 添加告警



步骤 8 配置告警基础信息，参数说明如表 11-47 所示。

表 11-24 告警模型基础配置

参数名称	参数说明
管道名称	该告警模型的执行管道，系统默认生成。
模型名称	自定义该条告警模型的名称。
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
描述	填写该告警模型的描述信息。

参数名称	参数说明
启用状态	设置该告警模型的启用状态。 •  ：表示启用，默认为此状态。 •  ：表示未启用。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤 9 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤 10 设置模型逻辑，参数说明如表 11-48 所示。

表 11-25 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。
查询计划	设置告警查询计划。 • 运行查询间隔：xx 分钟/小时/天。 当运行查询间隔为分钟时，可设置为 5-59 分钟；当运行查询为小时时，可设置为 1-23 小时；当运行查询为天时，可设置为 1-14 天。 • 时间窗口：xx 分钟/小时/天。 当时间窗口为分钟时，可设置为 5-59 分钟；当时间窗口为小时时，可设置为 1-23 小时；当时间窗口为天时，可设置为 1-14 天。 • 延迟执行时间：xx 分钟，可以设置为 0-5 分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置 key+value 信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于 xx 时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警

参数名称	参数说明
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。

步骤 11 设置完成后，单击页面右下角“下一步”，进入模型详情预览页面。

步骤 12 预览确认无误后，单击页面右下角“确定”。

----结束

11.5.9 图表统计

11.5.9.12 图表统计概述

当您执行了查询分析语句后，态势感知（专业版）支持通过图表统计的形式对查询和分析的结果进行可视化展示。同时，还支持将指标保存为卡片，方便后续在布局中使用。

目前支持以下图表类型：

- 11.5.9.2 表格
- 11.5.9.3 折线图
- 11.5.9.4 柱状图
- 11.5.9.5 饼图

11.5.9.13 表格

查询分析结果可以通过表格形式进行展示。

表格为最常见的数据展示类型，通过对数据的整理，可以快速对数据进行分析。在态势感知（专业版）中，通过查询分析语句得到的数据结果在图标统计中，默认以表格形式进行展示。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

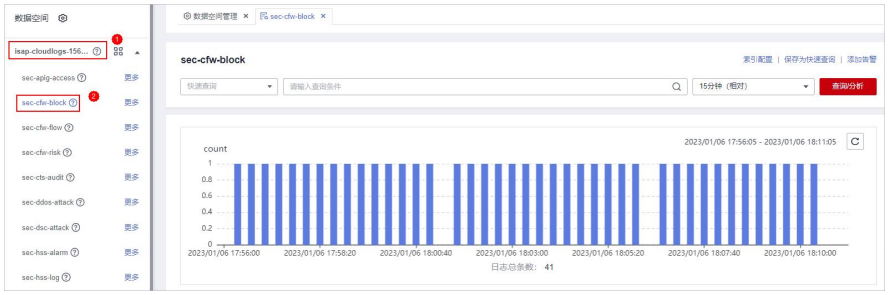
图 11-87 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-88 进入安全分析页面

步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-89 管道数据页面



步骤 6 输入查询分析语句，设置时间范围，并单击“查询分析”。

步骤 7 选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中单击 。

步骤 8 配置表格参数。

表 11-26 表格参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义表格标题名称。

参数类别	参数名称	参数说明
图表配置	隐藏字段	选择目标字段，将该字段在表格中隐藏。

图表设置完成后，左侧可预览配置后的数据分析情况。

----结束

相关操作

- 添加指标卡：配置后，如需将指标信息保存为卡片，可单击表格右上角“添加指标卡”，并在弹出的对话框中，设置指标卡名称后，单击“保存”。
- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

11.5.9.14 折线图

查询分析结果可以通过折线图形式进行展示。

折线图一般用于展示一组数据在某一周期内的某一个有序数据类别上的变化情况，属于趋势类的分析图表，可以清晰直观地分析数据变化的趋势。

操作步骤

步骤 1 登录管理控制台。

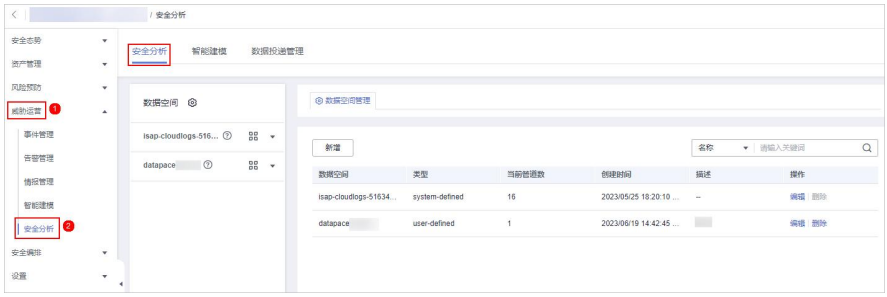
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-90 进入目标工作空间管理页面

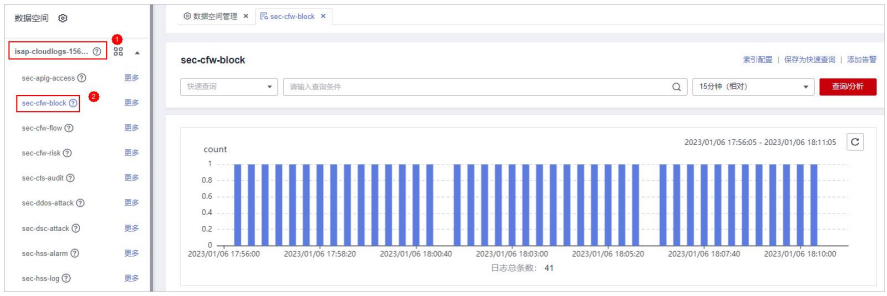
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-91 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-92 管道数据页面



步骤 6 输入查询分析语句，设置时间范围，并单击“查询分析”。

步骤 7 选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中单击  。

步骤 8 配置折线图参数。

表 11-27 折线图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	X 轴标题	自定义 X 轴标题名称。
	Y 轴标题	自定义 Y 轴标题名称。
	X 轴字段	选择 X 轴显示字段。
	Y 轴字段	选择 Y 轴显示字段。
图例配置	显示图例	确认是否显示图例。
	图例位置	开启显示图例时须配置。 图例在图表中的位置，可以配置为上、下、左和右。

图表设置完成后，左侧可预览配置后的数据分析情况。

----结束

相关操作

- 添加指标卡：配置后，如需将指标信息保存为卡片，可单击表格右上角“添加指标卡”，并在弹出的对话框中，设置指标卡名称后，单击“保存”。
- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

11.5.9.15 柱状图

查询分析结果可以通过柱状图形式进行展示。

柱状图是一种由矩形表示类别的数据显示方法，可以在多个数据和趋势分析之间进行清晰比较。态势感知（专业版）中，柱状图默认采用垂直柱子（即矩形块的宽度一定，高度代表数值大小）来展示数据。

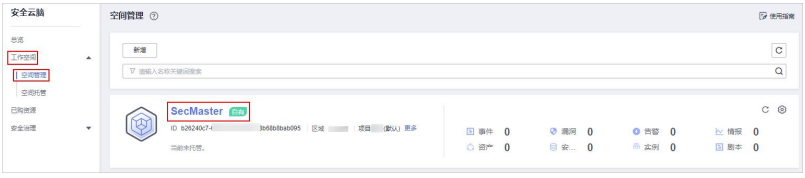
操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

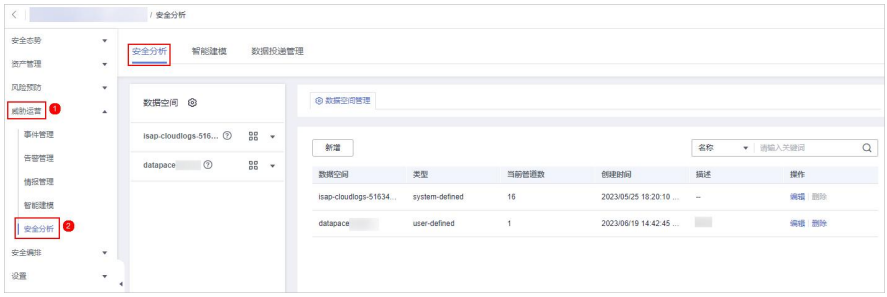
步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-93 进入目标工作空间管理页面



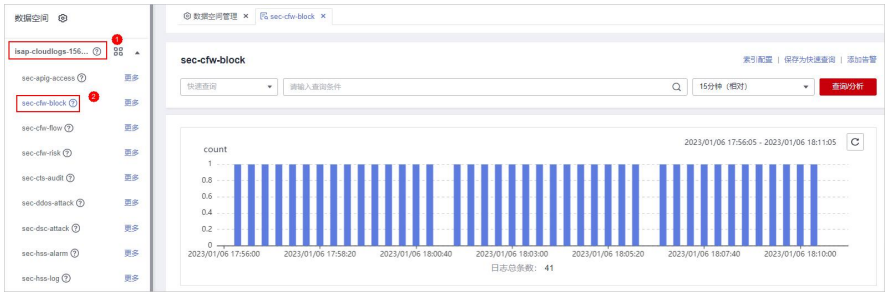
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-94 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-95 管道数据页面



步骤 6 输入查询分析语句，设置时间范围，并单击“查询分析”。

步骤 7 选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中单击  。

步骤 8 配置柱状图参数。

表 11-28 柱状图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	X 轴标题	自定义 X 轴标题名称。
	Y 轴标题	自定义 Y 轴标题名称。
	X 轴字段	选择 X 轴显示字段。
	Y 轴字段	选择 Y 轴显示字段。
图例配置	显示图例	确认是否显示图例。
	图例位置	开启显示图例时须配置。 图例在图表中的位置，可以配置为上、下、左和右。

图表设置完成后，左侧可预览配置后的数据分析情况。

----结束

相关操作

- 添加指标卡：配置后，如需将指标信息保存为卡片，可单击表格右上角“添加指标卡”，并在弹出的对话框中，设置指标卡名称后，单击“保存”。
- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

11.5.9.16 饼图

查询分析结果可以通过饼图形式进行展示。

饼图用于表示不同分类的占比情况，通过弧度大小来对比各种分类。

操作步骤

步骤 1 登录管理控制台。

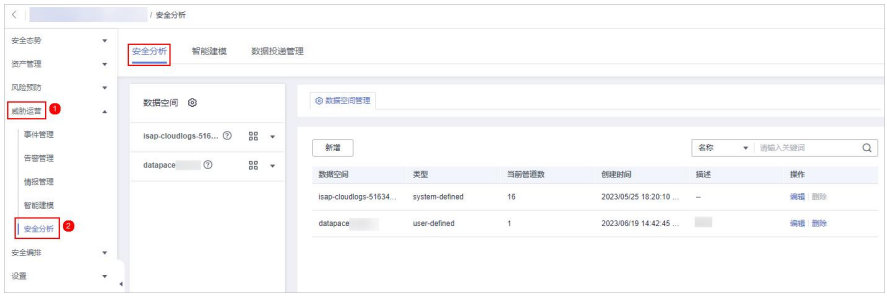
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-96 进入目标工作空间管理页面

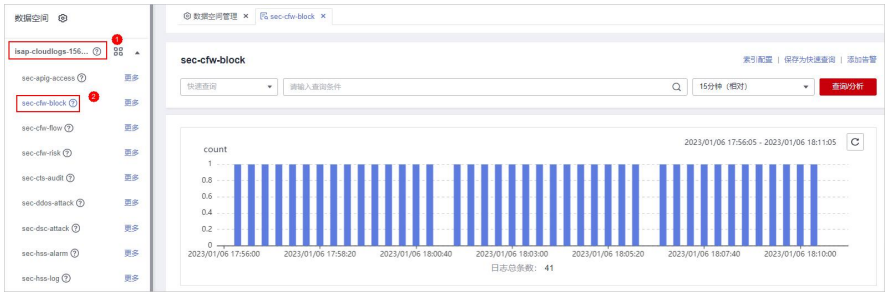
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-97 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-98 管道数据页面



步骤 6 输入查询分析语句，设置时间范围，并单击“查询分析”。

步骤 7 选择“图表统计”页签，并在图表统计页面右侧的“图表类型”中单击  。

步骤 8 配置饼图参数。

表 11-29 饼图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	分类	数据分类。
	数列值	分类数据对应的数值。
图例配置	显示图例	确认是否显示图例。
	图例位置	开启显示图例时须配置。 图例在图表中的位置，可以配置为上、下、左和右。

图表设置完成后，左侧可预览配置后的数据分析情况。

----结束

相关操作

- 添加指标卡：配置后，如需将指标信息保存为卡片，可单击表格右上角“添加指标卡”，并在弹出的对话框中，设置指标卡名称后，单击“保存”。
- 下载日志：配置后，如需导出当前查询分析数据，可单击表格右上角“下载日志”，系统将下载当前查询分析日志数据至本地。
- 收起配置：图表配置完成后，在“预览图表”右侧单击“收起配置”，页面将不显示图表配置参数。
- 展开配置：图标配置收起后，如需再次配置，可在“预览图表”右侧单击“展开配置”。

11.5.10 管理数据空间

11.5.10.1 新增数据空间

操作场景

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一载均衡策略。

当您需要使用态势感知（专业版）提供的**安全分析**、**数据分析**、**智能建模**等功能时，需要新增数据空间。

本章节介绍如何创建数据空间。

前提条件

已新增工作空间，具体操作请参见 5.2 新增工作空间。

约束与限制

一个工作空间中最多可创建 5 个数据空间。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-99 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-100 进入安全分析页面

步骤 5 在数据空间列表左上角，单击“新增”，系统从右侧弹出新增数据空间界面。

图 11-101 新增数据空间

步骤 6 在新增数据空间页面中，配置新建数据空间参数，参数说明如表 11-53 所示。

表 11-30 新增数据空间

参数名称	参数说明
数据空间	输入数据空间名称。命名规则如下： • 名称长度取值范围为 5-63 个字符。 • 可包含英文字母、数字和-。其中，-不能出现在开头和结尾，且不能连续出现。 • 名称须为全局唯一，不能与其他数据空间名称相同。
描述	可选参数，设置该数据空间的备注信息。

步骤 7 单击“确定”，完成数据空间的新增。

新增完成后，可以在数据空间列表中查看已新增的数据空间。

----结束

11.5.10.2 查看数据空间详情

操作场景

该任务指导用户通过管理控制台查看数据空间的信息，包括名称、类型和创建时间等。

操作步骤

步骤 1 登录管理控制台。

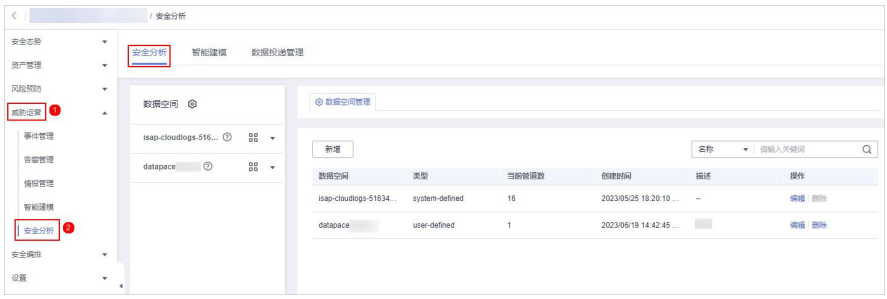
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-102 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-103 进入安全分析页面



步骤 5 在数据空间管理页面中，查看全部数据空间信息，相关参数说明如表 11-54 所示。

表 11-31 数据空间

参数名称	参数说明
数据空间	数据空间名称。
类型	数据空间中的数据所属类型，包含以下两种类型： • system-defined：数据接入时，系统默认创建的数据空间。 • user-defined：用户自行创建的数据空间。
当前管道数	数据空间中目前已有管道的数量。
创建时间	数据空间的创建时间。
描述	数据空间的描述信息。
操作	用户可以在操作栏中，执行编辑、删除等操作。

步骤 6 在左侧数据空间栏中，单击某个数据空间名称后的 ，右侧弹出当前数据空间的详情。

图 11-104 进入数据空间详情页面

步骤 7 在数据空间详情中，可以查看某个数据空间的详细信息，参数说明如表 11-55 所示。

表 11-32 数据空间详情

参数名称	参数说明
数据空间	数据空间名称。
当前管道数	该数据空间中目前已有管道的数量。
创建时间	数据空间的创建时间。
描述	数据空间的描述信息。

----结束

11.5.10.3 编辑数据空间

操作场景

数据空间新增成功后，如果需要对其**描述信息**进行修改，可参见本章节进行处理。

操作步骤

步骤 1 登录管理控制台。

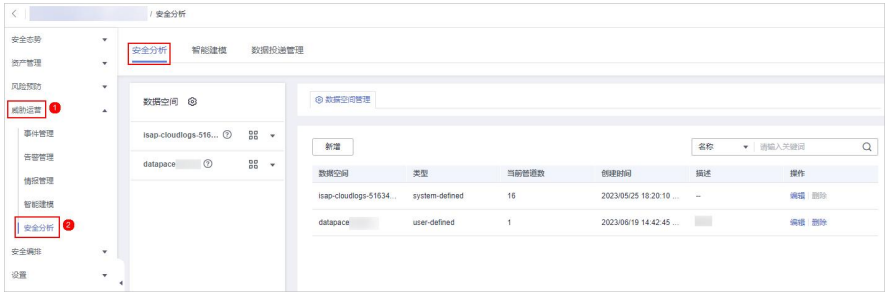
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-105 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-106 进入安全分析页面



步骤 5 在待编辑数据空间所在行“操作”列，单击“编辑”。

步骤 6 在弹出编辑数据空间界面，修改数据空间描述信息。

步骤 7 单击“确定”。

----结束

11.5.10.4 删除数据空间

操作场景

如果不再需要某个数据空间，可以参照本章节进行删除。

约束与限制

- 系统创建默认数据空间**不支持**删除操作。
- 如果待删除数据空间中，存在数据管道，则该数据空间不能直接删除。您需要先删除数据管道，再删除数据空间。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-107 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-108 进入安全分析页面

步骤 5 在需要删除的数据空间所在行的“操作”列，单击“删除”。

步骤 6 在弹出的对话框中单击“确认”，完成删除数据空间的操作。

> **⚠ 注意**
>
> 如果待删除数据空间中，存在数据管道，则该数据空间不能直接删除。您需要先删除数据管道，再删除数据空间。

----结束

11.5.11 管理管道

11.5.11.1 创建管道

操作场景

数据传输消息主题和存储索引组合为数据管道。

当您需要使用态势感知（专业版）提供的**安全分析**、**数据分析**、**智能建模**功能时，需要创建管道。

本章节介绍如何创建管道。

前提条件

- 已新建工作空间，具体操作请参见 5.2 新增工作空间。
- 已新增数据空间，具体操作请参见 11.5.10.1 新增数据空间。

约束与限制

一个数据空间中最多可创建 20 个数据管道。

操作步骤

步骤 1 登录管理控制台。

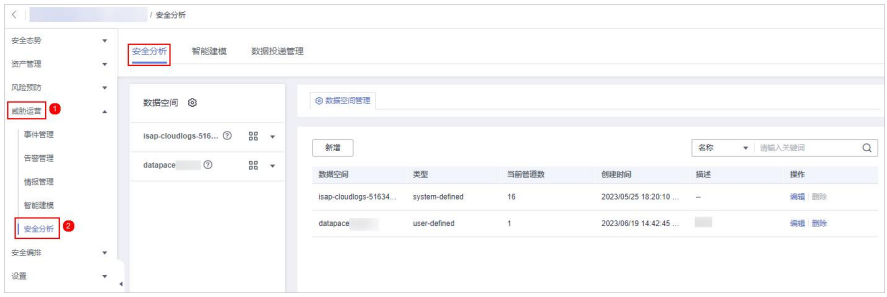
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-109 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-110 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称右侧的，并在下拉选项中选择的“创建管道”，系统从右侧弹出创建管道页面。

图 11-111 创建管道

步骤 6 在创建管道页面中，配置管道参数，参数说明如表 11-56 所示。

表 11-33 创建管道

参数名称	参数说明
数据空间	该管道所属的数据空间，系统默认生成。
管道名称	自定义管道的名称。命名规则如下： • 名称长度取值范围为 5-63 个字符。 • 可包含英文字母、数字和-。其中，-不能出现在开头和结尾，且不能连续出现。 • 名称须为数据空间中的唯一，不能与数据空间中其他管道名称相同。
Shard 数	该管道的 Shard 数量。取值范围为：1-64。
生命周期	该管道内数据的生命周期。取值范围为：7-180。
描述	可选参数，设置该管道的备注信息。

步骤 7 单击“确定”。

创建成功后，可单击数据空间名称或数据空间栏后的，展开查看已创建的管道。

----结束

11.5.11.2 查看管道详情

操作场景

该任务指导用户通过管理控制台查看管道的信息，包括名称、所属数据空间和创建时间等。

操作步骤

步骤 1 登录管理控制台。

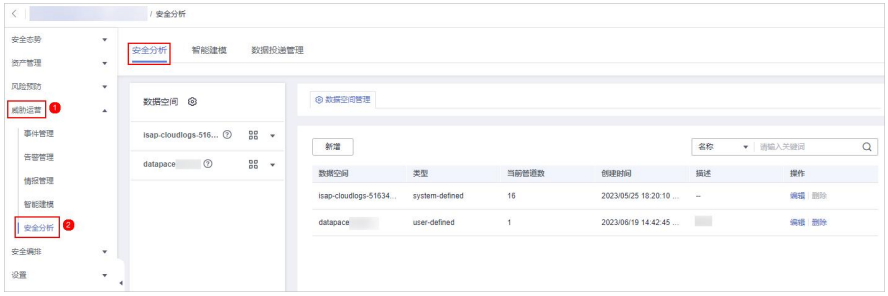
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-112 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-113 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的，展开已创建的管道。

图 11-114 查看管道

步骤 6 单击待查看管道名称后的，右侧将显示管道的详细信息。

表 11-34 管道参数说明

参数名称	参数说明
工作空间名称	当前管道所属工作空间的名称。
工作空间 ID	当前管道所属工作空间的 ID。
数据空间名称	当前管道所属数据空间的名称。
数据空间 ID	当前管道所属数据空间的 ID。
管道名称	当前管道的名称。
管道 ID	当前管道的 ID。
Shard 数	管道的 Shard 数。
生命周期	管道内数据保存周期。
创建时间	管道的创建时间。
描述	管道的描述信息。

----结束

11.5.11.3 编辑管道

操作场景

管道创建成功后，可对管道 **Shard 数**、**描述**、**生命周期**进行修改。

本章节介绍如何修改管道参数信息。

约束与限制

系统创建的数据管道**不支持**编辑操作。

操作步骤

步骤 1 登录管理控制台。

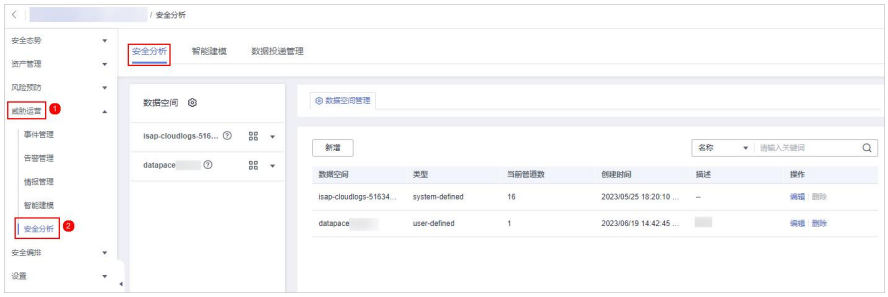
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-115 进入目标工作空间管理页面

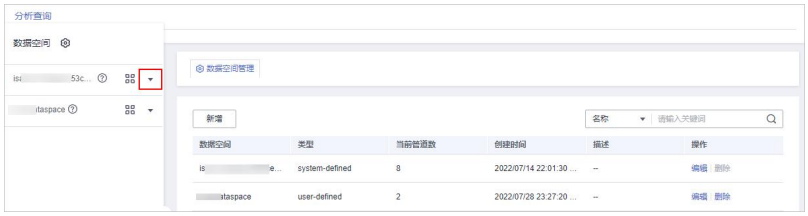
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-116 进入安全分析页面



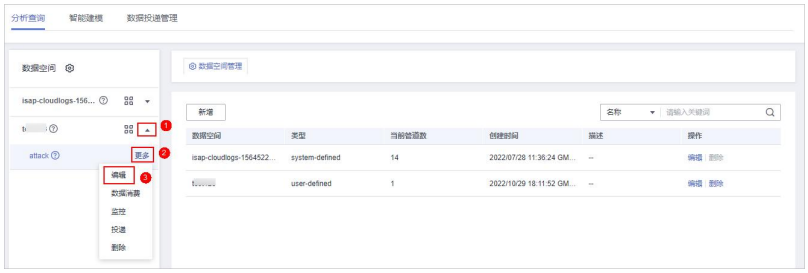
步骤 5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的 ▼，展开已创建的管道。

图 11-117 查看管道



步骤 6 单击管道名称后的“更多 > 编辑”。

图 11-118 编辑管道入口



步骤 7 从编辑管道页面中，配置管道参数，参数说明如表 11-58 所示。

表 11-35 编辑管道

参数名称	参数说明
数据空间	该管道所属的数据空间。系统默认，**不支持**修改。
管道名称	您创建管道时设置的名称，创建后**不支持**修改。
Shard 数	该管道的 Shard 数量。取值范围为：1-64。
生命周期	该管道内数据的生命周期。取值范围：7-180。
描述	可选参数，设置该管道的备注信息。

步骤 8 单击“确定”。

----结束

11.5.11.4 删除管道

操作场景

本章节介绍如何删除管道。

数据将会被同步删除，且不可恢复，请谨慎操作。

约束与限制

系统创建的数据管道**不支持**删除操作。

操作步骤

步骤 1 登录管理控制台。

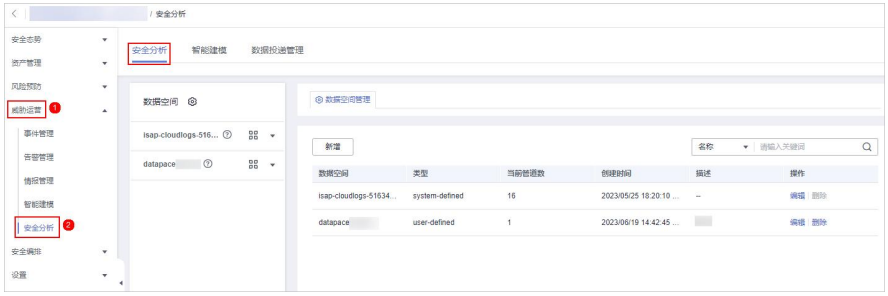
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-119 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-120 进入安全分析页面

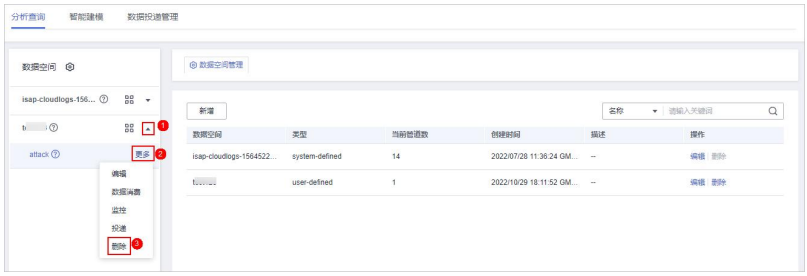


步骤 5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的 ▼，展开已创建的管道。

图 11-121 查看管道

步骤 6 单击管道名称后的“更多 > 删除”。

图 11-122 删除管道



步骤 7 在弹出的删除确认框中，单击“确认”，完成删除管道的操作。

----结束

11.6 数据消费

数据消费是指第三方软件、云产品等通过客户端实时消费日志服务的数据，是对全量数据的顺序读写。

态势感知（专业版）提供数据消费功能，支持通过客户端实时消费数据。

开启数据消费

步骤 1 登录管理控制台。

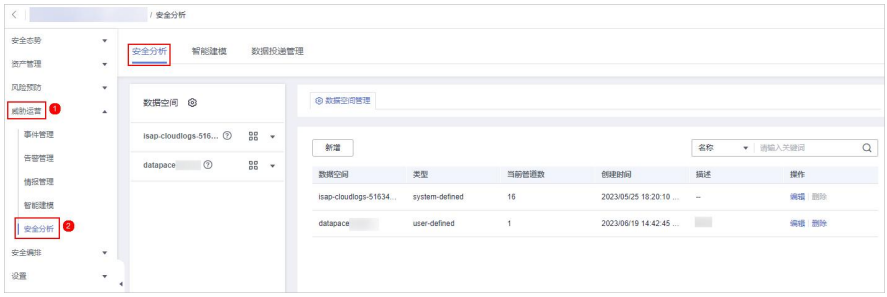
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-123 进入目标工作空间管理页面

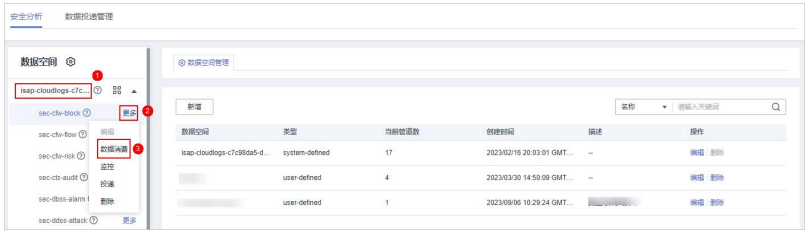
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-124 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，单击目标管道名称后的“更多 > 数据消费”，进入数据消费页面。

图 11-125 进入数据消费页面



步骤 6 在数据消费页面中，单击当前状态后的  ，开启数据消费。

开启后，将显示消费配置信息，具体说明如表 11-59 所示。

表 11-36 数据消费参数说明

参数名称	参数说明
当前状态	当前管道中数据消费配置状态。
管道名称	当前数据管道的名称。
订阅器	系统预制的订阅模式，决定数据如何传递给消费者。
访问节点	当前数据的访问节点。

----结束

相关操作

数据消费开启后，如需关闭，则可在数据消费页面，单击“当前状态”后的  ，关闭数据消费。

11.7 数据投递

11.7.1 新增数据投递

操作场景

态势感知（专业版）支持将数据实时投递至其他管道或其他云产品中，便于您存储数据或联合其它系统消费数据。配置数据投递后，态势感知（专业版）将定时将采集到的数据投递至其他管道或对应的云产品。

目前支持投递到以下云产品中：对象存储服务（Object Storage Service，OBS）、云日志服务（Log Tank Service，LTS）。

本章节介绍如何新增数据投递。

前提条件

- 如需投递到 OBS 中，需要已有一个**桶策略**为**公共读写**的可用的桶。
- 如需投递到 LTS 中，需要已有可用的日志组和日志流。

约束与限制

跨账号投递仅支持投递到其他账号管道中，不支持投递到其他云服务。

新增数据投递

步骤 1 登录管理控制台。

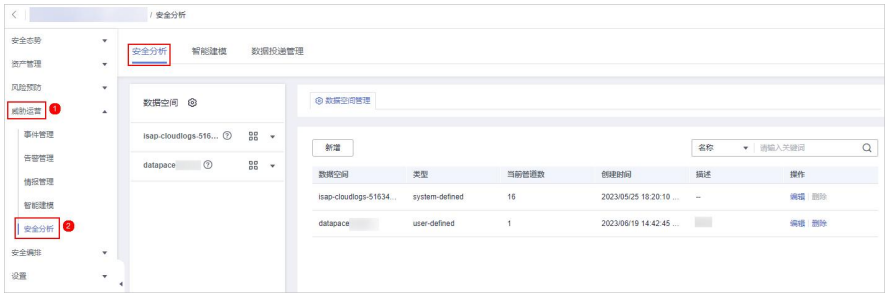
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-126 进入目标工作空间管理页面

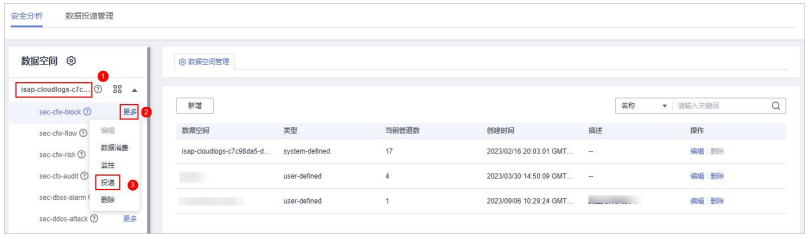
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-127 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道后，单击目标管道名称后的“更多 > 投递”，右侧弹出现在数据投递设置页面。

图 11-128 进入投递设置页面



步骤 6 （可选）首次投递到目的投递类型需要进行授权，如果已经授权，请跳过该步骤。

在弹出的授权提示中，确认无误后，单击“确认”，完成授权。

步骤 7 在新增投递配置页面中，配置数据投递相关参数。

1. 配置基本信息。

表 11-37 基本信息

参数名称	参数说明
投递名称	自定义投递规则的名称。
投递资源消耗	默认生成，**无需配置**。

2. 配置数据源。

数据源配置中，显示当前管道数据的详细信息，**无需配置**。

表 11-38 数据源参数说明

参数名称	参数说明
投递类型	数据投递类型，默认显示为 PIPE。

参数名称	参数说明
区域	当前管道所在区域。
工作空间	当前管道所属的工作空间。
数据空间	当前管道所属的数据空间。
管道	管道的名称
数据位置策略	当前管道中数据位置的策略。
读取身份	数据源读取身份信息说明。

3. 配置数据目的，请根据投递目的进行配置。
   - PIPE：将当前管道数据投递到本账号其他管道或其他账号的管道中，请根据您的需要进行选择配置。
     - 本账号投递：将当前管道数据投递到本账号的其他管道中，参数配置说明如表 11-62 所示。

表 11-39 配置数据目的-本账号 PIPE

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型，此处选择“本账号”。
投递类型	选择投递类型，此处选择 PIPE。
工作空间	选择目的 PIPE 所在工作空间。
数据空间	选择目的 PIPE 所在数据空间。
管道	选择目的 PIPE 所在管道。
写入身份	默认生成，无需配置。

     - 跨账号投递：将当前管道数据投递到其他账号的管道中，参数配置说明如表 11-63 所示。

表 11-40 配置数据目的-跨账号 PIPE

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型，此处选择“跨账号”。
投递类型	选择投递类型，此处选择 PIPE。
账号 ID	输入目的 PIPE 所在账号的 ID。
工作空间 ID	输入目的 PIPE 所在工作空间的 ID，查询方法请参见步骤 6。

参数名称	参数说明
数据空间 ID	输入目的 PIPE 所在数据空间的 ID，查询方法请参见步骤 6。
管道 ID	输入目的 PIPE 所在管道的 ID，查询方法请参见步骤 6。
写入身份	默认生成，无需配置。

- LTS：将当前管道数据投递到 LTS 服务，参数配置说明如表 11-64 所示。
  投递到 LTS 中，需要已有可用的日志组和日志流。

表 11-41 配置数据目的-LTS

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型。投递到 LTS 服务仅支持选择“本账号”类型。
投递类型	选择投递类型，此处选择 LTS。
日志组	选择目的 LTS 日志组。
日志流	选择目的 LTS 日志流
写入身份	默认生成，无需配置。

- OBS：将当前管道数据投递到 OBS 服务，参数配置说明如表 11-65 所示。
  投递到 OBS 中，需要已有一个**桶策略**为**公共读写**的可用的桶。

表 11-42 配置数据目的-OBS

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型。投递到 OBS 服务仅支持选择“本账号”类型。
投递类型	选择投递类型，此处选择 OBS。
桶名称	选择目的 OBS 桶名称。
写入身份	默认生成，无需配置。

4. 在“访问授权”中，查看步骤 6 中授予的权限。
   投递请求需要获取访问您云资源的读写权限，授权后，投递任务才能拥有对您云资源相应的访问权限。

步骤 8 单击“确定”。

----结束

后续处理

数据投递新增后，需进行投递权限授予操作，接受授权后，投递才会生效，详细操作请参见 11.7.2 数据投递授权。

11.7.2 数据投递授权

操作场景

数据投递新增后，需进行投递权限授予操作，接受授权后，投递才会生效。

本章节介绍如何执行数据投递投递授权。

前提条件

已新增数据投递。

约束与限制

如果新增的数据投递为跨账号投递，则需要登录目的账号进行授权操作。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-129 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

步骤 5 在数据投递管理页面，选择“跨租投递权限授予”页签，进入跨租投递权限授权页面后，单击目标投递任务所在行“操作”列的“接受”。

如需批量接受授权，可以勾选所有需要授权的任务，然后单击列表左上角的“接受”。

图 11-130 数据投递授权

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况，详细操作请参见 11.7.3 查看数据投递情况。

----结束

相关操作

在跨租投递权限授权页面可以的投递权限进行**拒绝**和**取消**授权操作：

表 11-43 跨租投递权限管理

操作	具体操作方法
拒绝	在目标投递任务所在行“操作”列，单击“拒绝”。 如需批量拒绝授权，可以勾选所有需要拒绝的任务，然后单击列表左上角的“拒绝”。
取消	1. 在目标投递任务所在行“操作”列，单击“取消”。 如需批量取消授权，可以勾选所有需要取消的任务，然后单击列表左上角的“取消”。 2. 在弹出的确认框中，单击“确定”。

11.7.3 查看数据投递情况

操作场景

数据投递成功后，可以到投递目的地查看数据投递情况。请根据您的投递目的地选择对应操作：

- 投递到其他数据管道
- 投递到 OBS 桶
- 投递到 LTS

前提条件

已完成数据投递操作，具体操作请参见 11.7.1 新增数据投递。

投递到其他数据管道

步骤 1 登录管理控制台。

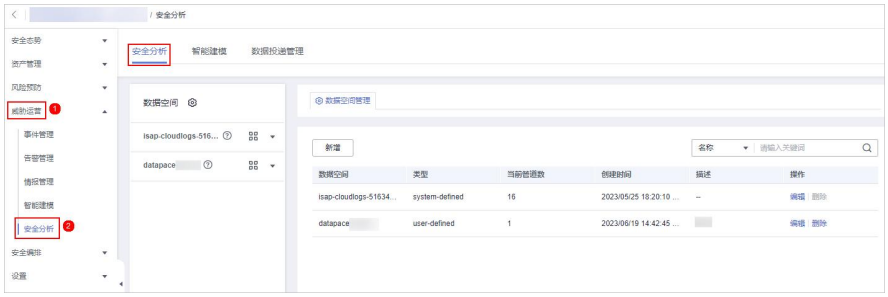
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-131 进入目标工作空间管理页面

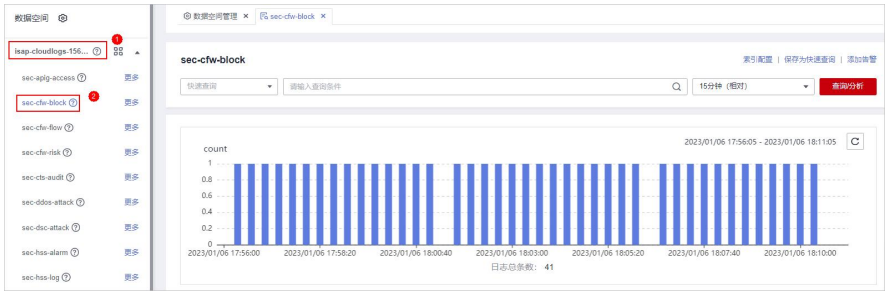
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-132 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 11-133 管道数据页面



步骤 6 在目标管道中，查看投递的日志信息。

----结束

投递到 OBS 桶

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“存储 > 对象存储服务”，默认进入桶列表管理页面。

步骤 3 在桶列表页面中，单击新增数据投递时选择的 OBS 桶的名称，进入目标 OBS 桶详情页面。

步骤 4 在 OBS 桶详情页面，查看投递的日志信息。

----结束

投递到 LTS

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“管理与监管 > 云日志服务”，进入日志管理页面。

步骤 3 在日志管理页面的“日志组列表”栏中，找到新增数据投递是填写的日志组，并单击日志组名称前的 ⌄ 按钮。

步骤 4 展开后，单击新增数据投递时选择的日志流的名称，进入日志流详情页面。

步骤 5 在日志流详情页面，查看投递的日志信息。

----结束

11.7.4 管理数据投递任务

操作场景

本章节介绍管理投递任务，请根据您的需要选择对应操作：

- 查看数据投递任务：查看数据投递任务相关信息。
- 挂起投递任务：数据投递成功后，如需停止投递，可挂起目标投递任务。
- 启动投递任务：数据投递任务停止投递后，如需重启投递，可启动目标投递任务。
- 删除投递任务：如果不在需要某个投递任务，可删除投递任务。

前提条件

已新增数据投递。

查看数据投递任务

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-134 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

图 11-135 进入数据投递管理页面

步骤 5 在投递任务列表页面中，查看已有投递任务。

表 11-44 投递任务

参数名称	参数说明
名称/ID	投递任务名称/ID。
数据源	投递任务的数据源所在管道。
消费策略	投递任务的消费策略。
目的类型	数据投递目的地所属的类型。
投递目的信息	数据投递目的地相关信息。
监控	数据投递监控情况。可单击监控图标，查看数据消费情况。
状态	投递任务的状态。
创建时间	投递任务创建时间。
操作	可对数据投递任务进行挂起、删除等操作。

----结束

挂起投递任务

数据投递新增并授权成功后，投递任务状态自动更新为投递中，如需停止投递，可挂起目标投递任务。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-136 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

图 11-137 进入数据投递管理页面

步骤 5 在数据投递管理页面，单击目标投递任务所在行“操作”列的“挂起”。

挂起后，投递任务状态更新为“挂起”，则表示挂起投递任务成功。

----结束

启动投递任务

数据投递任务停止投递后，如需重启投递，可启动目标投递任务。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-138 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

图 11-139 进入数据投递管理页面

步骤 5 在数据投递管理页面，单击目标投递任务所在行“操作”列的“启动”。

启动后，投递任务状态更新为“投递中”，则表示启动投递任务成功。

----结束

删除投递任务

如果不再需要某个数据投递任务，可执行删除操作。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-140 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面后，选择“数据投递管理”页签，进入数据投递管理页面。

图 11-141 进入数据投递管理页面

步骤 5 在数据投递管理页面，单击目标投递任务所在行“操作”列的“删除”，并在弹出的确认框红中单击“确定”。

----结束

11.7.5 投递日志数据至 LTS

操作场景

态势感知（专业版）支持集成 WAF、HSS、CFW 等其他云产品日志，具体集成操作及支持集成的云服务请参见 13.2 数据集成。

集成后的日志还支持投递至云日志服务（Log Tank Service，简称 LTS），方便用户快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

本章节将介绍如何将集成的日志数据投递至 LTS。

前提条件

- 已完成需投递日志的数据集成至态势感知（专业版）操作，详细操作请参见 13.2 数据集成。
- 投递到 LTS 中，需要已有可用的日志组和日志流。

操作步骤

新增数据投递

步骤 1 登录管理控制台。

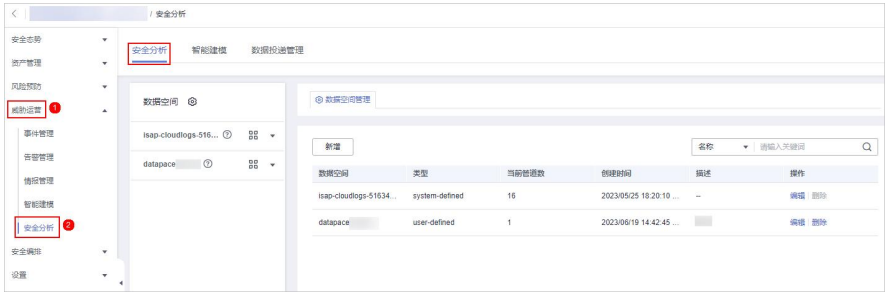
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-142 进入目标工作空间管理页面

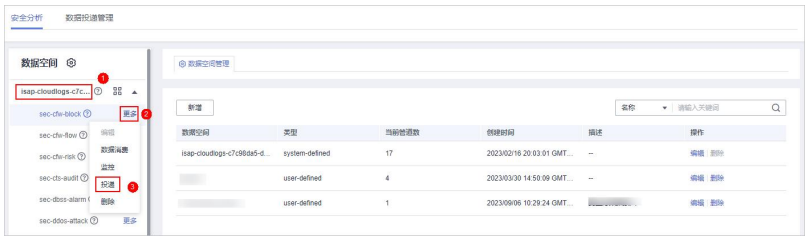
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-143 进入安全分析页面



步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道后，单击目标管道名称后的“更多 > 投递”，右侧弹出现在数据投递设置页面。

图 11-144 进入投递设置页面



步骤 6 （可选）首次投递到目的投递类型需要进行授权，如果已经授权，请跳过该步骤。

在弹出的授权提示中，确认无误后，单击“确认”，完成授权。

步骤 7 在新增投递配置页面中，配置数据投递相关参数。

- 投递名称：自定义数据投递名称。

- 账号类型：此处请选择“本账号”。投递到 LTS 服务仅支持投递本账号内的日志数据。
- 投递类型：此处请选择“LTS”。
- 日志组：选择 LTS 日志组。
- 日志流：选择目的 LTS 日志流。

其他配置参数，系统默认生成，无需配置。

步骤 8 单击“确定”。

数据投递授权

步骤 9 在数据投递管理页面，选择“跨租投递权限授予”页签，进入跨租投递权限授权页面后，单击目标投递任务所在行“操作”列的“接受”。

如需批量接受授权，可以勾选所有需要授权的任务，然后单击列表左上角的“接受”。

图 11-145 数据投递授权

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况。

查看数据投递情况

步骤 10 单击页面左上方的 ☰，选择“管理与监管 > 云日志服务”，进入日志管理页面。

步骤 11 在日志管理页面的“日志组列表”栏中，找到新增数据投递是填写的日志组，并单击日志组名称前的 ⌄ 按钮。

步骤 12 展开后，单击新增数据投递时选择的日志流的名称，进入日志流详情页面。

步骤 13 在日志流详情页面，查看投递的日志信息。

----结束

11.8 数据监控

态势感知（专业版）数据监控功能支持监控态势感知（专业版）管道上下游的生产速率、生产量、消费总速率等指标，您可以根据监控判断业务运行状态。

相关概念

- 生产者：是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。
- 订阅器：用于订阅态势感知（专业版）管道消息，一个管道可由多个订阅器进行订阅，态势感知（专业版）通过订阅器进行消息分发。
- 消费者：是用来接收并处理数据的运行实体，负责通过订阅器把态势感知（专业版）管道中的消息进行消费并处理。
- 消息队列：是数据存储和传输的实际容器。

查看监控指标

步骤 1 登录管理控制台。

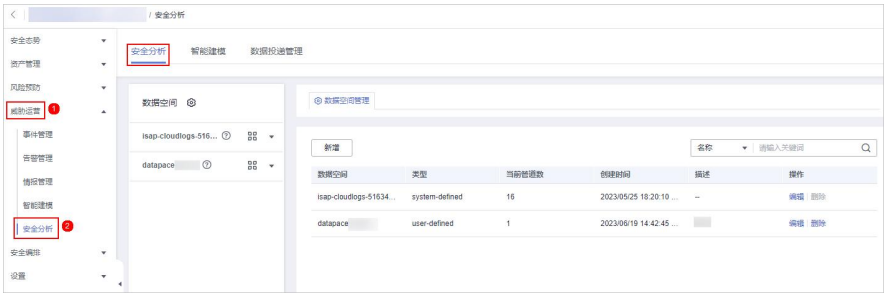
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-146 进入目标工作空间管理页面

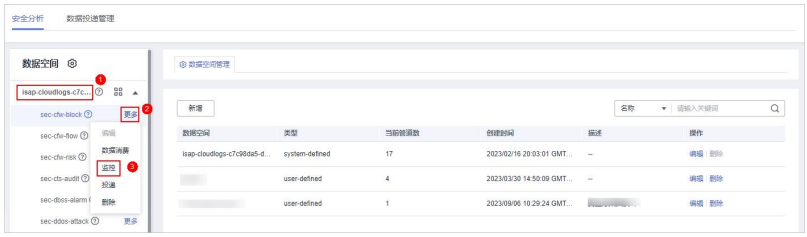
步骤 4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 11-147 进入安全分析页面



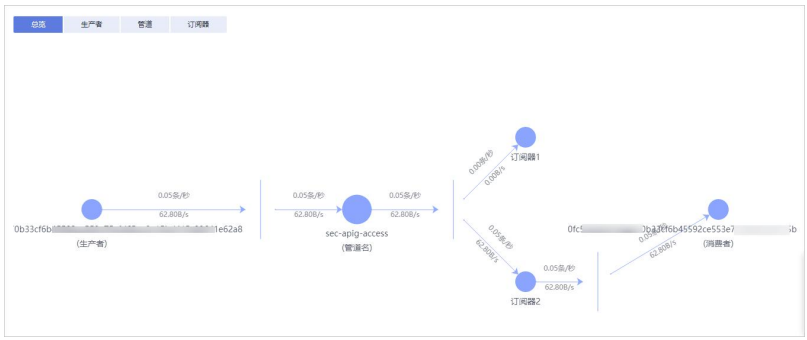
步骤 5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，单击目标管道名称后的“更多 > 监控”，进入管道监控页面。

图 11-148 进入数据监控页面



步骤 6 在数据管道的监控页面，查看监控指标。

图 11-149 数据监控



- 总览：显示当前管道中生产者、管道、订阅器、消费者之间生产速率等信息。
- 生产者：显示生产者的“当前生产 TPS”、“当前生产速率”、“当前生产量”、“当前消息存储大小”等相关指标信息。
- 管道：显示当前管道指定时间（近 2/6/12/24 小时、近 7 天或自定义）内的“管道存储的消息大小(MB)”、“生产到管道的消息大小(MB)”、“生产到管道的消息数量(条)”、“从管道消费的消息大小(MB)”、“从管道消费的消息数量(条)”、“未确认的消息大小(MB)”、“管道的生产速率(条/秒)”、“管道的消费速率(条/秒)”、“每条消息大小平均值(KB)”、“未卸载的消息大小(B)”等相关指标信息。
- 订阅器：显示当前订阅器指定时间（近 2/6/12/24 小时、近 7 天或自定义）内的“订阅器消费总速率(条/秒)”、“订阅器消费的数据大小(B)”、“订阅器消费的数据数量(条)”、和“活跃消费者”等相关指标信息。

----结束

12 安全编排

12.1 安全编排概述

安全编排（Security Orchestration）是将企业和组织在安全运营过程中涉及的不同系统或者一个系统内部不同组件的安全功能按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。旨在帮助企业和组织的安全团队快速并高效地响应网络威胁，实现安全事件的高效、自动化响应处置。

安全编排的主要功能如下：

- 剧本管理：内置自动响应的剧本，支持按需定义扩展。
- 流程管理：绘制流程图响应剧本触发。
- 实例管理：支持对运行的实例进行监控管理及记录查看。
- 安全事件自动化响应：对需要处理的安全事件以及可疑事件，通过安全编排实现自动化处置及事件调查。

相关概念

- 剧本

  剧本是安全运营流程在安全编排系统中的形式化表述，通常是在编排器中的工作流引擎驱动下执行。

  编写剧本的过程就是将安全运营流程和规程转换为剧本，并在剧本中将各种应用编排到一起的过程，也是将人读安全运营流程转换为机读工作流的过程。

- 流程

  流程是将安全运营相关的工具/技术、流程和人员等各种能力整合到一起的一种协同工作方式。流程是剧本触发时响应的方式。

  它是将系统内部不同组件的安全功能通过可编程接口（API）封装后形成的安全能力（即应用）和人工检查点按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。

12.2 内置剧本、流程和资产连接

安全编排根据需求内置了剧本、流程和资产连接，可以根据需要直接进行使用。

内置剧本

表 12-1 内置剧本

安全防线	剧本名	描述	数据类
主机安全	主机告警状态同步	自动同步主机告警状态	Alert
	高危漏洞自动通知	对威胁等级为 High 的漏洞进行邮件或者短信通知	Vulnerability
	攻击链路分析告警通知	针对攻击链路进行分析，如果主机产生告警，就会查看关联主机所属的网站，如果有对应网站信息且有告警，就进行告警通知	Alert
应用安全	WAF 攻击自动化安全封堵	将告警里的源 IP 研判后封堵在 WAF 中	Alert
其他/通用	高危告警自动通知	对威胁级别为 High 或者 Fatal 的告警进行邮件或者短信通知	Alert
	告警指标提取	将告警中 IP 信息抽取，通过情报系统进行验证，若为恶意 IP，可以将 IP 信息设置成指标，并与源告警相互关联	Alert
	重复告警自动关闭	将近 7 日内第二次及第二次以上出现的告警状态置为关闭，并关联 7 日内同名告警	Alert
	自动更新告警名称	根据客户需要，筛选关键字段信息，拼接告警名称	Alert
	告警 ip 指标打标	告警添加告警关联攻击源 IP 及目标 IP 的标签信息	Alert

内置流程

表 12-2 内置流程

安全防线	流程名称	描述	数据类
主机安全	主机告警状态同步	自动同步主机告警状态	Alert
	高危漏洞自动通知	对威胁等级为 High 的漏洞进行邮件或者短信通知	Vulnerability
	漏洞处理	调用主机安全接口修复主机漏洞	Vulnerability

安全防线	流程名称	描述	数据类
	策略管理-安全组阻断	将目标 IP 添加到所有安全组中	Policy
	策略管理-安全组取消阻断	将目标 IP 从所有安全组中取消	Policy
	主机一键隔离	将目标主机进行全端口的隔离	Alert
	主机一键解封	将目标主机从隔离安全组中移除	Alert
	攻击链路分析告警通知	针对攻击链路分析，主机告警影响资产关联网站资产有对应攻击告警进行告警通知	Alert
应用安全	WAF 一键拦截	对目标 IP 封堵在该账号的 WAF 服务里的所有中策略	Alert
	WAF 一键解封	对目标 IP 从该账号的 WAF 服务里的目标策略组中解封	Alert
	WAF 攻击自动化安全封堵	将告警里的源 IP 研判后封堵在 WAF 中	Alert
	策略管理-WAF 阻断	将目标 IP 添加到 WAF 的黑名单中	Policy
	策略管理-WAF 取消阻断	将目标 IP 从 WAF 的黑名单中移除	Policy
网络安全	CFW 一键拦截	将目标 IP 添加到 CFW 的黑名单中	Alert
	CFW 一键解封	将目标 IP 从 CFW 的黑名单中移除	Alert
	策略管理-CFW 阻断	将目标 IP 添加到 CFW 的黑名单中	Policy
	策略管理-CFW 取消阻断	将目标 IP 从 CFW 的黑名单中移除	Policy
其他/通用	高危告警自动通知	对威胁级别为 High 或者 Fatal 的告警进行邮件或者短信通知	Alert
	告警指标提取	将告警中 ip 信息抽取，进行微步外部验证，置成指标，并与源告警相互关联	Alert
	重复告警自动关闭	7 日内第二次及第二次以上出现的告警状态置为关闭，并关联 7 日内同名告警	Alert
	自动更新告警名称	根据客户需要，筛选关键字段信息，拼接告警名称	Alert
	告警打 ip 标签	告警添加告警关联攻击源 IP 及目标 IP 的标签信息	Alert

安全防线	流程名称	描述	数据类
	一键解封	根据不同的告警数据源产品选择执行不同的解封子流程	Alert
	一键阻断	根据不同的告警数据源产品选择执行不同的阻断子流程	Alert
	态势感知（专业版）报告通知	态势感知（专业版）日报按钮或定时发送订阅人员	CommonContext

内置资产连接

表 12-3 内置资产连接

连接名称	插件	连接方式
CFW 云服务认证凭据	HTTP	云服务委托
CFW 认证资产	CFW	云服务委托
DBSS 云服务认证凭据	DBSS	云服务委托
ECS 云服务认证凭据	ECS	云服务委托
EIP 云服务认证凭据	EIP	云服务委托
EPS 云服务认证凭据	HTTP	用户名及密码
HSS 云服务认证凭据	HSS	云服务委托
IAM 云服务认证凭据	IAM	云服务委托
OBS 云服务认证凭据	OBS	AK&SK
RDS 云服务认证凭据	RDS	云服务委托
SecMaster 云服务认证凭据	HTTP	云服务委托
SecMaster 布局信息凭据	HTTP	云服务委托
SMN 云服务认证凭据	SMN	云服务委托
VPC 云服务认证	VPC	云服务委托
WAF 云服务认证凭据	HTTP	云服务委托
WAF 认证资产	WAF	云服务委托
告警处理业务方法集	SecMasterBiz	--
微步认证凭据	ThreatBook	其他

连接名称	插件	连接方式
通用工具方法集	SecMasterUtilities	--
通知 SMN 处理人员凭证	HTTP	云服务委托
通知 SMN 运营人员凭证	HTTP	云服务委托

12.3 安全编排使用流程

安全编排的使用流程如下：

图 12-2 安全编排使用流程

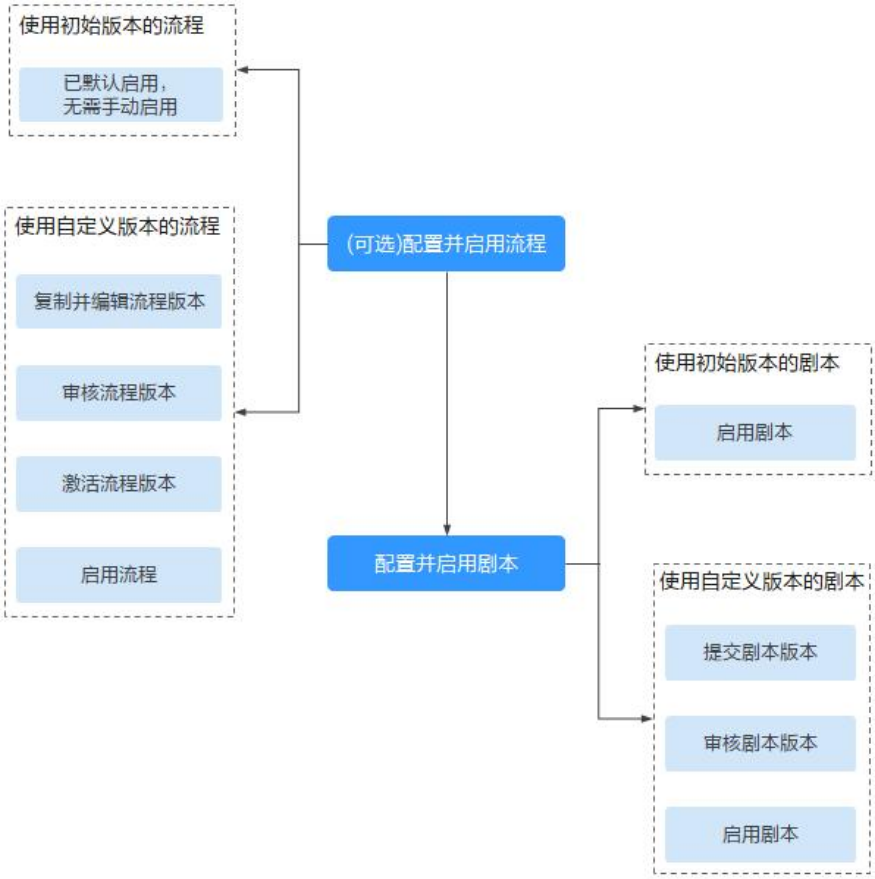


表 12-4 使用流程

序号	操作项	说明

序号	操作项	说明
1	（可选）12.4 （可选）配置并启用流程	启用需要的态势感知（专业版）内置的流程。 态势感知（专业版）默认提供了“WAF 一键解封”、“主机告警状态同步”、“告警指标提取”等流程，且流程的初始版本（V1）也已启用，无需手动启用。 同时，如果需要对某个流程进行编辑，可以复制初始版本进行处理。
2	12.5 配置并启用剧本	启用需要的态势感知（专业版）内置的剧本。 态势感知（专业版）默认提供了“告警指标提取”、“主机告警状态同步”、“重复告警自动关闭”等剧本，且剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。 同时，如果需要对某个剧本进行编辑，可以复制初始版本进行处理。

12.4（可选）配置并启用流程

操作场景

态势感知（专业版）默认提供了“WAF 一键解封”、“主机告警状态同步”、“告警指标提取”等流程，且流程的初始版本（V1）也已启用，无需手动启用。

同时，还支持对已有流程进行自定义编辑，使用自定义流程。本章节将介绍如何配置并启用自定义版本的流程。

启用自定义版本的流程

进入流程管理页面

步骤 1 登录管理控制台。

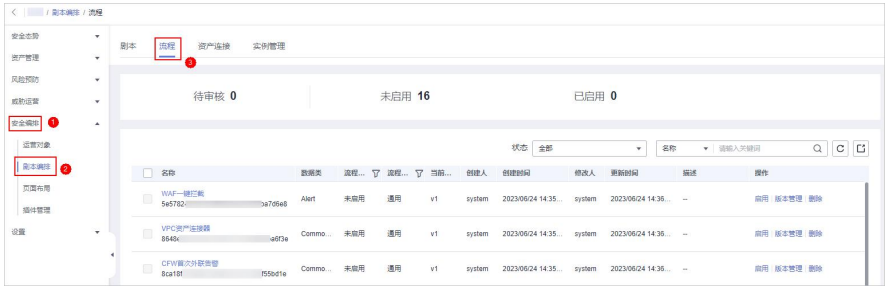
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-3 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

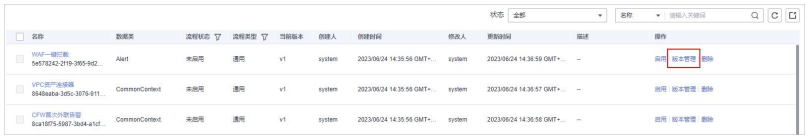
图 12-4 流程管理页面



复制流程版本

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-5 进入流程版本管理页面



步骤 6 在**流程版本管理**页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“复制”，弹出确认框。

步骤 7 在弹出的确认框中，单击“确认”。

编辑并提交流程版本

步骤 8 在**流程版本管理**页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤 9 在流程图绘制页面中，从左侧资源库（提供基础节点、流程节点、插件节点）拖拽节点到右边画布，进行设计。

表 12-5 资源库参数详情

参数名称	参数说明

参数名称			参数说明
基础	基础节点	开始节点	一个流程的开始。每个流程仅允许一个开始节点，整个流程从开始节点启动执行。
		结束节点	一个流程的结束。每个流程存在多个结束节点，但是流程必须以结束节点收尾，即结束节点不允许出现在其他节点执行之前。
		人工审核	流程执行到该节点会暂停，此时在 8.3.1 查看待办任务页面产生一条待办任务。 用户在我的待办页面处理完成后，继续执行后续节点。 人工审核节点参数说明如表 12-6 所示。
		子流程	另起一个流程，主要用于执行循环操作。相当于流程中的循环体。
	系统插件	排他网关	线路分流时，根据条件表达式选择多条线路中的一条执行。 线路汇聚时，多条线路只要有一条线路到达则继续后面的节点执行。
		并行网关	线路分流时，所有线路都会执行。 线路汇聚时，多条线路全部到达，才会继续后续节点的执行(若有一条失败，则整个流程都会失败)
		包容网关	线路分流时，根据条件表达式选择符合条件的所有表达式执行。 线路汇聚时，所有分流时被执行的线路都到达包容网关时，才会继续后续节点执行(若有一条失败，则整个流程都会失败)
流程节点			可以选择当前工作空间中已经发布的所有流程。
插件节点			可以选择当前工作空间中所有插件。

表 12-6 人工审核节点参数说明

参数名称	参数说明
主键 ID	系统自动生成主键 ID，可根据需要进行修改。
名称	自定义人工审核节点名称。
到期时间	人工审核节点到期时间。
描述	自定义人工审核节点的描述信息。

参数名称	参数说明
查看参数	单击 »，并在弹出的选择上下文页面中，选择已有的参数名称。如需新增，可单击“新增参数”进行添加。
人工处理参数	输入参数 Key。如需新增，可单击“新增参数”进行添加。
处理人	设置此流程的审核处理人为当前账号中的 IAM 用户。设置后如有流程需审批，仅设置的责任人可在 8.3.1 查看待办任务页面进行处理，非责任人仅支持查看。 **说明** 首次使用，需要授权。具体操作如下： 1. 单击“现在授权”，右侧弹出访问授权页面。 2. 在访问授权页面中，勾选“同意授权”，并单击“确认”。

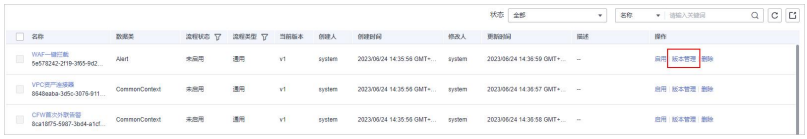
步骤 10 设计完成后，单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

如果流程校验失败，请根据失败提示进行检查。

审核流程版本

步骤 11 编辑并提交流程版本后，页面返回流程管理页面。在**流程管理**页面中，单击目标流程“操作”列“版本管理”，右侧弹出流程版本管理页面。

图 12-6 进入流程版本管理页面



步骤 12 在**流程版本管理**页面中，单击目标流程所在行的“操作”列的“审核”，弹出审核确认框。

步骤 13 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

激活流程版本

步骤 14 在**流程版本管理**页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“激活”。

步骤 15 在弹出确认框中，单击“确认”。

启用流程

步骤 16 在**流程管理**页面中，单击目标流程所在行的“操作”列的“启用”，页面弹出启用确认框。

步骤 17 在弹出的确认框中，选择启用的流程版本后，单击“确定”。

----结束

12.5 配置并启用剧本

态势感知（专业版）默认提供了“告警指标提取”、“主机告警状态同步”、“重复告警自动关闭”等剧本，且剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

同时，如果需要对某个剧本进行编辑，可以复制初始版本进行处理。

本章节主要介绍配置并启用剧本。

- 启用初始版本的剧本
- 启用自定义版本的剧本

启用初始版本的剧本

步骤 1 登录管理控制台。

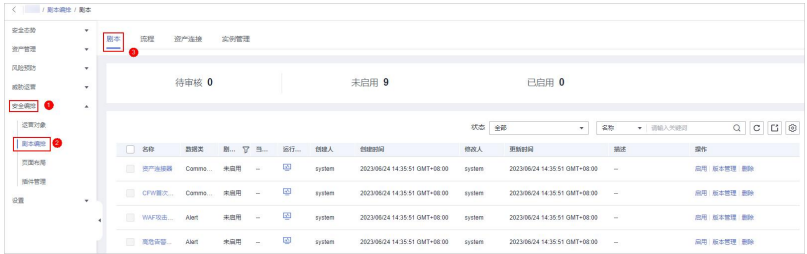
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-7 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-8 进入剧本管理页面



步骤 5 在待启用剧本所在行“操作”列，单击“启用”，弹出启用确认信息框。

步骤 6 选择启用的剧本版本后，单击“确认”。

----结束

启用自定义版本的剧本

进入剧本管理页面

步骤 1 登录管理控制台。

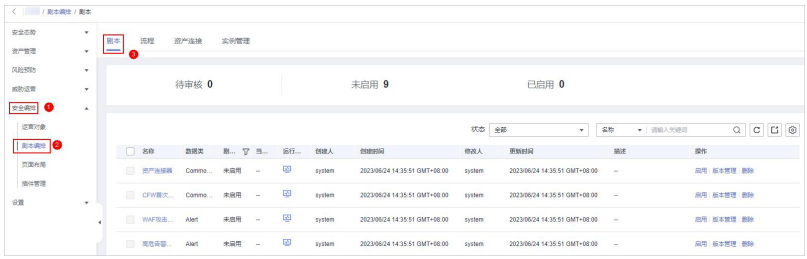
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-9 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-10 进入剧本管理页面



复制剧本版本

步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-11 进入剧本版本管理页面

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“复制”，弹出复制版本页面。

步骤 7 在弹出复制版本信息框中，单击“确认”。

编辑并提交剧本版本

步骤 8 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“编辑”，弹出编辑版本页面。

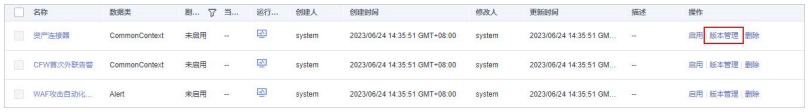
步骤 9 在剧本版本编辑页面，编辑版本信息。

步骤 10 单击“确定”。

审核剧本版本

步骤 11 编辑并提交剧本版本后，页面返回剧本管理页面。在**剧本管理**页面中，单击目标剧本“操作”列“版本管理”，右侧弹出剧本版本管理页面。

图 12-12 进入剧本版本管理页面



步骤 12 在**剧本版本管理**页面中，单击目标剧本版本所在行的“操作”列的“审核”，弹出审核确认框。

步骤 13 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

启用剧本

步骤 14 在**剧本管理**页面中，单击目标剧本所在行的“操作”列的“启用”，页面弹出启用确认框。

步骤 15 在弹出的确认框中，选择启用的剧本版本后，单击“确定”。

----结束

12.6 运营对象管理

12.6.1 数据类

12.6.1.1 查看已有数据类

操作场景

安全编排与响应中的剧本和流程的运行都需要绑定数据类，由数据对象（数据类的实例）触发剧本。

本章节介绍如何查看已有数据类。

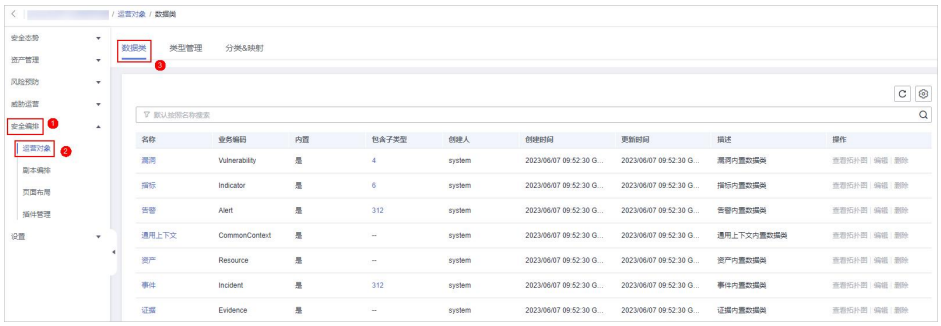
操作步骤

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-13 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，默认进入运营对象的数据类管理页面。

图 12-14 进入数据类管理页面



步骤 3 在数据类列表中，查看已有数据类信息。

当数据类较多时，可以通过搜索功能，选择数据类的“名称”、“业务编码”、“内置”或者“描述”，并在搜索框中输入关键词，单击，即可快速查询指定数据类。

表 12-7 数据类信息

参数名称	参数说明
名称	数据类的名称。
业务编码	数据类的业务编码。
内置	是否为系统内置数据类。
创建人	数据类的创建人信息。
创建时间	数据类的创建时间。
更新时间	数据类的更新时间。
描述	数据类的具体描述信息。
操作	可对数据类进行编辑、删除等操作。

步骤 4 如需查看某个数据类的详细信息，可单击目标数据类的名称，右侧将弹出目标数据类的详情页面。

----结束

12.6.2 类型管理

12.6.2.1 管理告警类型

操作场景

本章节介绍如何管理告警类型，详细操作如下：

- 查看已有告警类型：**查看**已有的告警类型及其详细信息。
- 新增告警类型：介绍如何自定义**新增**告警类型。
- 告警类型关联布局：介绍如何将自定义新增的告警类型**关联已有布局**。
- 编辑已有告警类型：介绍如何**编辑**自定义新增的告警类型。
- 管理已有告警类型：介绍如何**启用**、**禁用**、**删除**自定义新增的告警类型。

约束与限制

- 系统内置告警类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置告警类型默认处于启用状态，且暂**不支持**进行编辑、禁用、删除操作。
- 自定义告警类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

查看已有告警类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-15 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-16 进入类型管理页面

步骤 3 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 4 在告警类型管理页面中，左侧“类型名称”中，可查看所有的告警类型。

如需查看某个告警类型中子类型的详细信息，可在左侧“类型名称”中单击目标类型名称，右侧将展示所有子类型详细信息，参数说明如表 12-8 所示。

如果子类型较多，可通过选择“子类型”、“关联布局”，并输入对应关键字进行搜索。

图 12-17 查看告警类型

表 12-8 查看告警类型参数说明

参数名称	参数说明
子类型/子类型标识	告警子类型的名称和标识。
关联布局	告警类型已关联的布局。
启用状态	告警类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
SLA	告警类型的 SLA 处理时间。
描述	告警类型的描述信息。
操作	可以对告警类型进行编辑、删除等操作。

----结束

新增告警类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-18 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-19 进入类型管理页面

步骤 3 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 4 在告警类型管理页面中单击“新增”，右侧弹出新增告警类型页面。在新增告警类型页面中，配置告警类型参数。

表 12-9 新增告警类型参数说明

参数名称	参数说明
类型名称	自定义新增告警类型的名称。
类型标识	填写告警类型标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
子类型	填写告警类型的子类型。
子类型标识	填写告警子类型标识。标识关键字需遵循大驼峰命名规范，例如 SubTypeName。
启动状态	设置告警类型的启动状态。 •  ：表示启用。 •  ：表示禁用。

参数名称	参数说明
SLA	设置告警的 SLA 处理时间。
描述	自定义告警类型描述信息。

说明

自定义告警类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 5 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在告警类型页面的“类型名称”中查看已新增的告警类型。

----结束

告警类型关联布局

说明

系统内置告警类型已默认关联已有布局，暂不支持自定义关联布局。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-20 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-21 进入类型管理页面

步骤 3 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 4 在告警类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 5 在绑定布局编辑框中，选择需要关联的布局。

步骤 6 单击“确认”。

----结束

编辑已有告警类型

说明

- 暂不支持编辑系统内置告警类型。
- 自定义告警类型新增成功后，不支持修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-22 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-23 进入类型管理页面

步骤 3 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 4 在告警类型管理页面的“类型名称”中，单击需要编辑的自定义告警类型名称，右侧将展示自定义告警类型的详细信息。

步骤 5 在右侧告警列表页面中，单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 6 在编辑告警类型页面中，修改告警类型的参数信息。

表 12-10 编辑告警类型参数说明

参数名称	参数说明
类型名称	告警类型的名称，**不支持修改**。
类型标识	告警类型标识，**不支持修改**。
子类型	填写告警类型的子类型。
子类型标识	告警子类型标识，**不支持修改**。
启动状态	设置告警类型的启动状态。 •  ：表示启用。 •  ：表示禁用。
SLA	设置告警的 SLA 处理时间。
描述	自定义告警类型描述信息。

步骤 7 在页面右下角单击“确认”。

----结束

管理已有告警类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-24 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-25 进入类型管理页面

步骤 3 在类型管理页面，选择“告警类型”页签，进入告警类型管理页面。

步骤 4 在告警类型管理页面中，对告警类型进行管理。

表 12-11 管理已有告警类型

参数名称	参数说明
启用 **说明** 系统内置告警类型默认处于启用状态，无需手动启用。	1. 在告警类型管理页面中，选择需要启用的告警类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的告警类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用 **说明** 暂不支持禁用系统内置告警类型。	1. 在告警类型管理页面中，选择需要禁用的告警类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的告警类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。
删除 **说明** 暂不支持删除系统内置告警类型。	1. 在告警类型管理页面中，选择需要删除的告警类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认界面中，单击“确认”，完成删除操作。

----结束

12.6.2.2 管理事件类型

操作场景

本章节介绍如何管理事件类型，详细操作如下：

- 查看已有事件类型：**查看**已有的事件类型及其详细信息。
- 新增事件类型：介绍如何自定义**新增**事件类型。
- 事件类型关联布局：介绍如何将自定义新增的事件类型**关联已有布局**。
- 编辑已有事件类型：介绍如何**编辑**自定义新增的事件类型。
- 管理已有事件类型：介绍如何**启用**、**禁用**、**删除**自定义新增的事件类型。

约束与限制

- 系统内置事件类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置事件类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义事件类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

查看已有事件类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-26 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-27 进入类型管理页面

步骤 3 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 4 在事件类型管理页面中，查看已有事件类型的详细信息，参数说明如表 12-12 所示。

图 12-28 查看事件类型

表 12-12 事件类型参数说明

参数名称	参数说明
类型名称	事件类型的名称。
子类型/子类型标识	事件子类型的名称和标识。
关联布局	事件类型已关联的布局。
启用状态	事件类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
SLA	事件类型的 SLA 处理时间。
描述	事件类型的描述信息。
操作	可以对事件类型进行编辑、删除等操作。

----结束

新增事件类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-29 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-30 进入类型管理页面

步骤 3 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 4 在事件类型管理页面中单击“新增”，右侧弹出新增事件类型页面。在新增事件类型页面中，配置事件类型参数。

表 12-13 事件类型参数说明

参数名称	参数说明
类型名称	自定义新增事件类型的名称。名称需遵循大驼峰命名规范，例如 TypeName。
类型标识	填写事件类型标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
子类型	填写事件类型的子类型。名称需遵循大驼峰命名规范，例如 SubType。
子类型标识	填写事件子类型标识。标识关键字需遵循大驼峰命名规范，例如 SubTypeName。
启动状态	设置事件类型的启动状态。 •  ：表示启用。 •  ：表示禁用。
SLA	设置事件的 SLA 处理时间。
描述	自定义事件类型描述信息。

说明

自定义事件类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 5 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在事件类型页面的“类型名称”中查看已新增的类型。

----结束

事件类型关联布局

说明

系统内置事件类型已默认关联已有布局，暂不支持自定义关联布局。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-31 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-32 进入类型管理页面

步骤 3 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 4 在事件类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 5 在绑定布局编辑框中，选择需要关联的布局。

步骤 6 单击“确认”。

----结束

编辑已有事件类型

说明

- 暂不支持编辑系统内置事件类型。
- 自定义事件类型新增成功后，不支持修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-33 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-34 进入类型管理页面

步骤 3 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 4 在事件类型管理页面的“类型名称”中，单击需要编辑的自定义事件类型名称，右侧将展示自定义事件类型的详细信息。

步骤 5 在右侧事件类型页面，单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 6 在编辑事件类型页面中，编辑参数信息。

表 12-14 事件类型参数说明

参数名称	参数说明
类型名称	事件类型的名称，**不支持修改**。
类型标识	事件类型标识，**不支持修改**。
子类型	填写事件类型的子类型。
子类型标识	事件子类型标识，**不支持修改**。
启动状态	设置事件类型的启动状态。 •  ：表示启用。 •  ：表示禁用。

参数名称	参数说明
SLA	设置事件的 SLA 处理时间。
描述	自定义事件类型描述信息。

步骤 7 在页面右下角单击“确认”。

----结束

管理已有事件类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-35 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-36 进入类型管理页面

步骤 3 在类型管理页面，选择“事件类型”页签，进入事件类型管理页面。

步骤 4 在事件类型管理页面中，对事件类型进行管理。

表 12-15 管理已有事件类型

参数名称	参数说明

参数名称	参数说明
启用 **说明** 系统内置事件类型默认处于启用状态，无需手动启用。	1. 在事件类型管理页面中，选择需要启用的类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的事件类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用 **说明** 暂不支持禁用系统内置事件类型。	1. 在事件类型管理页面中，选择需要禁用的类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的事件类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。
删除 **说明** 暂不支持删除系统内置事件类型。	1. 在事件类型管理页面中，选择需要删除的类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认界面中，单击“确认”，完成删除操作。

----结束

12.6.2.3 管理威胁情报

操作场景

本章节介绍如何管理威胁情报类型。

- 查看已有威胁情报类型：**查看**已有的威胁情报类型及其详细信息。
- 新增威胁情报类型：介绍如何自定义**新增**威胁情报类型。
- 威胁情报类型关联布局：介绍如何将自定义新增的威胁情报类型**关联已有布局**。
- 编辑已有威胁情报类型：介绍如何**编辑**自定义新增的威胁情报类型。
- 管理已有威胁情报类型：介绍如何**启用**、**禁用**、**删除**自定义新增的威胁情报类型。

约束与限制

- 系统内置威胁情报类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置威胁情报类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义威胁情报类型新增成功后，**不支持**修改类型标识。

查看已有威胁情报类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-37 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-38 进入类型管理页面

步骤 3 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 4 在威胁情报类型管理页面中，查看已有威胁情报的详细信息，参数说明如表 12-16 所示。

图 12-39 查看威胁情报

表 12-16 威胁情报参数说明

参数名称	参数说明
类型名称/类型标识	威胁情报的名称和标识。

参数名称	参数说明
关联布局	威胁情报已关联的布局。
启用状态	威胁情报的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
失效时间	威胁情报的失效时间。
内置	是否为系统内置的威胁情报。
描述	威胁情报的描述信息。
操作	可以对威胁情报进行编辑、删除等操作。

----结束

新增威胁情报类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-40 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-41 进入类型管理页面

步骤 3 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 4 在威胁情报类型管理页面中单击“新增”，右侧弹出新增类型页面。在新增类型页面中，配置类型参数。

表 12-17 威胁情报参数说明

参数名称	参数说明
类型名称	自定义新增威胁情报的名称。名称需遵循大驼峰命名规范，例如 TypeName。
类型标识	填写威胁情报标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
启动状态	设置威胁情报的启动状态。 •  ：表示启用。 •  ：表示禁用。
失效时间	设置威胁情报的失效时间。 • 永不失效：表示当前情报类型永不失效。 • 时间间隔：设置情报失效的间隔时间。
描述	自定义威胁情报的描述信息。

说明

自定义威胁情报类型新增成功后，**不支持**修改类型标识。

步骤 5 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在威胁情报类型页面的表格中查看已新增的类型。

----结束

威胁情报类型关联布局

说明

系统内置威胁情报类型已默认关联已有布局，暂不支持自定义关联布局。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-42 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-43 进入类型管理页面

步骤 3 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 4 在威胁情报类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 5 在绑定布局编辑框中，选择需要关联的布局。

步骤 6 单击“确认”。

----结束

编辑已有威胁情报类型

说明

- 暂不支持编辑系统内置威胁情报类型。
- 自定义威胁情报类型新增成功后，不支持修改类型名称。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-44 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-45 进入类型管理页面

步骤 3 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 4 在威胁情报类型管理页面中，选择需要编辑的类型，并单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 5 在编辑页面中，编辑对应类型的参数信息。

表 12-18 威胁情报参数说明

参数名称	参数说明
类型名称	自定义威胁情报的名称。
类型标识	威胁情报标识，**不支持修改**。
启动状态	设置威胁情报的启动状态。 •  ：表示启用。 •  ：表示禁用。
失效时间	设置威胁情报的失效时间。 • 永不失效：表示当前情报类型永不失效。 • 时间间隔：设置情报失效的间隔时间。
描述	自定义威胁情报的描述信息。

步骤 6 在页面右下角单击“确认”。

----结束

管理已有威胁情报类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-46 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-47 进入类型管理页面

步骤 3 在类型管理页面，选择“威胁情报”页签，进入威胁情报类型管理页面。

步骤 4 在威胁情报类型管理页面中，对威胁情报类型进行管理。

表 12-19 管理已有威胁情报类型

参数名称	参数说明
启用 **说明** 系统内置威胁情报类型默认处于启用状态，无需手动启用。	1. 在威胁情报类型管理页面中，选择需要启用的类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的情报类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。
禁用 **说明** 暂不支持禁用系统内置威胁情报类型。	1. 在威胁情报类型管理页面中，选择需要禁用的类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的情报类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。

参数名称	参数说明
删除 说明 暂不支持删除系统内置威胁情报类型。	1. 在威胁情报类型管理页面中，选择需要删除的类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认界面中，单击“确认”，完成删除操作。

----结束

12.6.2.4 管理漏洞类型

操作场景

本章节介绍如何管理漏洞类型，详细操作如下：

- 查看已有漏洞类型：**查看**已有的漏洞类型及其详细信息。
- 新增漏洞类型：介绍如何自定义**新增**漏洞类型。
- 漏洞类型关联布局：介绍如何将自定义新增的漏洞类型**关联已有布局**。
- 编辑已有漏洞类型：介绍如何**编辑**自定义新增的漏洞类型。
- 管理已有漏洞类型：介绍如何**启用**、**禁用**、**删除**自定义新增的漏洞类型。

约束与限制

- 系统内置漏洞类型暂**不支持**自定义关联布局。
- 系统内置漏洞类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义漏洞类型新增成功后，**不支持**修改类型标识。

查看已有漏洞类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-48 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-49 进入类型管理页面

步骤 3 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 4 在漏洞类型管理页面中，查看已有漏洞类型的详细信息，参数说明如表 12-20 所示。

图 12-50 查看漏洞类型

表 12-20 漏洞类型参数说明

参数名称	参数说明
类型名称/类型标识	漏洞类型的名称和标识。
关联布局	漏洞类型已关联的布局。
启用状态	漏洞类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
内置	是否为系统内置的漏洞类型。
描述	漏洞类型的描述信息。
操作	可以对漏洞类型进行编辑、删除等操作。

----结束

新增漏洞类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-51 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-52 进入类型管理页面

步骤 3 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 4 在漏洞类型管理页面中单击“新增”，右侧弹出新增类型页面。在新增类型页面中，配置类型参数。

表 12-21 漏洞类型参数说明

参数名称	参数说明
类型名称	自定义新增漏洞类型的名称。名称需遵循大驼峰命名规范，例如 TypeName。
类型标识	填写漏洞类型标识。标识关键字需遵循大驼峰命名规范，例如 TypeTag。
启动状态	设置漏洞类型的启动状态。 •  ：表示启用。 •  ：表示禁用。
描述	自定义漏洞的描述信息。

说明

自定义漏洞类型新增成功后，**不支持**修改“类型标识”。

步骤 5 在页面右下角单击“确认”，完成新增操作。

新增完成后，可以在漏洞类型页面的表格中查看已新增的类型。

----结束

漏洞类型关联布局

说明

系统内置漏洞类型暂不支持自定义关联布局。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-53 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-54 进入类型管理页面

步骤 3 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 4 在漏洞类型管理页面中，选择需要关联布局的类型，并单击目标类型所在行“操作”列的“关联布局”，页面弹出绑定布局编辑框。

步骤 5 在绑定布局编辑框中，选择需要关联的布局。

步骤 6 单击“确认”。

----结束

编辑已有漏洞类型

说明

- 暂不支持编辑系统内置漏洞类型。
- 自定义漏洞类型新增成功后，不支持修改类型标识。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-55 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-56 进入类型管理页面

步骤 3 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 4 在漏洞类型管理页面中，选择需要编辑的类型，并单击目标类型所在行“操作”列的“编辑”，右侧弹出编辑页面。

步骤 5 在编辑页面中，编辑对应类型的参数信息。

表 12-22 漏洞类型参数说明

参数名称	参数说明
类型名称	自定义漏洞类型的名称。
类型标识	漏洞类型标识，**不支持修改**。
启动状态	设置漏洞类型的启动状态。 •  ：表示启用。 •  ：表示禁用。
描述	自定义漏洞的描述信息。

步骤 6 在页面右下角单击“确认”。

----结束

管理已有漏洞类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-57 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-58 进入类型管理页面

步骤 3 在类型管理页面，选择“漏洞类型”页签，进入漏洞类型管理页面。

步骤 4 在漏洞类型管理页面中，对漏洞类型进行管理。

表 12-23 管理已有漏洞类型

参数名称	参数说明
启用 **说明** 系统内置漏洞类型默认处于启用状态，无需手动启用。	1. 在漏洞类型管理页面中，选择需要启用的类型，并单击类型列表左上角“批量启用”。 也可以直接单击需要启用的漏洞类型所在行“启用状态”所在列的禁用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“启用”时，则表示启用成功。

参数名称	参数说明
禁用 **说明** 暂不支持禁用系统内置漏洞类型。	1. 在漏洞类型管理页面中，选择需要禁用的类型，并单击类型列表左上角“批量禁用”。 也可以直接单击需要禁用的漏洞类型所在行“启用状态”所在列的启用按钮。 2. 在弹出的确认框中，单击“确认”。 当系统提示操作成功，且目标类型“启用状态”更新为“禁用”时，则表示禁用成功。
删除 **说明** 暂不支持删除系统内置漏洞类型。	1. 在漏洞类型管理页面中，选择需要删除的类型，并单击目标类型所在行“操作”列的“删除”，右侧弹出删除确认界面。 2. 在弹出的确认界面中，单击“确认”，完成删除操作。

----结束

12.6.2.5 查看自定义类型

操作场景

本章节介绍如何查看自定义类型。

约束与限制

- 系统内置的类型和子类型**不支持**关联布局、编辑、删除、启用和禁用。
- 自定义类型新增成功后，**不支持**修改“数据类”、“类型名称”、“类型标识”。
- 子类型新增成功后，**不支持**修改“数据类”、“类型名称”、“类型标识”、“子类型标识”。

查看已有的自定义类型/子类型

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-59 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“类型管理”页签，进入类型管理页面。

图 12-60 进入类型管理页面

步骤 3 在类型管理页面，选择“自定义类型”页签，进入自定义类型管理页面后，查看已有自定义类型/子类型的详细信息。

- 左侧显示类型列表，展示已有的类型。
- 如需查看某个类型的详细信息，请单击左侧类型列表中类型的名称，右侧将展示类型的详细信息。具体信息如下：
  - 目标类型的基本信息：名称、创建人、创建时间、关联布局。
  - 子类型列表：已有子类型、子类型名称、子类型关联的布局等信息。

----结束

12.6.3 分类&映射

12.6.3.1 查看已有分类映射

操作场景

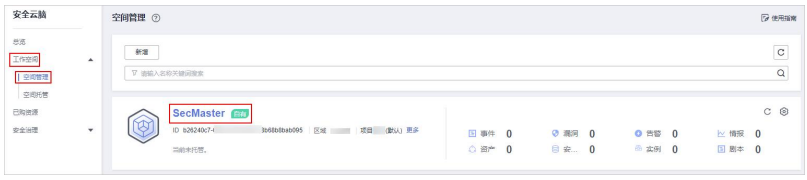
分类和映射是对云服务告警进行类型匹配和字段映射。

本章节介绍如何查看已有分类映射。

操作步骤

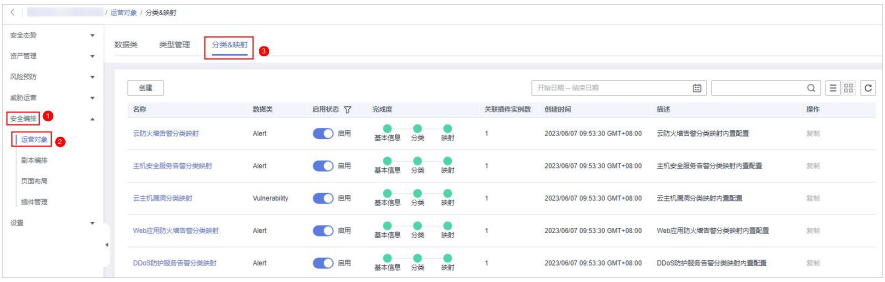
步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-61 进入目标工作空间管理页面



步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

图 12-62 进入分类&映射管理页面



步骤 3 在分类映射管理页面中，查看已创建分类映射的详细信息。

表 12-24 分类映射信息

参数名称	参数说明
名称	分类映射的名称。
数据类	分类映射所属的数据类类型。
启用状态	分类映射的启用状态。 • 启用：当前分类映射已启用。 • 禁用：当前分类映射已被禁用。
完成度	分类映射的完成度。
关联插件实例数	分类映射关联插件实例总数。
创建时间	分类映射的创建时间。
描述	分类映射的描述信息。

步骤 4 如需查看某个分类映射的详细信息，可以单击目标分类映射的名称，进入分类映射详情页面。

----结束

12.6.3.2 创建/复制/编辑分类映射

操作场景

分类和映射是对云服务告警进行类型匹配和字段映射。

本章节介绍如何创建、编辑、复制分类映射。

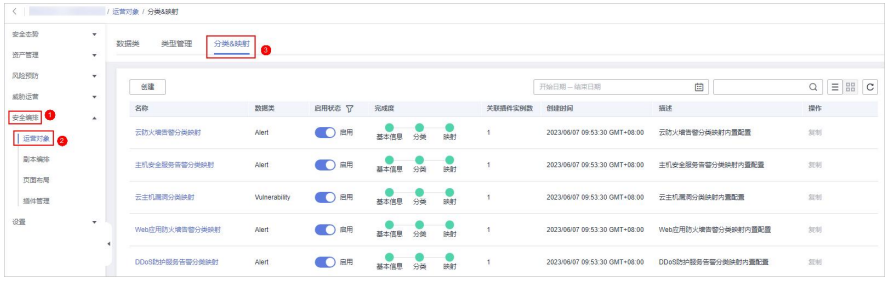
创建分类映射

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-63 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

图 12-64 进入分类&映射管理页面



步骤 3 在分类映射管理页面中，单击“创建”，进入创建分类映射页面。

步骤 4 在创建分类映射页面中，配置分类映射参数信息。

图 12-65 创建分类映射

1. 在左侧“基本信息配置”栏中，配置分类映射的基本信息，参数说明如表 12-25 所示。

表 12-25 配置基本信息

参数名称	参数说明
名称	自定义分类映射名称。

参数名称	参数说明
数据类	选择对应的数据类。
描述	自定义分类映射描述信息。

2. 选择左侧“数据源”栏中，选择分类映射的数据源。

   当“数据源”选择“上传 JSON 文件”时，需要单击“上传 JSON 文件”，并上传 JSON 文件。

3. 在右侧“分类”页签中，选择分类方式，并配置对应参数。
4. 完成分类配置后，单击页面右上角，保存配置。
5. 在右侧“映射”页签中，选择映射方式，并配置对应参数。
6. 完成分类映射后，单击页面右上角，保存配置。
7. 在右侧“预处理”页签中，设置预处理映射参数参数。
8. 完成预处理配置后，单击页面右上角，保存配置。

----结束

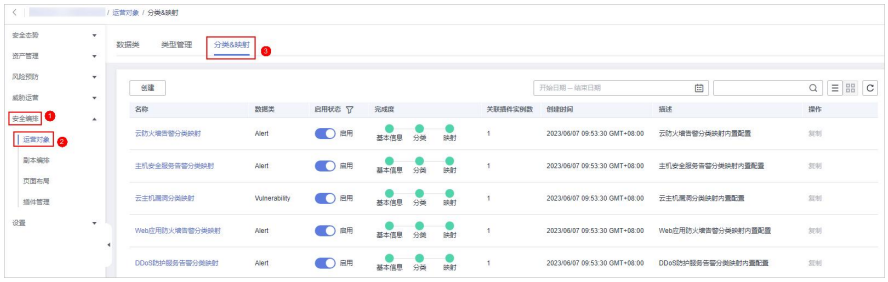
复制已有的分类映射

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-66 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

图 12-67 进入分类&映射管理页面



步骤 3 在分类映射管理页面中，单击目标分类映射所在行“操作”列的“复制”。

步骤 4 在弹出的确认框中，编辑复制项名称，并单击“确认”。

----结束

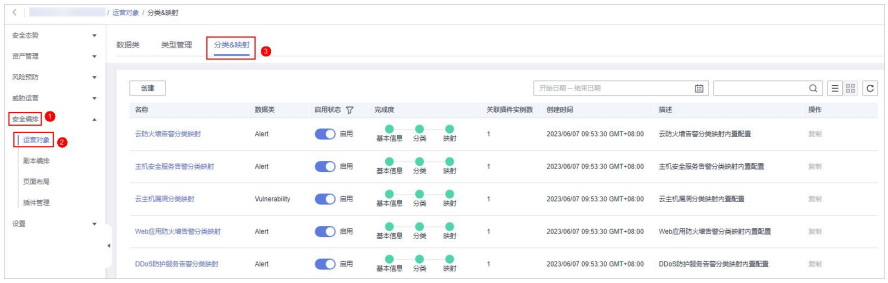
编辑分类映射

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-68 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

图 12-69 进入分类&映射管理页面



步骤 3 在分类映射管理页面中，单击目标分类映射名称，进入编辑页面。

步骤 4 在编辑分类映射页面，编辑分类映射参数信息。

1. 在左侧“基本信息配置”栏中，配置分类映射的基本信息，参数说明如表 12-25 所示。

表 12-26 配置基本信息

参数名称	参数说明
名称	自定义分类映射名称。
数据类	选择对应的数据类，暂不支持编辑
描述	自定义分类映射描述信息。

2. 选择左侧“数据源”栏中，选择分类映射的数据源。
   当“数据源”选择“上传 JSON 文件”时，需要单击“上传 JSON 文件”，并上传 JSON 文件。
3. 在右侧“分类”页签中，选择分类方式，并配置对应参数。
4. 完成分类配置后，单击页面右上角，保存配置。
5. 在右侧“映射”页签中，选择映射方式，并配置对应参数。
6. 完成分类映射后，单击页面右上角，保存配置。
7. 在右侧“预处理”页签中，设置预处理映射参数参数。
8. 完成预处理配置后，单击页面右上角，保存配置。

----结束

12.6.3.3 管理分类映射

操作场景

本章节介绍如何管理分类映射，如启用、禁用、删除操作。

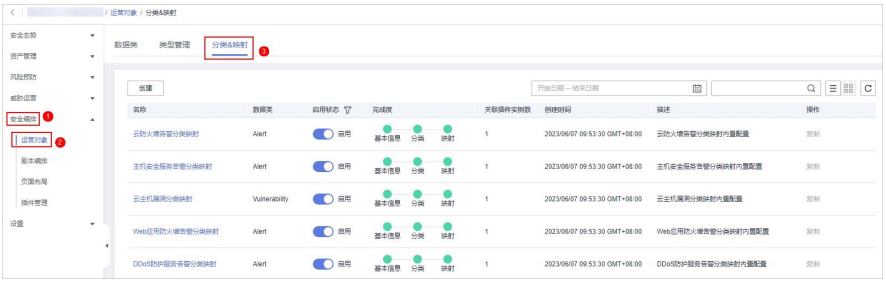
操作步骤

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-70 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 运营对象”，进入运营对象的数据类页面后，选择“分类&映射”页签，进入分类映射管理页面。

图 12-71 进入分类&映射管理页面



步骤 3 在分类映射管理页面中，对分类映射进行管理。

表 12-27 管理分类映射

参数名称	参数说明
启用 说明 自定义新增的分类映射暂不支持启用操作。	在分类映射管理页面中，单击目标分类映射所在行“启用状态”列的禁用按钮。 当“启用状态”更新为“启用”时，表示启用成功。
禁用 说明 自定义新增的分类映射暂不支持禁用操作。	在分类映射管理页面中，单击目标分类映射所在行“启用状态”列的启用按钮。 当“启用状态”更新为“禁用”时，表示禁用成功。
删除 说明 暂不支持删除系统内置分类映射。	1. 在分类映射管理页面中，单击目标分类映射所在行“操作”列的“删除”。 2. 在弹出的删除映射确认页面中，确认无误后，单击“删除”。 说明 ● 删除分类映射时，与待删除分类映射关联的插件、连接等都将立即停止。 ● 分类映射删除后，无法恢复，请谨慎操作。

----结束

12.7 剧本编排管理

12.7.1 剧本

12.7.1.1 提交剧本版本

操作场景

本章节主要介绍如何提交剧本版本。

前提条件

已启用剧本绑定的流程，具体操作请参见 12.7.2.2 启用流程。

操作步骤

步骤 1 登录管理控制台。

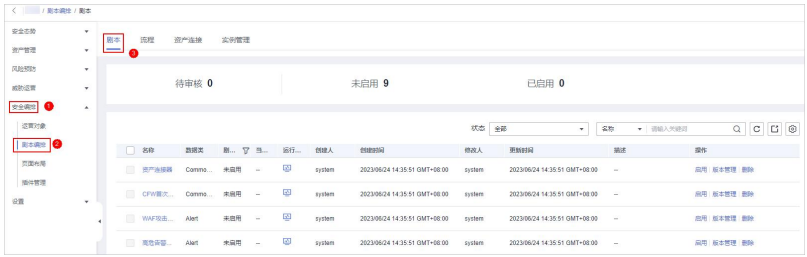
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-72 进入目标工作空间管理页面

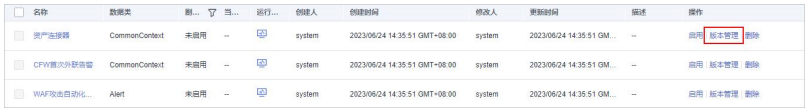
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-73 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-74 进入剧本版本管理页面



步骤 6 在剧本版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“提交”，弹出提交审核确认框。

步骤 7 在确认框中，单击“确认”，提交剧本版本。

说明

- 剧本版本提交后“版本状态”变为“待审核”。
- 剧本版本提交后不可以再编辑，如果需要编辑可以新建版本，或者在审核中驳回提交。

----结束

后续处理

剧本版本提交后，需要进行审核，详细操作请参见 12.7.1.2 审核剧本版本。

12.7.1.2 审核剧本版本

操作场景

本章节主要介绍如何审核剧本版本。

前提条件

已提交剧本，具体操作请参见 12.7.1.1 提交剧本版本。

操作步骤

步骤 1 登录管理控制台。

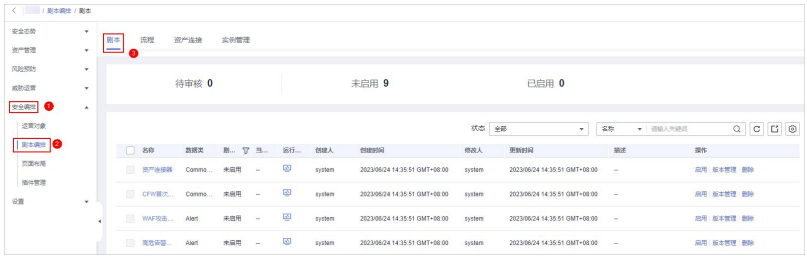
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-75 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-76 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-77 进入剧本版本管理页面

步骤 6 在版本管理页面中，单击“审核”，弹出审核剧本版本页面。

步骤 7 在审核剧本版本页面，填写审核信息，审核剧本版本参数说明如表 12-28 所示。

表 12-28 审核剧本版本参数说明

参数	说明
审核意见	勾选审核结论。 • 通过，通过后剧本版本状态更新为已激活。 • 驳回，驳回后剧本版本状态更新为审核驳回，可再次编辑后提交。
驳回原因	当“审核意见”为“驳回”时，需要填写该参数。 输入审核意见（当审核意见勾选驳回时必填）。

说明

当前剧本仅有一个剧本版本时，审核通过后的剧本“版本状态”默认为“已激活”。

步骤 8 单击“确定”，完成审核剧本版本。

----结束

后续处理

剧本版本审核后，需要启用剧本，详细操作请参见 12.7.1.3 启用剧本。

12.7.1.3 启用剧本

操作场景

完成剧本版本审核后可启用剧本，本章节主要介绍如何启用剧本。

前提条件

已激活剧本版本，具体操作请参见激活/失活剧本版本。

操作步骤

步骤 1 登录管理控制台。

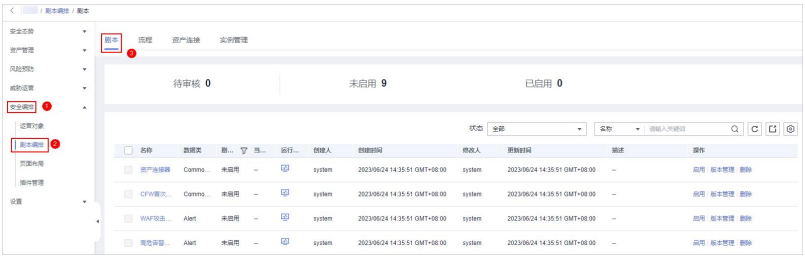
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-78 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-79 进入剧本管理页面



步骤 5 在待启用剧本所在行“操作”列，单击“启用”，弹出启用确认信息框。

步骤 6 选择启用的剧本版本后，单击“确认”，完成剧本启用。

----结束

12.7.1.4 管理剧本

操作场景

本章节将介绍如何执行查看已有剧本、导入剧本信息、导出剧本信息、禁用剧本、删除剧本等操作。

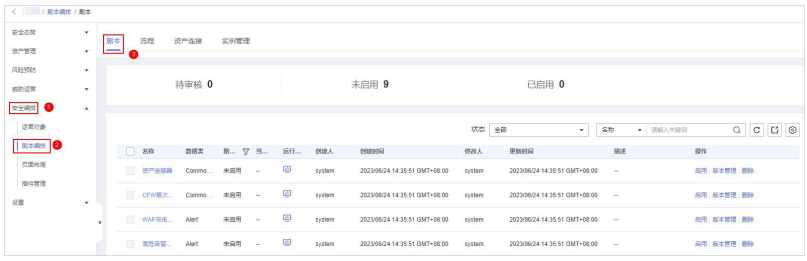
查看已有剧本

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-80 进入目标工作空间管理页面

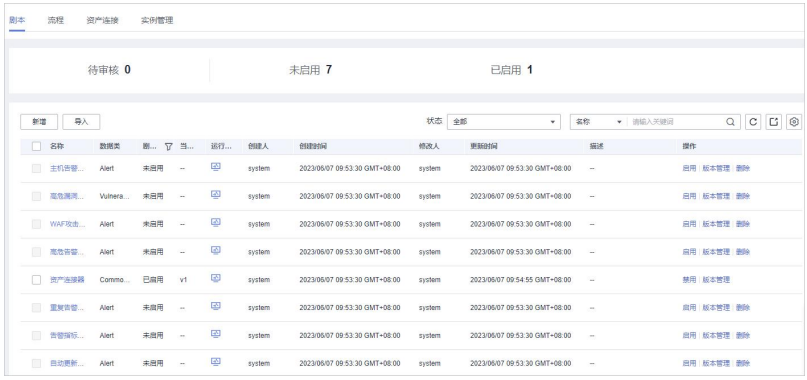
步骤 2 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-81 进入剧本管理页面



步骤 3 在剧本管理页面，查看剧本的信息。

图 12-82 查看剧本信息



- 剧本列表上方，呈现当前**待审核**、**未启用**、**已启用**剧本的总数。
- 在剧本列表中查看已有剧本的信息。

  当剧本较多时，可以通过搜索功能，选择剧本的“状态”、“名称”、“描述”或“数据类”，并在搜索框中输入关键词，单击，即可快速查询指定剧本。

表 12-29 剧本参数说明

参数名称	参数说明
名称	创建的剧本的名称。
数据类	剧本对应的数据类。
剧本状态	剧本当前状态。当前分为已启用和未启用两种状态。
当前版本	剧本当前版本。
运行监控	单击，查看剧本运行监控。 • 选择时间：选择查看的监控时间。支持最近 24 小时、最近 3 天、最近 30 天和最近 90 天的查询。 • 版本：选择查看的监控版本。支持全部、当前有效和已删除类型的查询。 • 运行次数：提供查看剧本的运行总次数、定时触发次数和事件触发次数。 • 平均运行时长：提供查看平均运行时长、最长运行时长和最短运行时长。其中，平均运行时长=实例运行总时长/实例总个数。 • 实例状态统计：提供查看实例运行总个数、运行成功个数、运行中的实例个数、运行失败个数和终止个数。
创建人	创建该剧本的用户。
创建时间	剧本的创建时间。
修改人	最近一次修改该剧本的用户。
更新时间	剧本最近一次更新的时间。
描述	剧本的描述信息。
操作	用户可以在操作栏中，执行启用、删除等操作。

步骤 4 如需查看某个剧本的详细信息，可单击待查看剧本的名称，进入剧本详情页面。

----结束

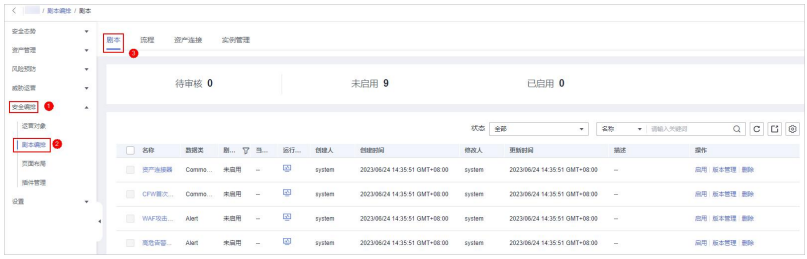
导入剧本信息

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-83 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-84 进入剧本管理页面



步骤 3 在剧本管理列表右上角单击“导入”，弹出导入剧本窗口。

步骤 4 单击“添加文件”，并选择待导入文件。

步骤 5 单击“上传”。

----结束

导出剧本信息

说明

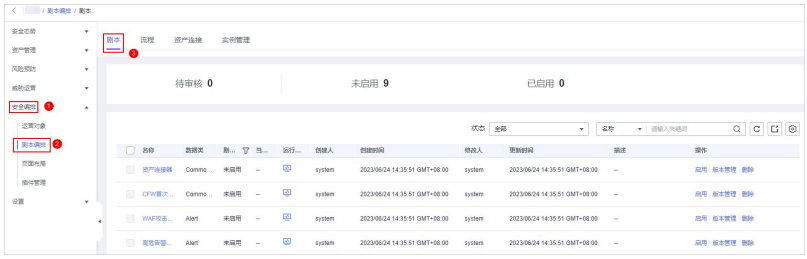
态势感知（专业版）支持导出“剧本状态”为“已启用”的剧本。

步骤 1 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-85 进入目标工作空间管理页面

步骤 2 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-86 进入剧本管理页面



步骤 3 勾选需导出的剧本，单击列表右上角的，弹出导出剧本确认信息框。

步骤 4 在弹出的确认框中，单击“确认”，导出剧本信息到本地。

----结束

禁用剧本

步骤 1 登录管理控制台。

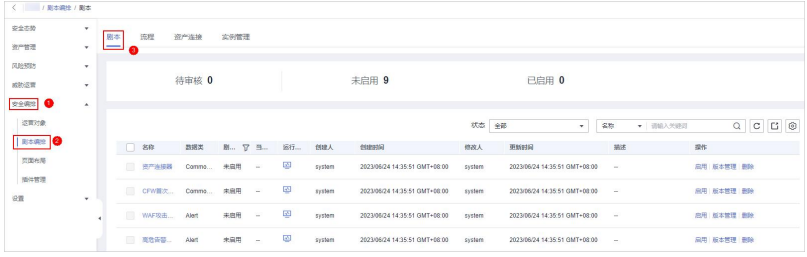
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-87 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-88 进入剧本管理页面



步骤 5 在目标剧本所在行“操作”列，单击“禁用”，弹出确认信息框。

步骤 6 在弹出确认框中，单击“确认”。

----结束

删除剧本

说明

删除剧本需要**全部满足**以下条件：

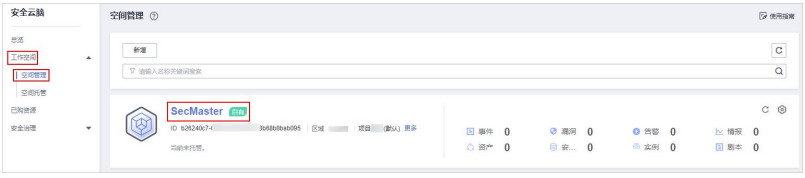
- “剧本状态”为“未启用”。
- 当前剧本中不存在激活的剧本版本。
- 不存在正在运行的剧本实例。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

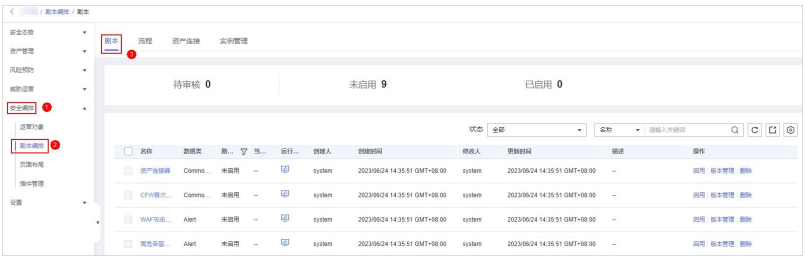
步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-89 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-90 进入剧本管理页面



步骤 5 在待删除的剧本“操作”列，单击“删除”，弹出删除剧本确认信息框。

步骤 6 在弹出删除剧本确认信息框中，单击“确认”，删除剧本。

说明

删除剧本默认删除当前剧本中的所有剧本版本，删除操作不可恢复，请谨慎操作。

----结束

12.7.1.5 管理剧本版本

操作场景

本章节将介绍如何执行预览剧本版本、编辑剧本版本、激活/失活剧本版本、复制剧本版本、删除剧本版本等操作。

预览剧本版本

说明

草稿版本暂不支持预览。

步骤 1 登录管理控制台。

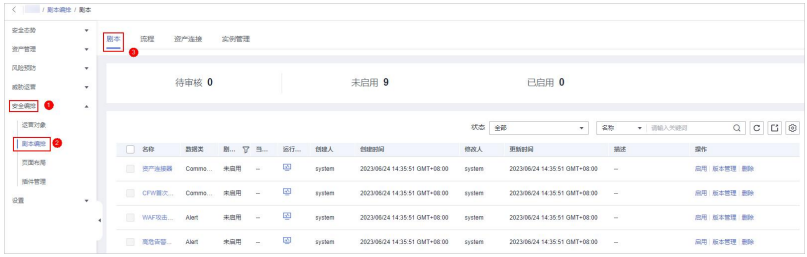
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-91 进入目标工作空间管理页面

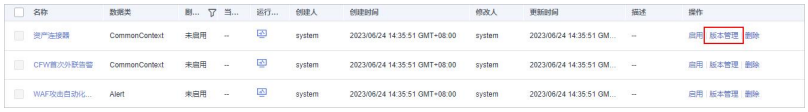
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-92 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-93 进入剧本版本管理页面



步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“预览”，弹出预览版本页面。

步骤 7 在剧本版本预览页面，查看目标剧本版本的详情，包括“基本信息”、“版本信息”、“匹配流程”等。

----结束

编辑剧本版本

说明

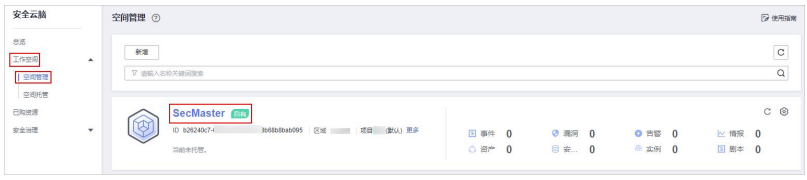
仅支持对版本状态为“未提交”的剧本版本进行编辑。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

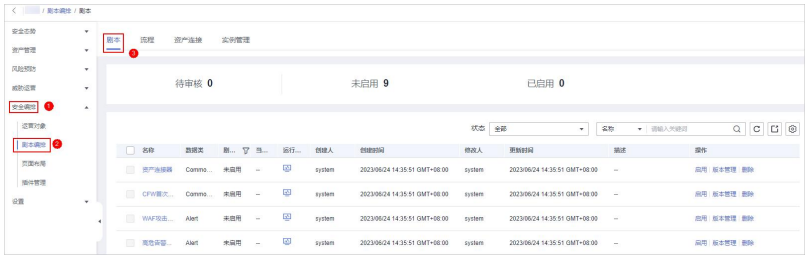
步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-94 进入目标工作空间管理页面



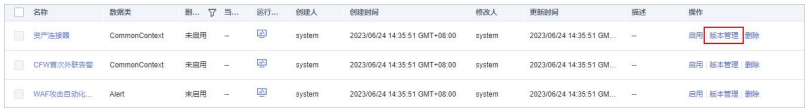
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-95 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-96 进入剧本版本管理页面



步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“编辑”，弹出编辑版本页面。

步骤 7 在剧本版本编辑页面，编辑版本信息。

步骤 8 单击“确定”，完成剧本的编辑。

----结束

激活/失活剧本版本

说明

- 只有版本状态为未激活的剧本版本才能激活。
- 每个剧本只允许存在一个激活版本。
- 激活当前版本后，之前激活的版本将会失活。例如，此次激活 V2 版本，则处于已激活状态的 V1 版本将被取消激活，更新为未激活状态。

步骤 1 登录管理控制台。

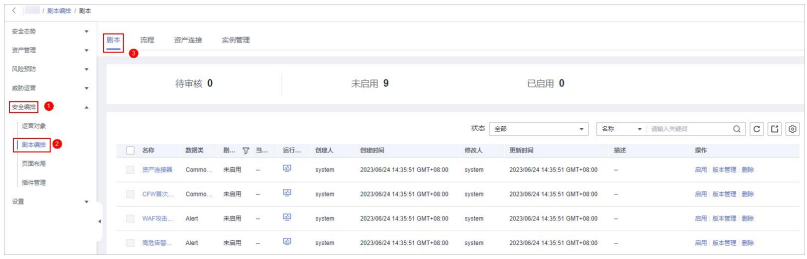
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-97 进入目标工作空间管理页面

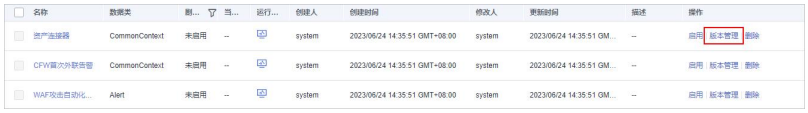
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-98 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-99 进入剧本版本管理页面



步骤 6 在版本管理页面中，单击“版本信息”栏中目标剧本版本所在行“操作”列的“激活”（或“取消激活”），完成激活（或失活）操作。

----结束

复制剧本版本

说明

仅支持复制“已激活”、“未激活”的剧本版本。

步骤 1 登录管理控制台。

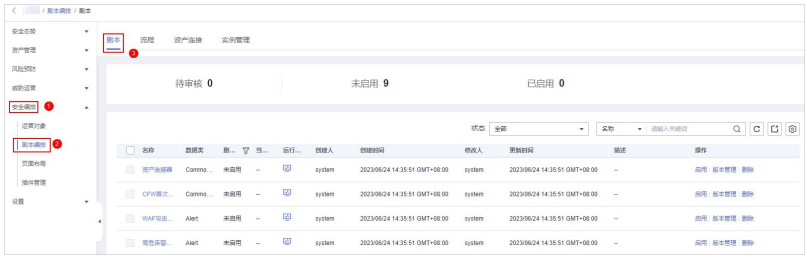
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-100 进入目标工作空间管理页面

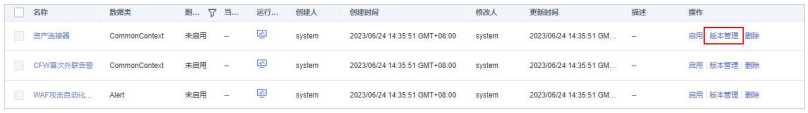
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-101 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-102 进入剧本版本管理页面



步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“复制”，弹出复制版本页面。

步骤 7 在弹出复制版本信息框中，单击“确认”，完成复制剧本版本。

----结束

删除剧本版本

说明

删除剧本版本需要**全部满足**以下条件：

- 剧本版本处于失活状态。
- 不存在正在运行的剧本版本实例。

步骤 1 登录管理控制台。

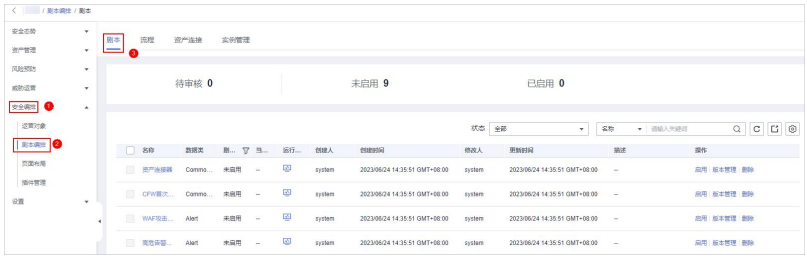
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-103 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 12-104 进入剧本管理页面



步骤 5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 12-105 进入剧本版本管理页面

步骤 6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“删除”，完成删除剧本版本。

说明

剧本版本删除后，不可找回，请谨慎操作。

----结束

12.7.2 流程

12.7.2.1 审核流程版本

操作场景

本章节主要介绍如何审核流程版本。

操作步骤

步骤 1 登录管理控制台。

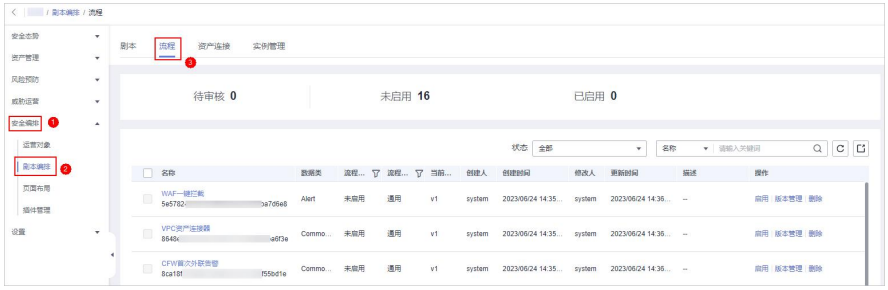
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-106 进入目标工作空间管理页面

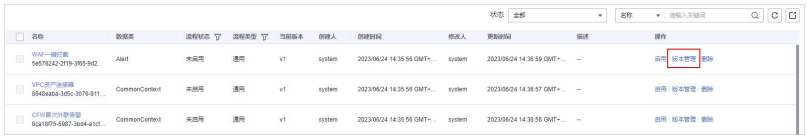
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-107 流程管理页面



步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-108 进入流程版本管理页面



步骤 6 在流程版本管理页面中，单击目标流程所在行的“操作”列的“审核”，弹出审核确认框。

步骤 7 在审核确认框中，选择“审核意见”，参数说明如表 12-30 所示。

表 12-30 审核流程参数说明

参数	说明
审核意见	勾选审核结论。 • 通过，通过后流程版本状态更新为已激活。 • 驳回，驳回后流程版本状态更新为审核驳回，可再次编辑后提交。
驳回原因	输入审核意见（当审核意见勾选驳回时必填）。

说明

- 审核驳回后的流程版本可进行编辑，具体操作请参见 12.7.2.4 管理流程版本。
- 流程版本状态变化：

  当前流程仅有一个流程版本时，审核通过后的流程“版本状态”默认为“已激活”。

步骤 8 单击“确定”，完成审核流程版本。

----结束

后续处理

流程版本审核后，需要启用流程，详细操作请参见 12.7.2.2 启用流程。

12.7.2.2 启用流程

操作场景

本章节主要介绍如何启用流程。

前提条件

已激活流程版本，具体操作请参见 12.7.2.4 管理流程版本。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

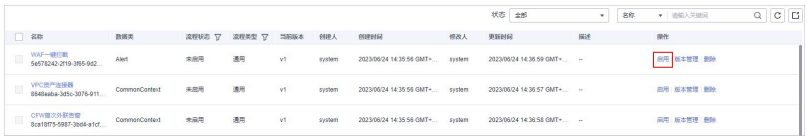
图 12-109 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-110 流程管理页面

步骤 5 在目标流程所在行的“操作”列，单击“启用”，页面弹出启用确认框。

图 12-111 启用流程



步骤 6 在弹出的确认框中，选择启用的流程版本后，单击“确定”，完成流程启用。

----结束

12.7.2.3 管理流程

操作场景

本章节将介绍如何查看流程、导入流程、导出流程、删除流程、禁用流程。

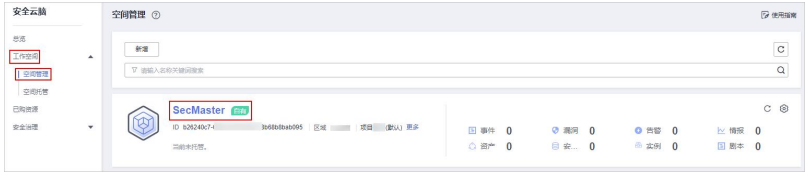
查看流程

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-112 进入目标工作空间管理页面

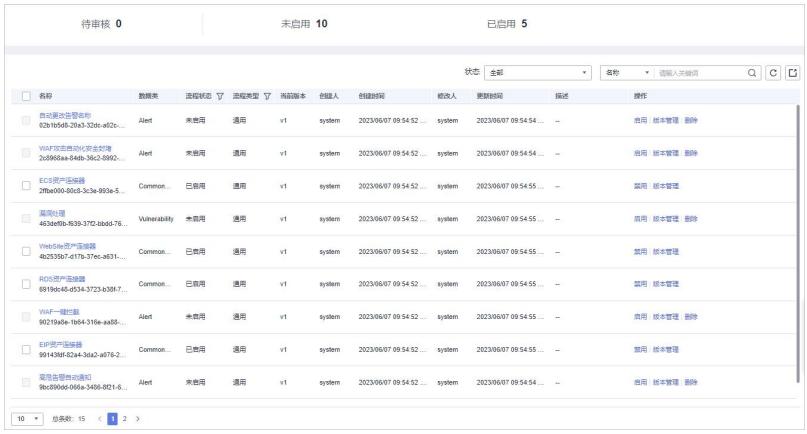


步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-113 流程管理页面

步骤 5 在流程管理页面中，查看已创建流程的信息。

图 12-114 查看流程信息



- 流程列表上方，呈现当前**待审核**、**未启用**、**已启用**流程的总数。
- 在流程列表中查看已有流程的信息。

  当流程较多时，可以通过搜索功能，选择流程的“状态”、“名称”、“描述”或“数据类”，并在搜索框中输入关键词，单击，即可快速查询指定流程。

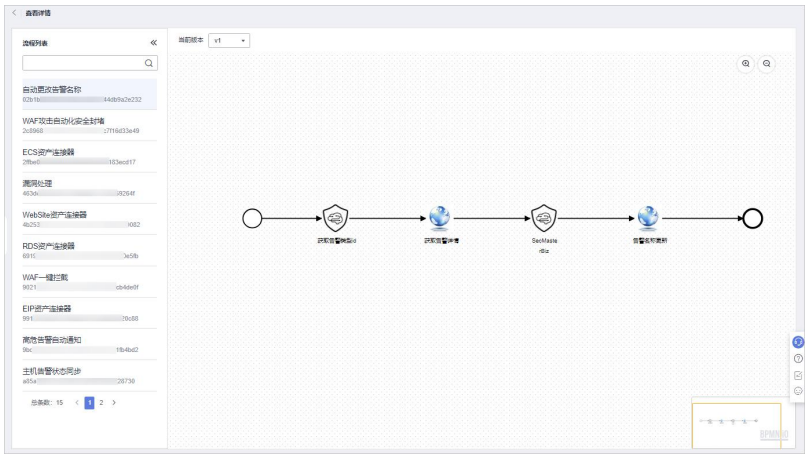
表 12-31 流程参数说明

参数名称	参数说明
名称	流程名称。
数据类	流程对应的数据类。
流程状态	流程当前状态。当前分为已启用和未启用两种状态。
流程类型	流程当前的类型。
当前版本	流程当前的版本。

参数名称	参数说明
创建人	创建该流程的用户。
创建时间	流程的创建时间。
修改人	最近一次修改该流程的用户。
更新时间	流程最近一次更新的时间。
描述	流程的描述信息。
操作	用户可以在操作栏中，执行启用、版本管理等操作。

步骤 6 如需查看某个流程的详细信息，可单击待查看流程的名称，进入流程详情页面查看流程的详细信息。

图 12-115 流程详情示例



----结束

导入流程

步骤 1 登录管理控制台。

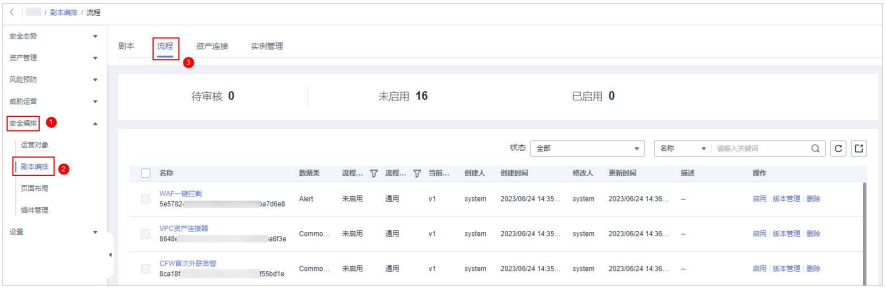
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-116 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-117 流程管理页面



步骤 5 在流程管理列表右上角单击“导入”，弹出导入流程窗口。

步骤 6 单击“添加文件”，并选择待导入文件。

步骤 7 单击“上传”。

----结束

导出流程

说明

支持导出“流程状态”为“已启用”的流程。

步骤 1 登录管理控制台。

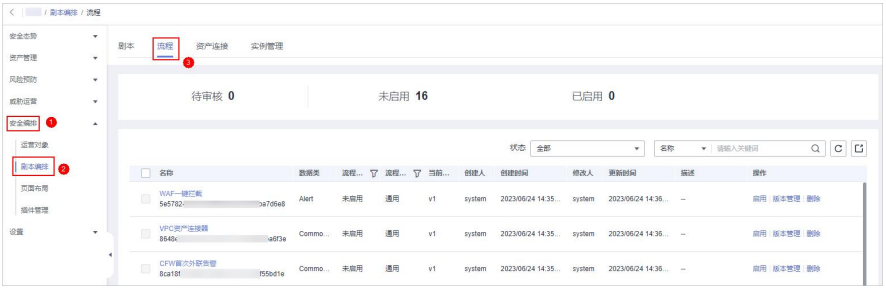
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-118 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-119 流程管理页面



步骤 5 在流程管理页面中，勾选需导出的流程，并单击列表右上角的  ，弹出导出流程确认框。

步骤 6 在弹出的确认框中，单击“确认”，系统将导出流程信息到本地。

----结束

删除流程

说明

删除流程需要**全部满足**下列条件：

- “流程状态”为“未启用”。
- 当前流程中不存在激活的流程版本。

步骤 1 登录管理控制台。

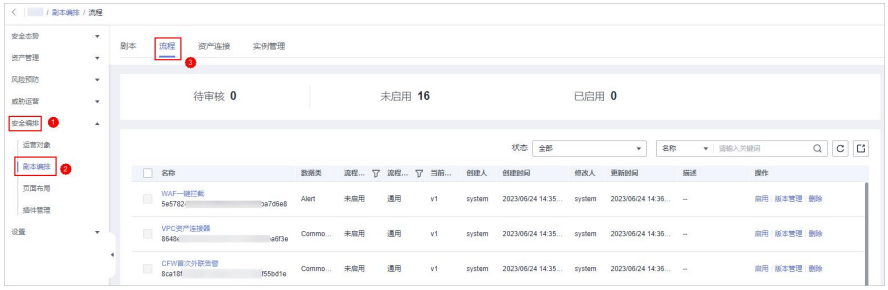
步骤 2 单击页面左上方的  ，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-120 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-121 流程管理页面



步骤 5 在流程管理页面中，单击目标流程所在行“操作”列的“删除”，弹出删除流程确认框。

步骤 6 单击“确认”，删除流程。

说明

删除时，默认删除当前流程中的所有历史版本，删除后不可恢复，请谨慎操作。

----结束

禁用流程

步骤 1 登录管理控制台。

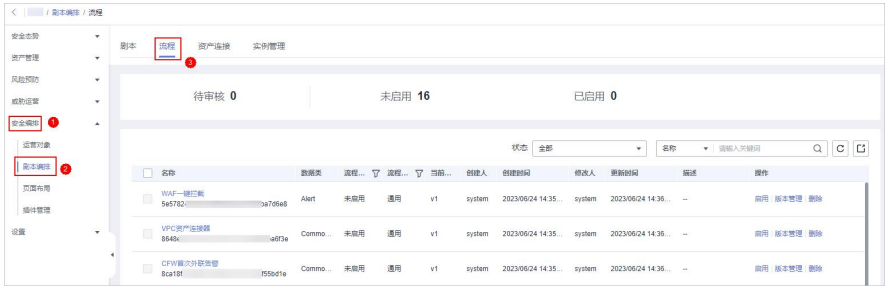
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-122 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-123 流程管理页面



步骤 5 在目标流程所在行的“操作”列，单击“禁用”，页面弹出禁用确认框。

步骤 6 在弹出的确认框中，单击“确认”，完成流程禁用。

----结束

12.7.2.4 管理流程版本

操作场景

本章节将介绍如何复制流程版本、编辑流程版本、提交流程版本、激活/失活流程版本、删除流程版本。

复制流程版本

步骤 1 登录管理控制台。

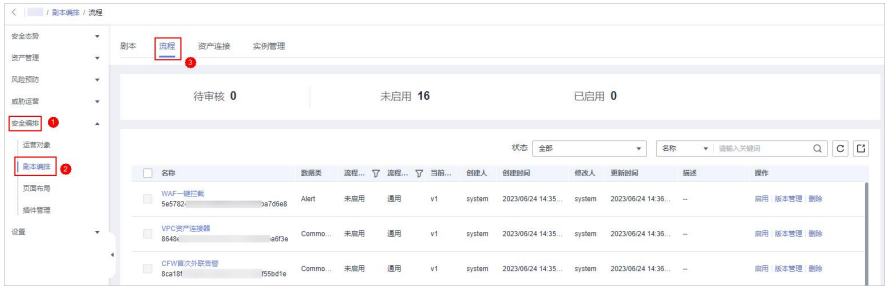
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-124 进入目标工作空间管理页面

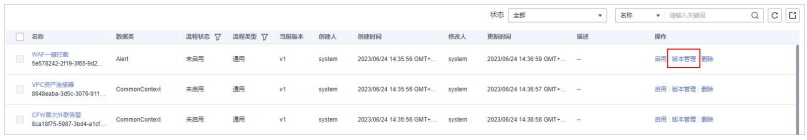
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-125 流程管理页面



步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-126 进入流程版本管理页面



步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“复制”，弹出确认框。

步骤 7 在弹出的确认框中，单击“确认”，完成复制流程版本。

----结束

编辑流程版本

说明

支持对“版本状态”为“待提交”或“审核驳回”的流程版本进行编辑。

步骤 1 登录管理控制台。

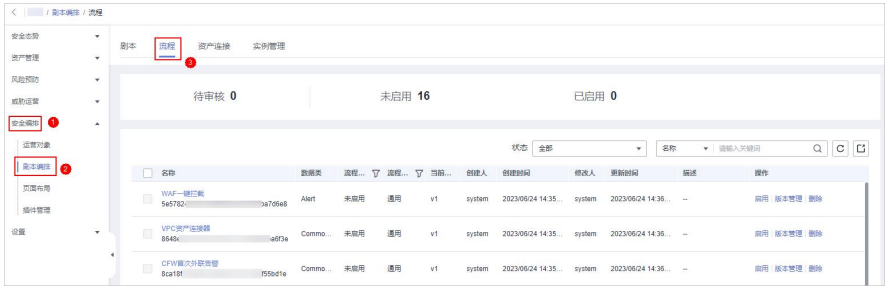
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-127 进入目标工作空间管理页面

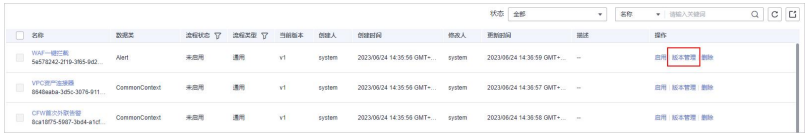
步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-128 流程管理页面



步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-129 进入流程版本管理页面



步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤 7 在流程图绘制页面中，从左侧资源库（提供基础节点、流程节点、插件节点）拖拽节点到右边画布，进行设计。

表 12-32 资源库参数详情

参数名称			参数说明
基础	基础节点	开始节点	一个流程的开始。每个流程仅允许一个开始节点，整个流程从开始节点启动执行。

参数名称			参数说明
		结束节点	一个流程的结束。每个流程存在多个结束节点，但是流程必须以结束节点收尾，即结束节点不允许出现在其他节点执行之前。
		人工审核	流程执行到该节点会暂停，此时在 8.3.1 查看待办任务页面产生一条待办任务。 用户在我的待办页面处理完成后，继续执行后续节点。 人工审核节点参数说明如表 12-33 所示。
		子流程	另起一个流程，主要用于执行循环操作。相当于流程中的循环体。
	系统插件	排他网关	线路分流时，根据条件表达式选择多条线路中的一条执行。 线路汇聚时，多条线路只要有一条线路到达则继续后面的节点执行。
		并行网关	线路分流时，所有线路都会执行。 线路汇聚时，多条线路全部到达，才会继续后续节点的执行(若有一条失败，则整个流程都会失败)
		包容网关	线路分流时，根据条件表达式选择符合条件的所有表达式执行。 线路汇聚时，所有分流时被执行的线路都到达包容网关时，才会继续后续节点执行(若有一条失败，则整个流程都会失败)
流程节点			可以选择当前工作空间中已经发布的所有流程。
插件节点			可以选择当前工作空间中所有插件。

表 12-33 人工审核节点参数说明

参数名称	参数说明
主键 ID	系统自动生成主键 ID，可根据需要进行修改。
名称	自定义人工审核节点名称。
到期时间	人工审核节点到期时间。
描述	自定义人工审核节点的描述信息。
查看参数	单击  ，并在弹出的选择上下文页面中，选择已有的参数名称。如需新增，可单击“新增参数”进行添加。

参数名称	参数说明
人工处理参数	输入参数 Key。如需新增，可单击“新增参数”进行添加。
处理人	设置此流程的审核处理人为当前账号中的 IAM 用户。设置后如有流程需审批，仅设置的责任人可在 8.3.1 查看待办任务页面进行处理，非责任人仅支持查看。 **说明** 首次使用，需要授权。具体操作如下： 1. 单击“现在授权”，右侧弹出访问授权页面。 2. 在访问授权页面中，勾选“同意授权”，并单击“确认”。

步骤 8 设计完成后，单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

如果流程校验失败，请根据失败提示进行检查。

----结束

提交流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

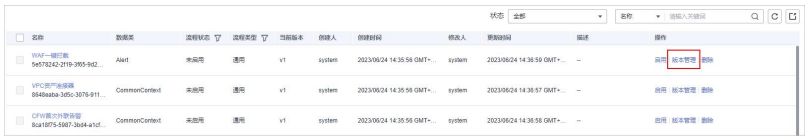
图 12-130 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-131 流程管理页面

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-132 进入流程版本管理页面



步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程所在行的“操作”列的“提交”，弹出提交确认框。

图 12-133 提交流程版本

步骤 7 在确认框中，单击“确认”，提交流程版本。

说明

- 流程版本提交后“版本状态”更新为“待审核”。
- 流程版本提交后不可以再编辑，如果需要编辑可以新建版本，或者在审核中驳回提交。

----结束

激活/失活流程版本

说明

- 只有版本状态为未激活的流程版本才能激活。
- 每个流程只允许存在一个激活版本。
- 激活当前版本后，之前激活的版本将会失活。例如，此次激活 V2 版本，则处于已激活状态的 V1 版本将被取消激活，更新为未激活状态。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

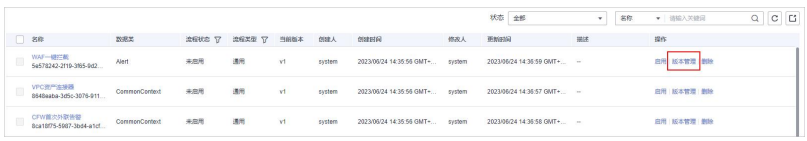
图 12-134 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-135 流程管理页面

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-136 进入流程版本管理页面



步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“激活”或者“取消激活”。

图 12-137 取消激活示例

步骤 7 在弹出确认框中，单击“确认”，完成激活/失活操作。

----结束

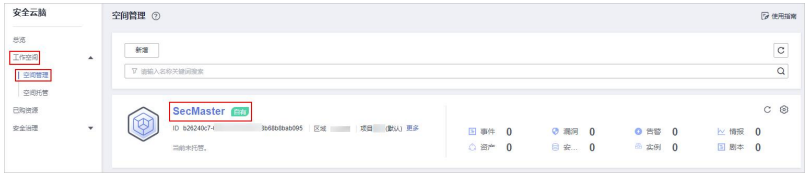
删除流程版本

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-138 进入目标工作空间管理页面

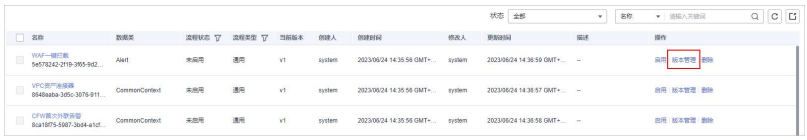


步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 12-139 流程管理页面

步骤 5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 12-140 进入流程版本管理页面



步骤 6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“删除”，并在弹出的确认框中，单击“确认”，删除流程版本。

说明

流程版本删除后，不可找回，请谨慎操作。

----结束

12.7.3 资产连接

12.7.3.1 新增资产连接

操作场景

本章节主要介绍如何新建资产连接。

前提条件

已新增工作空间，具体操作请参见 5.2 新增工作空间。

操作步骤

步骤 1 登录管理控制台。

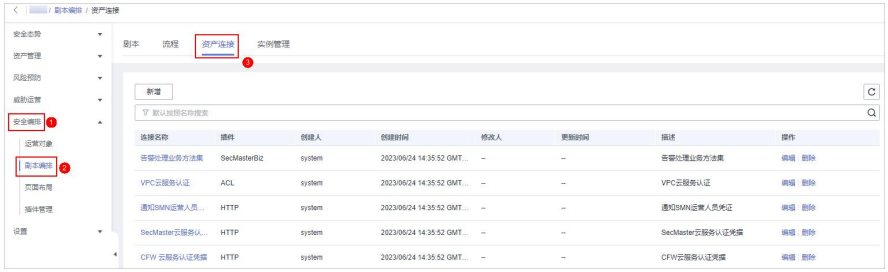
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-141 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 12-142 资产连接管理页面



步骤 5 在资产连接管理页面中，单击“新增”，右侧弹出新增资产连接面板。

步骤 6 在新增资产连接面板中，配置资产连接参数，参数说明如表 12-34 所示。

表 12-34 资产连接参数说明

参数名称	说明
连接名称	输入资产连接名称。名称规则如下： • 可输入英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（_）。 • 长度不能超过 64 个字符。
描述	可选参数，输入资产描述，描述信息长度不能超过 64 个字符。
插件	选择资产连接所需的插件。插件详细信息请参见 12.9.2 查看插件详情。

步骤 7 单击“确认”，返回资产列表，即可查询已经创建的资产连接信息。

----结束

12.7.3.2 管理资产连接

操作场景

本章节主要介绍如何查看资产连接、编辑资产连接、删除资产连接。

查看资产连接

步骤 1 登录管理控制台。

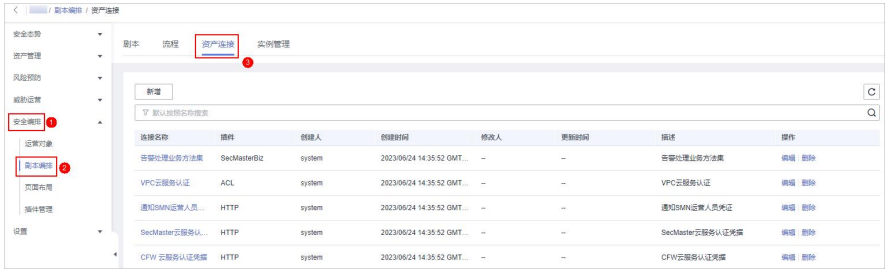
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-143 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 12-144 资产连接管理页面



步骤 5 在资产连接管理页面，查看资产连接信息。

当资产连接较多时，可以通过搜索功能，选择资产的“连接名称”、“插件”、“创建人”、“创建时间”、“修改人”、“更新时间”或“描述”，并在搜索框中输入关键词，单击，即可快速查询指定资产连接。

图 12-145 查看资产连接信息

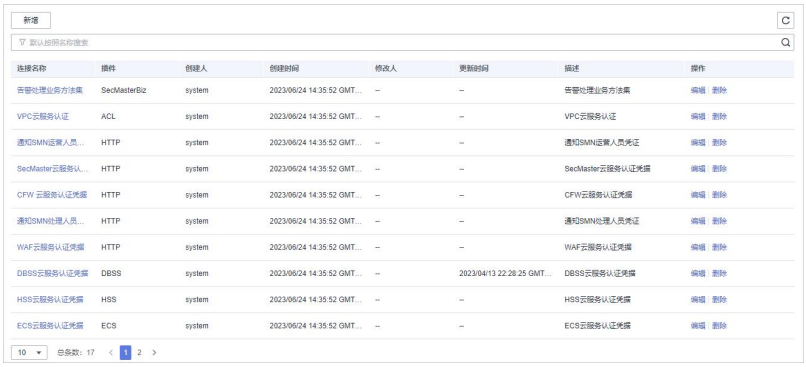


表 12-35 资产连接参数说明

参数名称	参数说明
连接名称	资产连接的名称。
插件	资产连接对应的插件。
创建人	创建资产连接的用户。
创建时间	资产连接的创建时间。
修改人	最近一次修改资产连接的用户。
更新时间	资产连接最近一次更新的时间。
描述	资产连接的描述信息。
操作	用户可以在操作栏中，执行编辑、删除操作。

步骤 6 如需查看某个资产连接的详细信息，可单击待查看资产连接的名称，进入资产连接详情页面进行查看。

----结束

编辑资产连接

步骤 1 登录管理控制台。

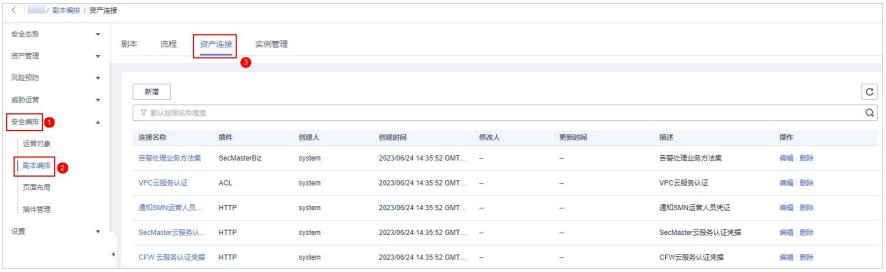
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-146 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 12-147 资产连接管理页面



步骤 5 在目标资产连接所在行“操作”列，单击“编辑”，弹出编辑资产连接页面。

步骤 6 在资产连接编辑页面中，编辑资产连接参数，参数说明如表 12-36 所示。

表 12-36 资产连接参数说明

参数名称	说明
连接名称	输入资产连接名称。名称规则如下： • 可输入英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（_）。 • 长度不能超过 64 个字符。
描述	可选参数，输入资产连接描述，描述信息长度不能超过 64 个字符。
插件	选择资产连接所需的插件。插件相关介绍请参见 12.9.2 查看插件详情。
创建人	资产连接的创建人，该参数**不支持修改**。
创建时间	资产连接的创建时间，该参数**不支持修改**。
修改人	资产连接的最近一次修改的用户，该参数**不支持修改**。

步骤 7 单击“确认”，完成资产连接的编辑。

----结束

删除资产连接

步骤 1 登录管理控制台。

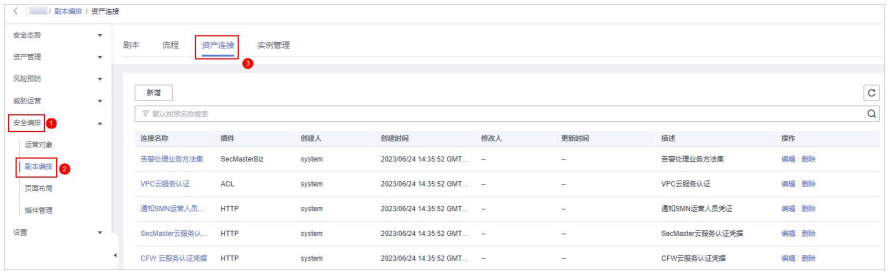
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-148 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 12-149 资产连接管理页面



步骤 5 在目标连接所在行“操作”列，单击“删除”，弹出删除确认框。

步骤 6 在弹出的确认框中，单击“确认”，完成资产连接删除。

说明

资产连接删除后，不可找回，请谨慎操作。

----结束

12.7.4 实例管理

12.7.4.1 查看剧本实例监控

操作场景

当剧本执行完成后，剧本实例管理列表中会生成剧本实例，即剧本实例监控。实例监控列表每条记录是一个实例，可呈现实例的历史实例任务列表，以及历史实例任务的运行情况。

本章节主要介绍如何查看实例监控信息。

约束与限制

流程实例最大手动重试次数为 3 次，且重试之后，须等剧本执行完毕之后才允许再次重试。

操作步骤

步骤 1 登录管理控制台。

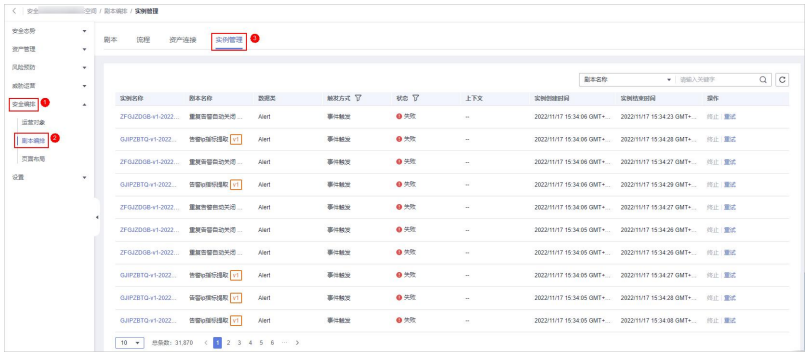
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-150 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“实例管理”页签，进入实例管理页面。

图 12-151 实例管理页面



步骤 5 在实例管理列表中，可查看实例名称、剧本名称、数据类等，参数说明如表 12-37 所示。

表 12-37 实例列表参数

参数名称	参数说明
实例名称	实例的名称。
剧本名称	实例对应的剧本名称。
数据类	剧本的运营对象，即数据类。
触发方式	实例的触发方式。 • 定时触发 • 事件触发
状态	实例的状态。 • 成功：剧本实例成功执行。 • 失败：剧本实例执行失败，单击操作列的重试可重新执行剧本。 • 运行中：剧本实例处于运行状态，单击操作列的终止可终止剧本。 • 重试中：剧本实例正在重试中。 • 终止中：剧本实例正在终止。 • 已终止：剧本实例已经成功终止。
上下文	实例的上下文信息。
实例创建时间	实例创建的具体时间。
实例结束时间	实例结束的具体时间。
操作	用户可执行终止、重试等操作。

步骤 6 如需查看某个实例的详细信息，可以单击任一实例名称，进入剧本实例图页面，可查看实例流程图和流程节点信息。

----结束

12.8 页面布局管理

12.8.1 查看已有布局模板

操作场景

布局中已有**告警管理**、**事件管理**、**漏洞管理**、**分析报告**、**情报管理**、**安全大屏**页面布局的管理页和详情页面模板。

本章节主要介绍如何查看已有布局模板。

操作步骤

步骤 1 登录管理控制台。

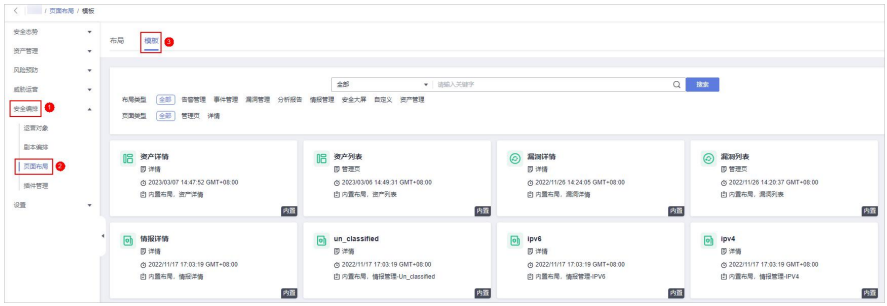
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-152 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 布局管理”，进入布局管理页面后，选择“模板”页签，进入布局模板页面。

图 12-153 进入布局模板页面



步骤 5 在布局模板页面，查看模板信息。

可以通过“布局类型”、“页面类型”，并输入关键字来搜索指定布局模板。

- 可以查看当前已有模板的名称、页面类型、创建时间等信息。
- 可以对已有模板的名称、模板内的布局进行编辑。
- 可以删除已有模板。

----结束

12.8.2 查看已有布局

操作场景

本章节将介绍如何查看已有布局。

查看已有布局

步骤 1 登录管理控制台。

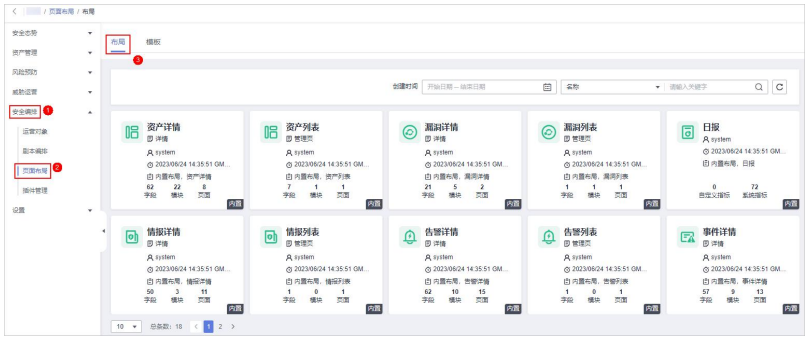
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-154 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 页面布局”，默认进入页面布局管理页面。

图 12-155 进入布局管理页面



步骤 5 在布局管理页面，查看已有布局。

将鼠标悬停在目标布局上，并单击布局右上角，可以进入布局配置详情页面进行查看。

----结束

12.9 插件管理

12.9.1 概述

态势感知（专业版）支持将安全编排流程中使用的插件进行统一管理。

名词解释

- **插件**：是包含函数、连接器、公共库的聚合。插件有自定义插件和商业插件两种类型，其中，自定义的插件可以在集市中显示，也可以在剧本中使用。
- **插件集**：是具有相同业务场景的插件集合。
- **函数**：是可以在剧本中选用的执行函数，在剧本中执行特定的行为。
- **连接器**：是用于连接数据源，将告警、事件等安全数据接入态势感知（专业版），包括事件触发和定时触发两种连接器类型。
- **公共库**：是一个公共模块，包含在其他组件中会使用到的 API 调用和公共函数。

12.9.2 查看插件详情

操作场景

本章节介绍如何查看态势感知（专业版）内置插件及详细信息。

操作步骤

步骤 1 登录管理控制台。

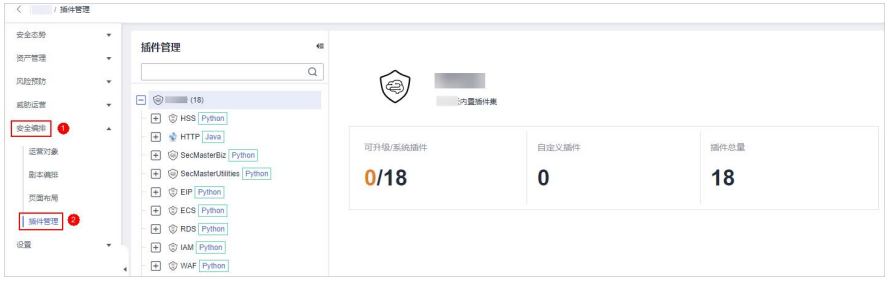
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-156 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“安全编排 > 插件管理”，进入插件管理页面。

图 12-157 进入插件管理页面



步骤 5 在插件管理页面中，查看插件详细信息。

- 左侧显示内置所有插件集、插件、函数信息。
- 如需查看某个查看详细信息，可以单击插件名称，右侧将展示插件的详细信息。
- 如果查看某个函数的详细信息，可以展开插件后，单击需要查看的函数名称，右侧将展示函数的详细信息。

----结束

13 设置

13.1 数据采集

13.1.1 数据采集概述

数据采集是指使用 Logstash 通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。

约束与限制

- 数据采集的 Agent 目前仅支持运行在某些版本的 EulerOS 的 Linux 系统的主机上，具体请参见支持的操作系统。
- 安装 Agent 时，在控制台中查看信息时，仅支持使用 IAM 账号登录。

支持的操作系统

数据采集的 Agent 目前仅支持运行在 Linux 系统 x86_64 架构的 ECS 主机上。ECS 主机支持以下操作系统类型：EulerOS 2.5、EulerOS 2.9、CentOS 7.9。

13.1.2 采集数据

操作场景

本章节介绍如何采集数据。

步骤一：购买 ECS

购买弹性云主机，详细操作请参见《弹性云主机用户指南》。

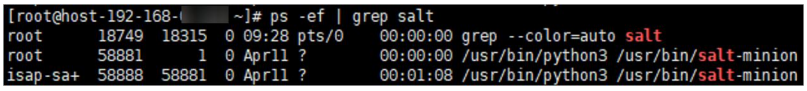
> **⚠ 注意**
>
> 数据采集的 Agent 目前仅支持运行在 Linux 系统 x86_64 架构的 ECS 主机上。ECS 主机支持以下操作系统类型：EulerOS 2.5、EulerOS 2.9、CentOS 7.9。
>
> 购买时，需注意操作系统和版本的选择。

图 13-1 选择操作系统版本

步骤二：安装 Agent

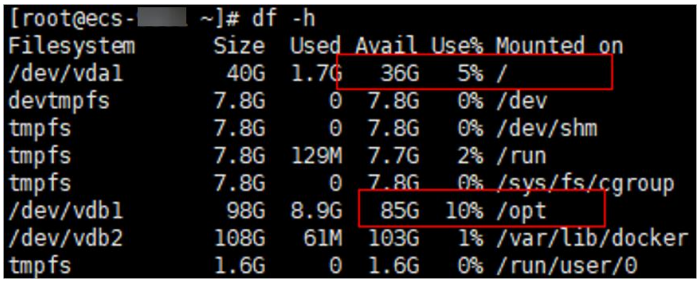
1. 安装 Agent 前预检查。
   a. 安装 Agent 前，执行 **ps -ef | grep salt** 命令，检查主机之前的 salt-minion 进程是否残留。
      - 如果有，请先关闭。
      - 如果没有，请继续执行 1.b。

      图 13-2 检查进程

   b. 安装 Logstash 前，执行 **df -h** 命令，检查磁盘的根目录盘或者 opt 盘预留 50G 以上，CPU 核数需要 2 核以上，内存需要 4G 以上。

      图 13-3 检查磁盘

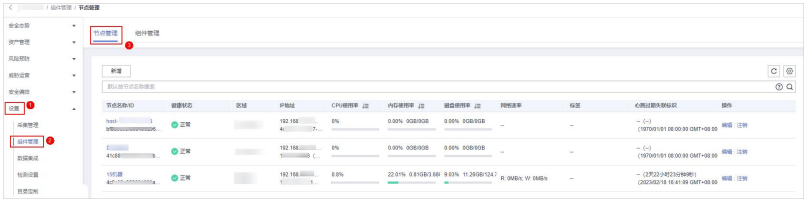
      

      如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。
2. 登录管理控制台。
3. 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。
4. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-4 进入目标工作空间管理页面

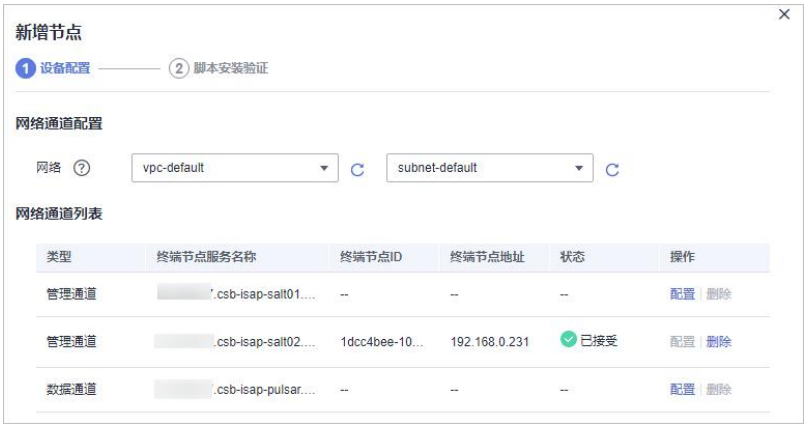
5. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 13-5 进入节点管理页面



6. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
7. 在新增节点页面中，配置设备。

图 13-6 新增节点



   a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。
   b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。
8. 单击页面右下角“下一步”，进入脚本安装验证页面后，单击 复制安装 Agent 的命令。
9. 远程登录待安装 Agent 的 ECS。
   - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机。

- 若您的主机已经绑定了弹性 IP，您也可以使用远程管理工具（例如：Xftp、SecureFX、WinSCP、PuTTY、Xshell 等）登录主机，并使用 root 账号在主机中安装 Agent。

10. 执行 **cd /opt/cloud** 命令，进入安装目录。

⚠ 注意

安装路径建议为“/opt/cloud”，本章节也以此路径为例进行介绍。如需安装在其他自定义路径中，请根据路径修改。

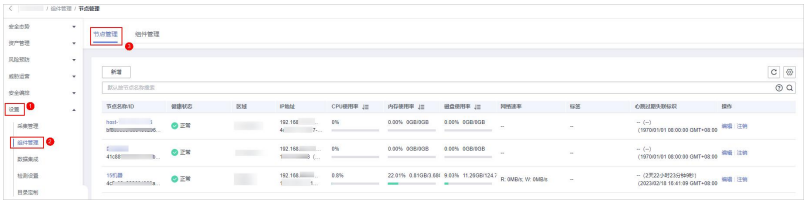
11. 粘贴在 8 复制的安装命令，以 root 权限执行，在 ECS 中安装 Agent。
12. 根据界面提示，输入登录控制台的 IAM 账号和密码。
13. 若界面回显类似如下信息时，则表示 Agent 安装成功。

```
install isap-agent successfully
```

步骤三：新增节点

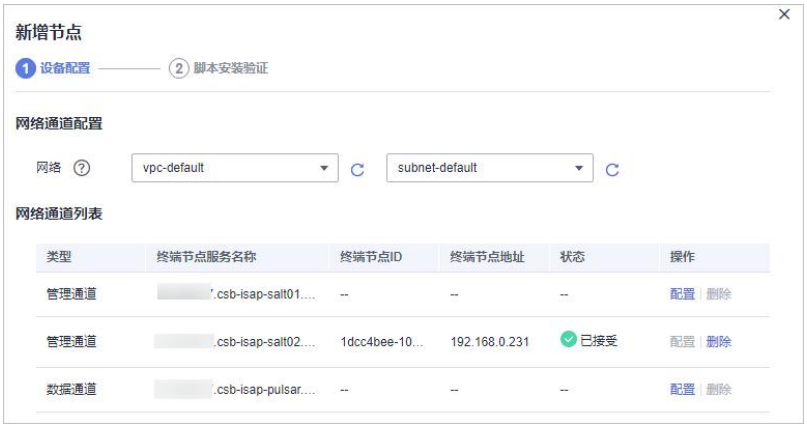
1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 13-7 进入节点管理页面



2. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
3. 在新增节点页面中，配置设备。

图 13-8 新增节点



a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。

b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。

4. 单击页面右下角“下一步”，进入“脚本安装验证”页面。

5. 确认已安装后，单击页面右下角“确认”。

步骤四：配置组件

1. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

2. 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

3. 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。

4. 单击页面右下角“保存并应用”。

步骤五：新增数据连接

1. 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 13-9 进入采集管理页面

2. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。

3. 新增数据连接来源。

   在“来源”页签中，选择数据源类型的来源，并根据选择的类型进行参数配置。

   数据源类型来源支持以下类型：传输控制协议 Tcp、文件 File、用户数据协议 Udp、对象存储 Obs、消息队列 Kafka、云脑管道 Pipe

4. 新增数据源连接目的。

   选择“目的”页签中，选择数据源类型的目的，并根据选择的类型进行参数配置。

   数据源类型目的支持以下类型：文件 File、传输控制协议 Tcp、用户数据协议 Udp、消息队列 Kafka、对象存储 Obs、云脑管道 Pipe

5. 设置完成后，单击页面右下角“确认”。

（可选）步骤六：配置解析器

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-10 进入解析器管理页面

2. 支持•自定义新增和•由模板创建，请根据您的需要进行选择。
   - **自定义新增**
     i. 在解析器列表管理页面中，单击“新增”，进入新增解析器页面。
     ii. 在新增解析器页面中，进行参数配置。

表 13-1 新增解析器

参数名称		参数说明
基本信息	名称	设置解析器名称。
	描述	输入解析器描述信息。
规则列表		设置解析器解析规则。操作步骤如下： 1. 单击“添加”，并选择规则类型。 • 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv 解析”、“mutate 解析”、“grok 解析”、“date 解析”、“drop 解析”、“prune 解析”、“csv 解析”、“json 解析”。 • 条件控制：选择解析器的条件控制原则，支持选择“if 条件”、“else 条件”、“else if 条件”。 2. 根据选择的规则配置对应的参数信息。

     iii. 设置完成后，单击页面右下角“确定”。
   - **由模板创建**
     i. 在解析器管理页面中，选择“模板列表”页签。
     ii. 在目标模板页面中，单击目标模板所在行“操作”列的“由模板创建”。
     iii. 在新增解析器页面中，进行参数配置。

表 13-2 新增解析器

参数名称	参数说明

参数名称		参数说明
基本信息	名称	解析器名称，系统已根据模板自动生成，可进行修改。
	描述	解析器描述信息，系统已根据模板自动生成，可进行修改。
规则列表		解析器解析规则，系统已根据模板自动生成，可进行修改。 如需添加规则，可以单击“添加”，选择规则类型，并根据选择的规则配置对应的参数信息。 • 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv 解析”、“mutate 解析”、“grok 解析”、“date 解析”、“drop 解析”、“prune 解析”、“csv 解析”、“json 解析”。 • 条件控制：选择解析器的条件控制原则，支持选择“if 条件”、“else 条件”、“else if 条件”。

iv. 设置完成后，单击页面右下角“确定”。

步骤七：新增采集通道

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 13-11 进入采集通道管理页面

2. 新增分组。
   a. 在采集通道管理页面中，单击“分组列表”右侧的。
   b. 输入分组名称，并单击，完成新增。

   分组新增完成后，如需编辑/删除，可以将鼠标悬停在分组名称后，单击编辑/删除按钮，进行编辑/删除操作。
3. 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。
4. 在“基础配置”页面中，配置基础信息。

表 13-3 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
目的配置	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择来源的相关信息。

5. 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。
6. 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

   如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见 13.1.3.2 管理解析器。
7. 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。
8. 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。
   - 运行参数：节点添加后，如在已添加节点中运行参数，请参照以下步骤进行处理：
     i. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。
     ii. 单击“添加配置”，设置运行键和运行值。
   - 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。
9. 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。
10. 在“通道详情预览”页面确认配置无误后，单击“确定”。

相关操作

14.1.8 Agent 安装失败问题排查

13.1.3 采集管理

13.1.3.1 管理连接

操作场景

本章节主要介绍如何执行新增连接、查看连接管理信息、编辑数据连接、删除数据连接操作。

约束与限制

- 数据连接新增成功后，仅支持对已选择的数据源类型的参数信息进行修改，不支持变更数据源类型。

新增连接

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-12 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 13-13 进入采集管理页面

步骤 5 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。

步骤 6 新增数据连接来源。

在“来源”页签中，选择数据源类型的来源，并根据选择的类型进行参数配置。

数据源类型来源支持以下类型：传输控制协议 Tcp、文件 File、用户数据协议 Udp、对象存储 Obs、消息队列 Kafka、云脑管道 Pipe

步骤 7 新增数据源连接目的。

选择“目的”页签中，选择数据源类型的目的，并根据选择的类型进行参数配置。

数据源类型目的支持以下类型：文件 File、传输控制协议 Tcp、用户数据协议 Udp、消息队列 Kafka、对象存储 Obs、云脑管道 Pipe

步骤 8 设置完成后，单击页面右下角“确认”。

----结束

查看连接管理信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-14 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 13-15 进入采集管理页面

步骤 5 在连接管理页面中，查看连接管理的详细信息。

表 13-4 连接管理参数说明

参数名称	参数说明

参数名称	参数说明
连接名称	连接的名称。
连接类型	连接的类型
连接信息	连接相关信息。
引用通道	连接被引用的通道数量。
描述	连接相关描述。
操作	支持对连接进行编辑、删除等操作。

----结束

编辑数据连接

说明

数据连接新增成功后，仅支持对已选择的数据源类型的参数信息进行修改，不支持变更数据源类型。

例如，新增数据连接时选择的数据源类型为“文件 File”，仅支持对文件类型中的参数进行修改，不支持变更“文件 File”类型。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-16 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 13-17 进入采集管理页面

步骤 5 在连接管理页面中，单击目标连接所在行“操作”列的“编辑”。

步骤 6 在“数据源类型选择”页面中，编辑数据源类型信息参数信息。

步骤 7 设置完成后，单击页面右下角“确认”。

----结束

删除数据连接

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-18 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 13-19 进入采集管理页面

步骤 5 在连接管理页面中，单击目标连接所在行“操作”列的“删除”。

步骤 6 在弹出的确认框中单击“确认”。

----结束

13.1.3.2 管理解析器

操作场景

本章节主要介绍如何执行创建解析器、查看解析器管理信息、导入解析器、编辑解析器、导出解析器、删除解析器操作。

创建解析器

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-20 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-21 进入解析器管理页面

步骤 5 支持•自定义新增和•由模板创建，请根据您的需要进行选择。

- **自定义新增**
  a. 在解析器列表管理页面中，单击“新增”，进入新增解析器页面。
  b. 在新增解析器页面中，进行参数配置。

表 13-5 新增解析器

参数名称		参数说明
基本信息	名称	设置解析器名称。
	描述	输入解析器描述信息。
规则列表		设置解析器解析规则。操作步骤如下： 1. 单击“添加”，并选择规则类型。 • 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv 解析”、“mutate 解析”、“grok 解析”、“date 解析”、“drop 解析”、“prune 解析”、“csv 解析”、“json 解析”。 • 条件控制：选择解析器的条件控制原则，支持选择“if 条件”、“else 条件”、“else if 条件”。 2. 根据选择的规则配置对应的参数信息。

c. 设置完成后，单击页面右下角“确定”。

- **由模板创建**

a. 在解析器管理页面中，选择“模板列表”页签。

b. 在目标模板页面中，单击目标模板所在行“操作”列的“由模板创建”。

c. 在新增解析器页面中，进行参数配置。

表 13-6 新增解析器

参数名称		参数说明
基本信息	名称	解析器名称，系统已根据模板自动生成，可进行修改。
	描述	解析器描述信息，系统已根据模板自动生成，可进行修改。
规则列表		解析器解析规则，系统已根据模板自动生成，可进行修改。 如需添加规则，可以单击“添加”，选择规则类型，并根据选择的规则配置对应的参数信息。 • 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv 解析”、“mutate 解析”、“grok 解析”、“date 解析”、“drop 解析”、“prune 解析”、“csv 解析”、“json 解析”。 • 条件控制：选择解析器的条件控制原则，支持选择“if 条件”、“else 条件”、“else if 条件”。

d. 设置完成后，单击页面右下角“确定”。

----结束

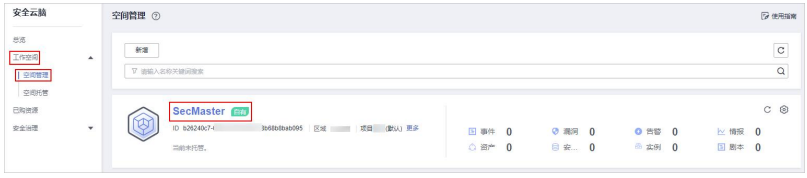
查看解析器管理信息

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-22 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-23 进入解析器管理页面

步骤 5 在解析器管理页面中，查看解析器的详细信息。

表 13-7 解析器管理参数说明

参数名称	参数说明
名称	解析器的名称。
引用通道	解析器被引用的通道数量。
描述	解析器相关描述。
操作	支持对解析器进行编辑、删除等操作。

步骤 6 在解析器管理页面中，选择“模板列表”页签，进入模板列表页面。

步骤 7 在模板列表页面中，查看解析器模板信息。

表 13-8 模板参数说明

参数名称	参数说明
名称	解析器模板名称。
描述	解析器模板相关描述。
操作	支持对解析器模板进行创建解析器操作。

----结束

导入解析器

说明

- 仅支持导入 json 格式的文件，且文件大小不超过 1MB。
- 一次最多支持导入 5 个解析器文件，且每个解析器文件最多支持包含 100 个解析器。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-24 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-25 进入解析器管理页面

步骤 5 在解析器列表管理页面中，单击解析器列表左上角的“导入”，弹出导入文件对话框。

步骤 6 在弹出的导入文件对话框中，单击“添加文件”，选择你需要导入的 json 文件。

⚠ 注意

- 仅支持导入 json 格式的文件，且文件大小不超过 1MB。
- 一次最多支持导入 5 个解析器文件，且每个解析器文件最多支持包含 100 个解析器。

步骤 7 选择完成后，单击“确定”，完成导入。

导入成功后，可以在解析器列表中查看导入的解析器信息。

----结束

编辑解析器

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-26 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-27 进入解析器管理页面

步骤 5 在解析器列表管理页面中，单击目标解析器所在行“操作”列的“编辑”。

步骤 6 在编辑解析器页面中，编辑解析器信息。

表 13-9 编辑解析器

参数名称		参数说明
基本信息	名称	设置解析器名称。
	描述	输入解析器描述信息。
规则列表		设置解析器解析规则。操作步骤如下： 单击“添加”，并选择规则类型。 • 解析规则：选择解析器的解析规则。 • 条件控制：选择解析器的条件控制原则。

步骤 7 设置完成后，单击页面右下角“确定”。

----结束

导出解析器

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-28 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-29 进入解析器管理页面

步骤 5 在解析器列表管理页面中，勾选需要导出的解析器，并单击列表上方的“导出”。

系统将自动下载.json 格式的解析器文件到本地。

----结束

删除解析器

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-30 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 13-31 进入解析器管理页面

步骤 5 在解析器管理页面中，单击目标解析器所在行“操作”列的“删除”。

步骤 6 在弹出的确认框中单击“确认”。

----结束

13.1.3.3 管理采集通道

操作场景

本章节主要介绍如何执行新增采集通道、查看采集通道、编辑采集通道、删除采集通道、启用/停止/重启采集通道操作。

新增采集通道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-32 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 13-33 进入采集通道管理页面

步骤 5 新增分组。

1. 在采集通道管理页面中，单击“分组列表”右侧的。
2. 输入分组名称，并单击，完成新增。

分组新增完成后，如需编辑/删除，可以将鼠标悬停在分组名称后，单击编辑/删除按钮，进行编辑/删除操作。

步骤 6 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。

步骤 7 在“基础配置”页面中，配置基础信息。

表 13-10 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
目的配置	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择来源的相关信息。

步骤 8 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。

步骤 9 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见 13.1.3.2 管理解析器。

步骤 10 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。

步骤 11 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。

- 运行参数：节点添加后，如在已添加节点中运行参数，请参照以下步骤进行处理：
  a. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。
  b. 单击“添加配置”，设置运行键和运行值。
- 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。

步骤 12 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。

步骤 13 在“通道详情预览”页面确认配置无误后，单击“确定”。

----结束

查看采集通道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-34 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 13-35 进入采集通道管理页面

步骤 5 在采集通道管理页面中，查看采集通道的详细信息。

表 13-11 采集通道参数说明

参数名称	参数说明

参数名称	参数说明
分组列表	采集通道分组列表及各分组名称。
名称	采集通道的名称。
连接信息	采集通道连接信息。
创建人	采集通道的创建人。
健康状态	采集通道的状态。
接收速率	采集通道的接收速率。
发送速率	采集通道的发送速率。
配置状态	采集通道的配置状态。
通道实例	采集通道数量。
运行状态	采集通道的运行状态。
操作	支持对采集通道进行编辑、停止等操作。

----结束

编辑采集通道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-36 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 13-37 进入采集通道管理页面

步骤 5 在采集通道管理列表中，单击目标通道所在行“操作”列的“更多 > 编辑”，进入编辑采集通道页面。

步骤 6 在“基础配置”页面中，配置基础信息。

表 13-12 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择目的的相关信息。

步骤 7 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。

步骤 8 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见 13.1.3.2 管理解析器。

步骤 9 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。

步骤 10 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。

- 运行参数：节点添加后，如在已添加节点中运行参数，请参照以下步骤进行处理：
  a. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。
  b. 单击“添加配置”，设置运行键和运行值。
- 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。

步骤 11 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。

步骤 12 在“通道详情预览”页面确认配置无误后，单击“确定”。

----结束

删除采集通道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-38 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 13-39 进入采集通道管理页面

步骤 5 在采集通道管理列表中，单击目标通道所在行“操作”列的“更多 > 删除”。

说明

只有当采集通道处于停止状态，才能执行删除操作。

步骤 6 在弹出的确认框中单击“确认”。

----结束

启用/停止/重启采集通道

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-40 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 13-41 进入采集通道管理页面

步骤 5 在采集通道管理列表中，单击目标通道所在行“操作”列的启用/停止/重启。

步骤 6 在弹出的确认框中单击“确认”。

----结束

13.1.3.4 管理采集节点

操作场景

本章节主要介绍如何执行查看采集节点信息操作。

查看采集节点信息

步骤 1 登录管理控制台。

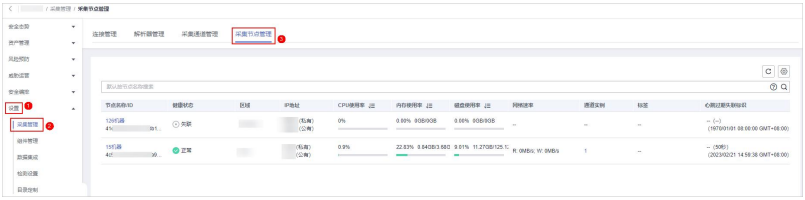
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-42 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集节点管理”页签，进入采集节点管理页面。

图 13-43 进入采集节点管理页面



步骤 5 在采集节点管理页面中，查看采集节点的详细信息。

当节点较多时，可以通过搜索功能，选择节点的“节点名称”或“节点 ID”，并在搜索框中输入关键词，单击，即可快速查询指定节点。

表 13-13 节点参数说明

参数名称	参数说明
节点名称/ID	节点的名称/ID。
健康状态	节点的健康状态。
区域	节点所在区域。
IP 地址	节点的 IP 地址。
CPU 使用率	节点的 CPU 使用率。
内存使用率	节点的内存使用率。
磁盘使用率	节点的磁盘使用率。
网络速率	节点的网络速率。
标签	节点的标签信息。
心跳过期失联标识	节点是否心跳过期失联。

步骤 6 如需查看某个节点的详细信息，可单击节点名称，在右侧弹出的详情页面进行查看。

----结束

13.1.4 组件管理

13.1.4.1 管理节点

操作场景

本章节将介绍如何执行新增节点、查看节点管理信息、编辑节点、注销节点操作。

新增节点

步骤 1 登录管理控制台。

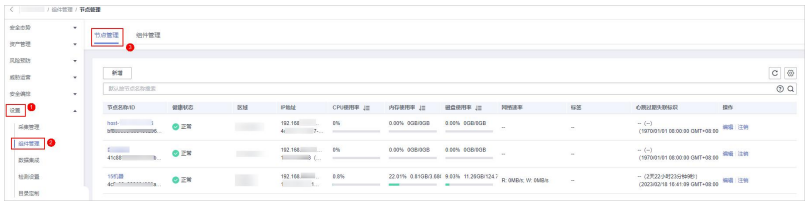
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-44 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 13-45 进入节点管理页面



步骤 5 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。

步骤 6 单击页面右下角“下一步”，进入“脚本安装验证”页面。

步骤 7 确认已安装后，单击页面右下角“确认”。

如未安装请参照步骤二：安装 Agent 进行处理。

----结束

查看节点管理信息

步骤 1 登录管理控制台。

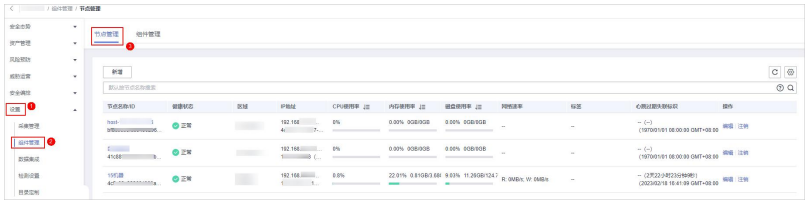
步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-46 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 13-47 进入节点管理页面



步骤 5 在节点管理页面中，查看节点的详细信息。

当节点较多时，可以通过搜索功能，选择节点的“节点名称”或“节点 ID”，并在搜索框中输入关键词，单击，即可快速查询指定节点。

表 13-14 节点参数说明

参数名称	参数说明
节点名称/ID	节点的名称/ID。
健康状态	节点的健康状态。
区域	节点所在区域。
IP 地址	节点的 IP 地址。
CPU 使用率	节点的 CPU 使用率。
内存使用率	节点的内存使用率。
磁盘使用率	节点的磁盘使用率。

参数名称	参数说明
网络速率	节点的网络速率。
标签	节点的标签信息。
心跳过期失联标识	节点是否心跳过期失联。

步骤 6 如需查看某个节点的详细信息，可单击节点名称，在右侧弹出的详情页面进行查看。

----结束

编辑节点

节点新增成功后，仅支持修改节点补充信息。

步骤 1 登录管理控制台。

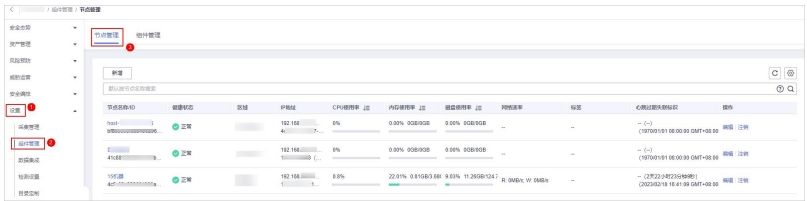
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-48 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 13-49 进入节点管理页面



步骤 5 在节点管理页面中，单击目标节点所在行“操作”列的“编辑”，页面右侧弹出编辑节点页面。

步骤 6 在编辑节点页面中，编辑节点补充信息。

表 13-15 节点补充信息

参数名称	参数说明
数据中心	自定义数据中心名称。
网络平面	选择节点网络平面。
标签	设置节点标签。
描述	自定义节点描述信息。
维护人	选择节点维护人。

步骤 7 单击页面右下角“确认”。

----结束

注销节点

步骤 1 登录管理控制台。

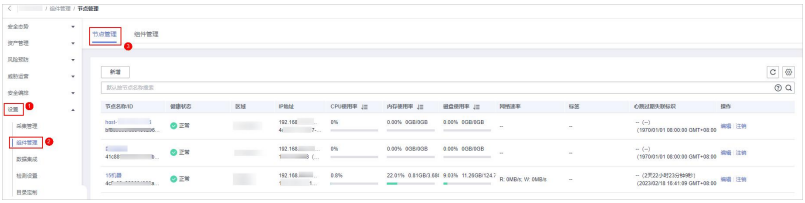
步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-50 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 13-51 进入节点管理页面



步骤 5 在节点管理页面中，单击目标节点所在行“操作”列的“注销”。

步骤 6 在弹出的确认框中，单击“确认”。

说明

仅注销节点，不会删除 ECS 和 endpointinterface 资源。

----结束

13.1.4.2 管理组件

操作场景

本章节将介绍如何配置组件、查看组件相关信息。

配置组件

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-52 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

步骤 5 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

步骤 6 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。

步骤 7 单击页面右下角“保存并应用”。

----结束

查看组件详情

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-53 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

步骤 5 在组件管理页面中，查看组件的详细信息。

- **运行节点：**

  单击待运行组件右上角“运行节点”，右侧将弹出该组件的运行节点信息。

- **查看配置：**

  单击待查看组件右上角“查看配置”，右侧将弹出该组件的详细配置信息。

- **编辑配置：**

  a. 单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

  b. 在节点配置栏中，编辑节点配置信息。

  - 添加节点：单击节点列表左上角“添加”，并在弹出的“添加节点”框中，选择节点后，单击“确认”。
  - 编辑已添加节点参数信息：单击节点名称前的，展开节点配置信息后，编辑节点参数信息。
  - 运行参数：单击目标节点所在行“操作”列的“运行参数”。
  - 移除节点：单击目标节点所在行“操作”列的“移除”。
  - 批量删除：选中带移除节点后，单击列表左上角“批量移除”。
  - 查看历史版本：单击页面右下角“历史版本”。

  c. 单击页面右下角“应用”。

----结束

13.2 数据集成

13.2.1 支持接入的日志

态势感知（专业版）支持集成多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

表 13-16 支持接入的日志

安全分类	云服务	日志描述	日志	集成后日志存储日期上限
主机安全	企业主机安全（Host Security Service，HSS）	主机安全告警	hss-alarm	180 天
		主机漏洞扫描结果	hss-vul	7 天
		主机安全日志	hss-log	15 天
应用安全	Web 应用防火墙（Web Application Firewall，WAF）	攻击日志	waf-attack	30 天
		访问日志	waf-access	30 天
	API 网关（API Gateway）	访问日志	apig-access	180 天
	云审计服务（Cloud Trace Service，CTS）	云审计服务日志	cts-audit	180 天
网络安全	入侵防御系统（Intrusion Prevention System，IPS）	攻击日志	nip-attack	180 天
	Anti-DDoS 流量清洗（Anti-DDoS）	攻击日志	ddos-attack	180 天
	云防火墙（Cloud Firewall，CFW）	访问控制日志	cfw-block	30 天
		流量日志	cfw-flow	15 天
		攻击事件日志	cfw-risk	180 天
数据安全	对象存储服务（Object Storage Service，OBS）	访问日志	obs-access	15 天
	数据库安全服务（Database Security Service，DBSS）	告警日志	dbss-alarm	180 天
	数据安全中心（Data Security Center，DSC）	告警日志	dsc-alarm	180 天
身份安全	统一身份认证（Identity and Access Management，IAM）	审计日志	iam-audit	180 天

13.2.2 接入数据

操作场景

态势感知（专业版）支持集成多种云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

本章节介绍如何接入数据并查看日志存储位置。

接入服务日志

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-54 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 数据集成”，进入数据集成页面。

步骤 5 在待接入云产品的“审计相关日志”列，单击，开启接入的云服务日志。

如需接入当前 region 所有云产品日志，可直接单击“一键接入服务日志”前的按钮，一键接入当前 region 所有云服务日志。

步骤 6 设置生命周期。

系统默认存储数据 7 天，您可以根据需要进行设置。

步骤 7 设置是否自动转告警。

在待设置云产品的“自动转告警”列，单击，开启接入的云服务日志满足告警条件时，自动转为告警，并且在“告警管理”页面中进行展示。

说明

- 如果此处未开启自动转告警，在对应日志满足告警条件时，将不会转为告警，也不会在“告警管理”页面中进行展示。
- 在态势感知（专业版）的“漏洞管理”页面可以接入主机漏洞扫描结果，如果数据集成操作时接入了主机漏洞扫描结果，但是未开启自动转告警，则在“漏洞管理”将不会展示主机相关的漏洞扫描情况。

步骤 8 单击“保存”，并在弹出的配置保存框中，单击“确定”。

接入完成后，将创建默认数据空间和管道。

----结束

查看日志数据的存储位置

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-55 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 数据集成”，进入数据集成页面后，在云产品接入表格的“存储位置”列查看日志数据存储位置。

查看后，可以前往目标工作空间的对应管道查看接入的日志数据。

----结束

相关操作

- 取消数据接入
  a. 在待取消接入云产品的“审计相关日志”列，单击，关闭接入的云服务日志。
  b. 单击“保存”。
- 编辑数据接入生命周期
  a. 在待编辑云产品的“生命周期”列，输入生命周期时间。
  b. 单击“保存”。
- 取消自动转告警
  a. 在待取消云产品的“自动转告警”列，单击，关闭告警映射。
  b. 单击“保存”。

13.3 检测设置

操作场景

使用云服务基线检查相关功能时，需要先参考本章节设置检查计划。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-56 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

步骤 5 在检测设置页面中，单击“创建计划”，系统右侧弹出新建检查计划页面。

步骤 6 配置检查计划。

1. 填写基本信息，具体参数配置如表 13-17 所示。

表 13-17 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。
检查时间	选择检测周期和检查触发时间。 • 检测周期：每隔 1 天、3 天、7 天、15 天、30 天检查一次 • 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00

2. 选择检查规范。

   选择需要检测的基线检查项目。

步骤 7 单击“确定”。

检查计划创建完成后，态势感知（专业版）会在指定的时间执行云服务基线扫描，扫描结果可以在“风险预防 > 基线检查”中查看。

----结束

13.4 目录定制

操作场景

态势感知（专业版）支持自定义目录，您可以根据需要对目录进行定制。本章节将介绍以下操作：

- 查看已有目录
- 更换布局

约束与限制

- 系统内置的目录**不支持**编辑、删除操作。

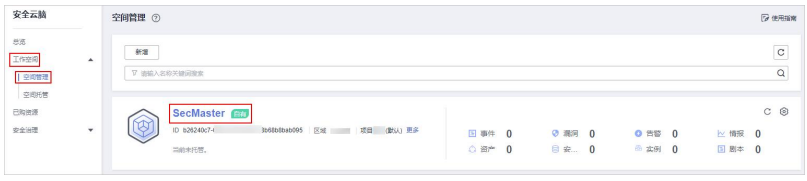
查看已有目录

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-57 进入目标工作空间管理页面



步骤 4 在左侧导航栏选择“设置 > 目录定制”，进入目录定制页面。

图 13-58 进入目录定制页面

步骤 5 在目录定制列表中，查看目录的详细信息。

表 13-18 目录参数说明

参数名称	参数说明
一级目录	目录所属的一级目录名称。
二级目录	目录所属的二级目录名称。
目录状态	目录所属的类型。
目录地址	目录所在地址。
布局	目录关联的布局。
发布者	目录的发布者。
操作	可对目录进行更换布局等操作。

----结束

更换布局

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 13-59 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“设置 > 目录定制”，进入目录定制页面。

图 13-60 进入目录定制页面

步骤 5 单击目标目录所在行“操作”列的“更换布局”，弹出更换布局页面。

步骤 6 在更换布局页面中，选择需要替换的布局。

步骤 7 单击“确定”。

----结束

14 常见问题

14.1 产品咨询

14.1.1 为什么没有看到攻击数据或者看到的攻击数据很少？

态势感知（专业版）支持检测云上资产遭受的各类攻击，并进行客观的呈现。

但是，如果您的云上资产在互联网上的暴露面非常少（所谓“暴露面”是指资产可被攻击或利用的风险点，例如，端口暴露和弱口令都可能成为风险点），那么遭受到攻击的可能性也将大大降低，所以，态势感知（专业版）可能会显示您的系统当前遭受的攻击程度较低。

14.1.2 态势感知（专业版）的数据来源是什么？

态势感知（专业版）基于云上威胁数据和云服务采集的威胁数据，通过大数据挖掘和机器学习，分析并呈现威胁态势，并提供防护建议。

- 一方面采集全网流量数据，以及安全防护设备日志等信息，通过大数据智能 AI 分析采集的信息，呈现资产的安全状况，并生成相应的威胁告警。
- 另一方面汇聚企业主机安全（Host Security Service，HSS）、Web 应用防火墙（Web Application Firewall，WAF）等安全防护服务上报的告警数据，从中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能 AI 分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

态势感知（专业版）通过对多方面的安全数据的分析，为安全事件的处置决策提供依据，实时呈现完整的全网攻击态势。

14.1.3 态势感知（专业版）与其他安全服务之间的关系与区别？

态势感知（专业版）与其他安全防护服务（WAF、HSS、Anti-DDoS、DBSS）的关系与区别如下：

- 关联：

  态势感知（专业版）：作为安全管理服务，依赖于其他安全服务提供威胁检测数据，进行安全威胁风险分析，呈现全局安全威胁态势，并提供防护建议。

  其他安全服务：威胁检测数据可以统一汇聚在态势感知（专业版）中，呈现全局安全威胁攻击态势。

- 区别：

  态势感知（专业版）：仅为可视化威胁检测和分析的平台，不实施具体安全防护动作，需与其他安全服务搭配使用。

  其他安全服务：仅展示对应服务的检测分析数据，并实施具体安全防护动作，不会呈现全局的威胁攻击态势。

态势感知（专业版）与其他安全防护服务区别，详细内容如表 14-1。

表 14-1 态势感知（专业版）与其他服务的区别

服务名称	服务类别	关联与区别	防护对象
态势感知（专业版）	安全管理	态势感知（专业版）着重呈现全局安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，并提供防护建议。	呈现全局安全威胁攻击态势。
Anti-DDoS 流量清洗（Anti-DDoS）	网络安全	Anti-DDoS 集中于异常 DDoS 攻击流量的检测和防御，相关攻击日志、防护等数据同步给态势感知（专业版）。	保障企业业务稳定性。
企业主机安全（HSS）	主机安全	HSS 着手于保障主机整体安全性，检测主机安全风险，执行防护策略，相关告警、防护等数据同步给态势感知（专业版）。	保障主机整体安全性。
Web 应用防火墙（WAF）	应用安全	WAF 服务对网站业务流量进行多维度检测和防护，防御常见攻击，阻断攻击进一步威胁。相关入侵日志、告警数据等同步给态势感知（专业版），呈现全网 Web 风险态势。	保障 Web 应用程序的可用性、安全性。
数据库安全服务（DBSS）	数据安全	DBSS 着力于数据库访问行为的防护和审计，相关审计日志、告警数据等同步给态势感知（专业版）。	保障云上数据库安全和资产安全。

14.1.4 态势感知（专业版）与 HSS 服务的区别？

服务含义区别

- 态势感知（专业版）是云原生的新一代安全运营中心，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。
- 主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了**主机**安全、**容器**安全和**网页防篡改**，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。

简而言之，态势感知（专业版）是呈现**全局**安全态势的服务，HSS 是提升**主机**和**容器**安全性的服务。

服务功能区别

- 态势感知（专业版）通过采集**全网安全数据**（包括 HSS、WAF、AntiDDoS 等安全服务检测数据），提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。
- HSS 通过在**主机**中安装 Agent，使用 AI、机器学习和深度算法等技术分析主机中风险，并从 HSS 云端防护中心下发检测和防护任务，全方位保障主机安全。同时可从可视化控制台，管理主机 Agent 上报的安全信息。

表 14-2 态势感知（专业版）与 HSS 主要功能区别

功能项		共同点	不同点
资产安全	主机资产	呈现主机资产的整体安全状态。	• 态势感知（专业版）：仅支持同步 HSS 主机资产风险信息，列表呈现各主机资产的整体安全状况。 • HSS：不仅支持呈现主机的安全状况，还支持深度扫描主机中的账号、端口、进程、Web 目录、软件信息和自启动任务。
	网站资产	-	• 态势感知（专业版）：支持检查和扫描网站安全状态，列表呈现各网站资产的整体安全状况。 • HSS：不支持该功能。
漏洞管理	主机漏洞	呈现主机漏洞扫描结果，管理主机漏洞。	• 态势感知（专业版）：仅支持同步 HSS 主机漏洞扫描结果，管理主机漏洞。 • HSS：支持检测 Linux 漏洞、Windows 漏洞、Web-CMS 漏洞、应用漏洞，提供漏洞概览，包括主机漏洞检测详情、漏洞统计、漏洞类型分布、漏洞 TOP5 和风险服务器 TOP5，帮助您实时了解主机漏洞情况。
基线检查	云服务基线	-	• 态势感知（专业版）：针对云服务关键配置项，从多种风险类别，了解云服务风险配置的所在范围和风险配置数目。 • HSS：不支持该功能。
	主机基线	-	• 态势感知（专业版）：不支持该功能。 • HSS：针对主机，提供基线检查功能，包括检测复杂策略、弱口令及配置详情，包括对主机配置基线通过率、主机配置风险 TOP5、主机弱口令检测、主机弱口令风险 TOP5 的统计。

14.1.5 如何更新安全评分？

态势感知（专业版）支持实时检测整体资产的安全状态，评估整体资产安全健康得分。通过查看安全评分，可快速了解未处理风险对资产的整体威胁状况。

资产安全风险修复后，为降低安全评分的风险等级，目前需手动忽略或处理告警事件，刷新告警列表中告警事件状态。告警事件状态刷新并启动重新检测后，安全评分将更新。

图 14-2 安全评分

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 14-3 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面，对不合格的基线检查项目进行处理。

步骤 5 在左侧导航栏选择“风险预防 > 漏洞管理”，进入漏洞管理页面，对漏洞进行处理。

步骤 6 在左侧导航栏选择“威胁运营 > 告警管理”，进入全部告警管理页面，对告警事件进行处理。

步骤 7 相应告警事件处理后，返回“安全态势 > 态势总览”页面，单击“重新检测”，检测后可查看更新的安全评分。

说明

由于检测需要一定的时间，请您在单击“重新检测”按钮**5分钟**后，再刷新页面，查看最新检测的安全评分。

----结束

14.1.6 如何处理暴力破解告警事件？

暴力破解是一种常见的入侵攻击行为，攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制，严重危害资产的安全。

态势感知（专业版）联动主机安全服务（HSS），接收 HSS 检测到的暴力破解行为，集中呈现和管理告警事件，提升运维效率。

处理告警事件

HSS 通过暴力破解检测算法和全网 IP 黑名单，若发现暴力破解主机的行为，对发起攻击的源 IP 进行拦截，并上报告警事件。

当接收到来源于 HSS 的告警事件时，请登录 HSS 管理控制台确认并处理告警事件。

- 若您的主机被爆破成功，检测到入侵者成功登录主机，账户下所有云服务器可能已被植入恶意程序，建议参考如下措施，立即处理告警事件，避免进一步危害主机的风险。
  a. 请立即确认登录主机的源 IP 的可信情况。
  b. 请立即修改被暴力破解的系统账户口令。
  c. 请立即执行检测入侵风险账户，排查可疑账户并处理。
  d. 请及时执行恶意程序云查杀，排查系统恶意程序。
- 若您的主机被暴力破解，攻击源 IP 被 HSS 拦截，请参考如下措施，加固主机安全。
  a. 请及时确认登录主机的源 IP 的可信情况。
  b. 请及时登录主机系统，全面排查系统风险。
  c. 请根据实际需求升级 HSS 防护能力。
  d. 请根据实际情况加固主机安全组、防火墙配置。

标记告警事件

告警事件处理完成后，您可以根据处理情况，标记已识别的告警事件，加强对告警事件的管理。

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 14-4 进入目标工作空间管理页面

步骤 4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警列表管理页面。

步骤 5 选择“暴力破解”类型，刷新告警列表。

步骤 6 选择目标告警，根据实际情况删除无威胁告警事件。

----结束

14.1.7 数据同步/一致性相关问题

为什么 WAF、HSS 中的数据和态势感知（专业版）中的数据不一致？

由于态势感知（专业版）中汇聚了 WAF、HSS 上报的所有历史告警数据，而 WAF 和 HSS 中展示的是实时告警数据，导致存在态势感知（专业版）与 WAF、HSS 中数据不一致的情况。

因此，建议您前往对应服务（WAF 或 HSS）进行查看并处理。

为什么总览页面中没有显示资产总数？

问题现象：

工作空间新增完成后，在工作空间内的“资产管理”页面中同步并已显示资产信息，但是“总览”页面中的资产总数仍然显示为 0。

问题原因：

工作空间创建成功，且资产等数据信息接入完成后，态势感知（专业版）将在**整点**进行数据同步，请耐心等待同步后再进行查看。

解决方法：

请您耐心等待，同步会系统将更新资产等相关数据信息。

14.1.8 Agent 安装失败问题排查

数据采集时，需要在 ECS 上安装 Agent，当出现安装失败等问题时，请参照本章节进行排查处理：

可能原因

Agent 安装失败的可能原因如下：

- 待安装 Agent 的 ECS 服务器与存储 Agent 的 OBS 桶之间网络不通

- ECS 服务器的磁盘空间不足
- 调用 iamtoken 请求，获取 iamtoken 失败
- workspaceId 校验失败
- Agent 已经安装，系统仍将重复安装

原因排查及解决方法

- **待安装 Agent 的 ECS 服务器与存储 Agent 的 OBS 桶之间网络不通**

  图 14-5 主机与 OBS 网络不通

  解决方法：

  - （可选）方法一：将 ECS 主机与 OBS 的网络连通。
  - （可选）方法二：手动将安装脚本以及安装包下载到本地后，再将安装包上传到主机的“/opt/cloud”路径下。
    i. 登录 OBS 管理控制台。
    ii. 在左侧导航栏选择“桶列表”，并单击目标桶名称，进入桶对象管理页面。
    iii. 单击目标桶对象名称，进入桶对象详情页面后，下载安装脚本和安装包。
    iv. 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
    v. 将安装包上传到主机的“/opt/cloud”路径下。

- **ECS 主机的磁盘空间不足**

  图 14-6 磁盘空间不足

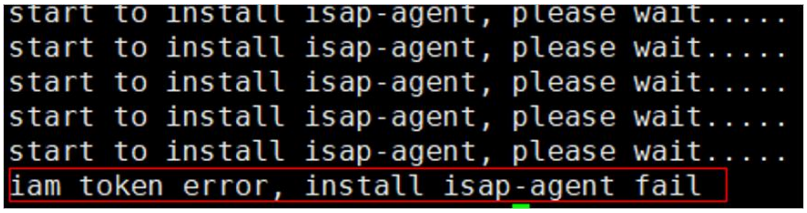
  解决方法：

  清理磁盘，预留足够空间。

- **调用 iamtoken 请求，获取 iamtoken 失败**
  - **问题现象**

    当日志出现如下图所示信息时，则表示调用 iamtoken 请求，获取 iamtoken 失败。

图 14-7 获取 iamtoken 失败



- **排查步骤和解决方法**

  i. 确认执行命令中的 IAM 账号或用户名是否有误。

  图 14-8 IAM 用户名和密码

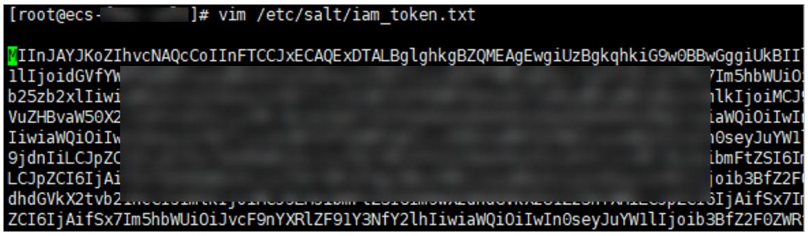
  

  - □ 有误，修改命令中的 IAM 账号或用户名后再次执行安装命令。
  - □ 无误，继续执行 ii。

  ii. 执行 **vim /etc/salt/iam_token.txt** 命令，查看“/etc/salt/iam_token.txt”文件检查是否存在。

  - □ 当出现如下图信息时，则表示存在，继续执行 iii。

  图 14-9 检查文件

  - □ 如果提示文件不存在，请联系技术支持进行处理。

  iii. 执行 **ping** 命令，检查主机是否可以连通网络地址，如果不通，用户需要打通网络。

  图 14-10 检查网络

- **workspaceId 校验失败**

  - **问题现象**

    当日志出现如下图所示信息时，则表示 Workspace ID 校验失败。

图 14-11 workspaceId 校验失败

```
start to install isap-agent, please wait.....
start to install isap-agent, please wait.....
start to install isap-agent, please wait.....
start to install isap-agent, please wait.....
start to install isap-agent, please wait.....
workspaceId error, install isap-agent fail
```

- **解决方法**

  i. 登录态势感知（专业版）管理控制台。

  ii. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

  iii. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点名称。

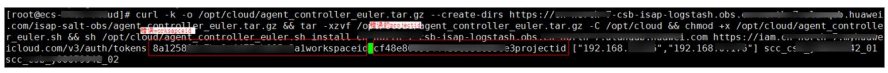
  iv. 查看执行命令中的 workspaceId 和 projectId。

  图 14-12 控制台中的参数信息

  v. 查看实际运行命令中的 workspaceId 和 projectId，是否与 iv 中的一致。

  图 14-13 命令中的参数信息

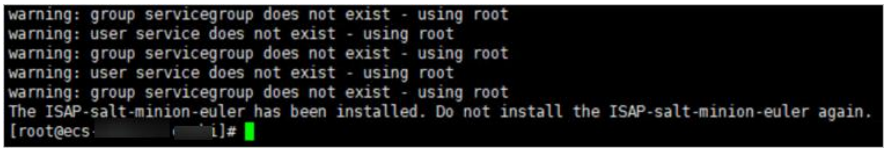
  vi. 修改实际执行命令中的 workspaceId 和 projectId。

- **Agent 已经安装，系统仍将重复安装**

  - **问题现象**

    当日志出现如下图所示信息时，则表示 Agent 已经安装。

图 14-14 Agent 重复安装



- **解决方法**

  i. （可选）方法一：通过管理控制台注销该节点。

  1) 登录态势感知（专业版）管理控制台。

  2) 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

  3) 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点所在行“操作”列的“注销”。

  4) 在弹出的确认框中，单击“确认”

  ii. （可选）方法二：通过脚本命令卸载 Agent。

  1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。

  2) 执行 **sh /opt/cloud/agent_controller_euler.sh uninstall** 命令，卸载 Agent。

  iii. 检查是否已完成卸载。

  1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。

  2) （可选）方法一：执行 **ls -a /opt/cloud/**查看“/opt/cloud”目录下的文件，当提示如下图所示信息（只有脚本文件）时，则表示已完成卸载。

  图 14-15 脚本文件

  3) （可选）方法二：执行 **salt-minion --version** 命令，当提示如下图所示信息时，则表示已卸载完成。

  图 14-16 检查 Agent 信息

⚠ 注意

节点注销需要一定的时间，不建议点完注销立刻安装。

14.2 购买咨询

14.2.1 态势感知（专业版）如何收费？

态势感知（专业版）服务提供包年/包月和按需计费的计费模式。

- 包年/包月

  购买时长越久越便宜，包周期计费按照订单的购买周期来进行结算。

- 按需计费

  按小时计费，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

14.2.2 态势感知（专业版）支持退订吗？

若用户不再使用态势感知（专业版）防护功能或增值包，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购 5 天内的资源，支持每年 10 次 5 天无理由“退订”；使用超过 5 天的资源，“退订”需要收取手续费。
- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

退订包周期计费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤 4 针对包周期购买的资产配额、或增值包，单击“退订”，进入“退订管理”列表页面。

步骤 5 在需要退订的实例所在行，单击“操作”列中的“退订资源”，进入“退订资源”页面。

步骤 6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤 7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

14.2.3 态势感知（专业版）即将到期，如何续费？

态势感知（专业版）续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不能变更版本规格，即不能改变“主机配额”。

续费操作仅针对包周期版本。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期版本到期时，用户需通过续费延长使用期。

- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤 1 登录管理控制台。

步骤 2 单击页面左上方的 ☰，选择“安全 > 态势感知（专业版）”，进入态势感知（专业版）管理页面。

步骤 3 在左侧导航栏选择“已购资源”，进入已购资源页面后，在待续费态势感知（专业版）版本所在 region 栏中，单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤 4 在态势感知（专业版）实例所在行，单击“续费”，跳转至“续费”页面。

步骤 5 配置“续费时长”，如选择“一年”。

步骤 6 （可选）设置并勾选“统一到期时间”。默认将统一到期时间设置为每月 1 号 23:59:59 GMT+08:00。

步骤 7 单击“去支付”，跳转至支付页面，完成付款。

步骤 8 返回续费管理页面，可查看态势感知（专业版）已续费成功。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本的资产配额、增值包、安全编排将自动续费，延长使用周期。

步骤 1 登录管理控制台。

步骤 2 单击“费用与成本 > 续费管理”，跳转至费用中心“续费管理”页面。

步骤 3 在“手动续费项”页签，选择态势感知（专业版）专业版实例，单击“开通自动续费”，跳转至自动续费配置页面。

步骤 4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤 5 单击“开通”，完成自动续费配置。

步骤 6 返回续费管理页面，在“自动续费项”页签，可查看态势感知（专业版）已开通自动续费。

后续将根据配置，自动续费延长使用期。

----结束

14.2.4 态势感知（专业版）到期后，会继续收费吗？

态势感知（专业版）到期后，不会继续收费。

若到期后，未及时续费，会根据“客户等级”和“订购方式”定义不同的保留期时长，保留期内不能访问及使用态势感知（专业版）资源，但对存储在态势感知（专业版）资源中的数据仍予以保留。

若保留期到期后，仍未及时续费，专业版会变为基础版。

14.2.5 如何修改或取消态势感知（专业版）自动续费？

态势感知（专业版）开通自动续费后，如果需要取消或修改，可参照本章节进行处理。

取消态势感知（专业版）自动续费

态势感知（专业版）开通自动续费后，支持取消自动续费操作。关闭自动续费后，版本到期将恢复为手动续费。

修改态势感知（专业版）自动续费

态势感知（专业版）开通自动续费后，支持修改续费配置，包括修改续费设定、修改自动续费周期、重置自动续费次数等。

14.2.6 态势感知（专业版）可以免费使用吗？

态势感知（专业版）（新版）提供暂不支持免费使用，可以选择包周期或按需计费购买。

A 修订记录

发布日期	修改记录
2024-5-30	第一次正式发布。