安全云脑

用户指南

文档版本 02

发布日期 2023-09-20

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2023。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

 版权所有 © 华为云计算技术有限公司

1 产品介绍

1.1 什么是安全云脑

安全云脑（SecMaster）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 功能特性

安全云脑基于云原生安全，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。

版权所有 © 华为云计算技术有限公司

工作空间管理

工作空间属于安全云脑顶层工作台，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	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。

安全态势

支持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。

表 1-3 安全态势功能介绍

功能模块		功能详情
态势总览	安全评分	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。
安全大屏		利用AI技术将海量云安全数据的分析并分类，通过安全大屏将数据可视化展示，集中呈现云上实时动态，云上关键风险一目了然，掌握云上安全态势更简单，更直观，更高效。
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

安全云脑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 1-4 资产管理功能说明

功能模块	功能详情
资源管理	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。

版权所有 © 华为云计算技术有限公司

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。
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。

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 1-5 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。

版权所有 © 华为云计算技术有限公司

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 1-6 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 1-7 数据集成功能说明

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 1-8 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。

版权所有 © 华为云计算技术有限公司

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”，安全云脑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。

版权所有 © 华为云计算技术有限公司

1.5 计费说明

计费项

安全云脑的**专业版**按选购的资产配额数和增值包计费，其中**增值包**功能为可选增值项目。

表 1-9 计费项说明

版本	计费项	计费说明
专业版	资产配额	按购买的资产配额数计费，包括主机资产配额数和网站资产配额数。
	按需购买计费	即开即停，按小时结算。
增值包	安全大屏	按实际使用时长计费。 **增值项**。若有安全大屏展示需求，您需在已购买资产配额基础上，**额外付费**购买。
	智能分析配额	按实际使用流量计费。 **增值项**。若有智能检索分析需求，您需在已购买资产配额基础上，**额外付费**购买。
	安全编排	按实际使用次数计费。 **增值项**。若有安全编排与响应需求，您需在已购买资产配额基础上，**额外付费**购买。

计费模式

安全云脑的计费模式为按需计费。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。
- 开通**增值包**功能

  当您需要**安全大屏**、**智能分析**、**安全编排**功能时，可在原有资产配额基础上，追加“安全大屏”、“智能分析”、“安全编排”功能。

须知

增值包中的“安全大屏”、“智能分析”、“安全编排”为专业版额外选购付费项目，如需使用，请先购买专业版。

版权所有 © 华为云计算技术有限公司

1.6 SecMaster 权限管理

如果您需要对云服务平台上创建的安全云脑（SecMaster）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云服务资源的访问。

通过IAM，您可以在帐号中给员工创建IAM用户，并授权控制他们对云服务资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有安全云脑（SecMaster）的使用权限，但是不希望他们拥有删除SecMaster等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用SecMaster，但是不允许删除SecMaster的权限，控制他们对SecMaster资源的使用范围。

如果帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用SecMaster的其它功能。

IAM是云服务平台提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**IAM产品简介**。

SecMaster 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

SecMaster部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问SecMaster时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云服务平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对SecMaster服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

如**表1-10**所示，包括了SecMaster的所有系统权限。

表 1-10 SecMaster 系统权限

系统角色/策略名称	描述	类别	依赖关系
SecMaster FullAccess	安全云脑的所有权限。	系统策略	无

版权所有 © 华为云计算技术有限公司

系统角色/策略名称	描述	类别	依赖关系
SecMaster ReadOnlyAccess	安全云脑只读权限，拥有该权限的用户仅能查看安全云脑数据，不具备安全云脑配置权限。	系统策略	无

1.7 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。

1.8 相关概念

本节介绍安全云脑相关概念。

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。对于安全云脑来讲，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）属于安全云脑顶层工作台，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。

版权所有 © 华为云计算技术有限公司

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

用于订阅安全云脑管道消息，一个管道可由多个订阅器进行订阅，安全云脑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，负责通过订阅器把安全云脑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。

 版权所有 © 华为云计算技术有限公司

2 服务委托授权

当您**首次**使用安全云脑时，需要先进行授权，才能正常访问，如果已经授权，请跳过该步骤。

前提条件

- 已完成IAM帐号授权操作，详细操作请参见**如何给IAM子帐号授权?** 。
- 已购买安全云脑。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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。

 版权所有 © 华为云计算技术有限公司

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

版权所有 © 华为云计算技术有限公司

3 版本管理

3.1 购买增值包

安全云脑在专业版的基础上，增加了增值包功能，请根据您的需要进行选购。

约束与限制

- 增值包为专业版额外选购付费项目，如需使用增值包，**须**先购买专业版。

按需方式购买增值包

步骤1 在左侧导航栏选择“已购资源”，进入已购资源页面后，单击页面右上角“购买增值包”，跳转到安全云脑购买页面。

步骤2 在购买安全云脑页面，配置购买参数。

1. 选择计费模式、区域和项目。
   - “计费模式”：此处选择“按需”，从开通开始到取消结束，按实际防护情况计费。
   - “区域”：选择您所在的区域。
2. “已配置”：显示已选择region安全云脑版本信息，无需配置。
3. 请根据您的需要选择对应增值包功能：

图 3-1 按需购买增值包

 版权所有 © 华为云计算技术有限公司

表 3-1 购买增值包

功能	购买	暂不购买
安全大屏	单击安全大屏后的  按钮，开启安全大屏，当状态显示为  则表示需要购买	保持  状态即可
智能分析配额	选择智能分析配额后的“现在购买”	请选择“暂不购买”
安全编排	选择安全编排后的“现在购买”	请选择“暂不购买”

步骤3 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤4 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤5 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

3.2 增加配额

购买安全云脑资产配额完成后，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。
- 在购买安全云脑时，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。

按需方式

步骤1 在左侧导航栏选择“已购资源”，并在对应区域栏单击“增加配额”，跳转到购买安全云脑页面。

步骤2 在购买安全云脑页面中查看当前配置，并配置“主机配额”。

主机配额，在原有配额数基础上，增加的资产配额数。

步骤3 配置完成后，单击“去支付”。

步骤4 返回安全云脑控制台页面，即可对相应配额数的主机进行安全防护。

----结束

3.3 退订

若用户不再使用安全云脑防护功能或增值包，可执行退订或一键取消操作。

 版权所有 © 华为云计算技术有限公司

- 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。

约束与限制

- **按需计费**的专业版中，退订/取消专业版资产配额时，增值包功能将一并退订/取消。

取消按需计费

步骤1 在“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤2 针对按需购买的版本或增值包，单击“取消”，一键释放按需计费的资产配额。

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

退订增值包

步骤1 在“总览”页面，单击右上角“专业版”，显示版本管理窗口。

步骤2 单击“取消”，一键释放按需计费的资产配额。返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

 版权所有 © 华为云计算技术有限公司

4 安全总览

4.1 总览

安全云脑“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。在“总览”查看安全概览信息和相关一键操作，实现云上安全态势一览和风险统一管控。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“总览”，进入安全云脑总览页面。

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**

----结束

安全评分

“安全评分”板块根据安全云脑的威胁检测能力，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。

版权所有 © 华为云计算技术有限公司

图 4-1 安全评分

- 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 4-2 安全监控

版权所有 © 华为云计算技术有限公司

表 4-1 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**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。 ● 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。
漏洞	展示您资产中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。 ● 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。

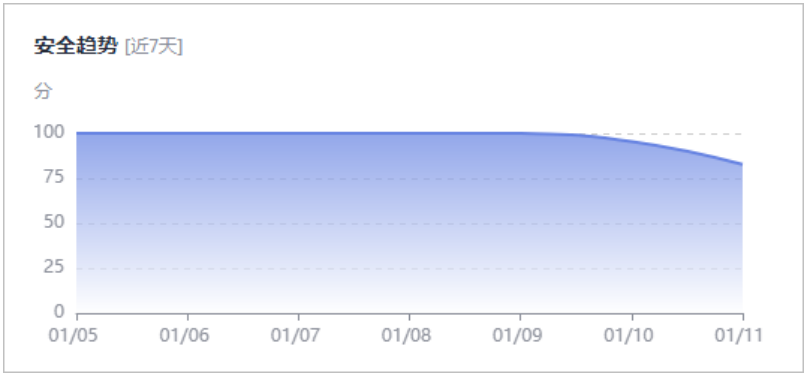
版权所有 © 华为云计算技术有限公司

参数名称	参数说明
合规检查	展示您资产中**近30天内**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。 ● 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**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。

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。

图 4-3 安全趋势



4.2 安全评分

安全云脑实时呈现您云上资产的整体安全评估状况，并根据安全云脑的威胁检测能力，评估整体资产安全健康得分。

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

SecMaster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”。

版权所有 © 华为云计算技术有限公司

- 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，安全评分实时更新。

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 4-2 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。
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4-3所示。

表 4-3 安全评分扣分项

分类	扣分项	单项扣分项	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		

版权所有 © 华为云计算技术有限公司

分类	扣分项	单项扣分项	处理建议	最高扣分上限
	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		

版权所有 © 华为云计算技术有限公司

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）属于安全云脑顶层工作台，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。

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

- 单帐号单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

工作空间（Workspace）属于安全云脑顶层工作台，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。

在安全云脑前，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。

 版权所有 © 华为云计算技术有限公司

约束与限制

单帐号单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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间页面。

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。

图 5-2 新增工作空间

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。
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，或者权限为企业主帐号的客户才可见。 **说明** “default”为默认企业项目，帐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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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 管理工作空间

5.3.1 查看工作空间详情

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。

查看工作空间

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间管理页面。

图 5-3 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 5-4 工作空间详情

版权所有 © 华为云计算技术有限公司

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。
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 5-5 工作空间基本信息

----结束

5.3.2 编辑工作空间

工作空间新增成功后，您可以对工作空间**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。

编辑工作空间

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

版权所有 © 华为云计算技术有限公司

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间管理页面。

图 5-6 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 5-7 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

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“工作空间 > 空间管理”，进入安全云脑工作空间管理页面。

图 5-8 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。

版权所有 © 华为云计算技术有限公司

图 5-9 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。

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。

步骤7 单击页面右下角“删除”。

----结束

版权所有 © 华为云计算技术有限公司

6 查看已购资源

在安全云脑的已购资源中可统一呈现当前帐号已经申请的资源，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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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：当前帐号已开通云脑的区域。
  - 可升级：当前帐号的所有已申请版本中，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：当前帐号已申请的总配额数量。
- 各区域具体申请安全云脑资源的详细情况。

----结束

 版权所有 © 华为云计算技术有限公司

7 安全态势

7.1 态势总览

“态势总览”页面实时呈现当前工作空间中资源整体安全评估状况。在“态势总览”查看安全概览信息和相关一键操作，实现云上安全态势一览和风险统一管控。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-1 工作空间页面

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**

----结束

版权所有 © 华为云计算技术有限公司

安全评分

“安全评分”板块根据安全云脑的威胁检测能力，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 7-2 安全评分

- 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

安全云脑实时呈现您资产的整体安全评估状况，并根据安全云脑的威胁检测能力，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
  根据安全云脑的威胁检测能力，评估整体资产安全健康得分。

版权所有 © 华为云计算技术有限公司

- 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，安全评分实时更新。

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 7-1 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7-2所示。

表 7-2 安全评分扣分项

分类	扣分项	单项扣分项	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		

版权所有 © 华为云计算技术有限公司

分类	扣分项	单项扣分项	处理建议	最高扣分上限
	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		

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 7-3 安全监控

版权所有 © 华为云计算技术有限公司

表 7-3 安全监控参数说明

参数名称	参数说明
威胁告警	呈现最**近7天内**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。 ● 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。
漏洞	展示您资产中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。 ● 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。

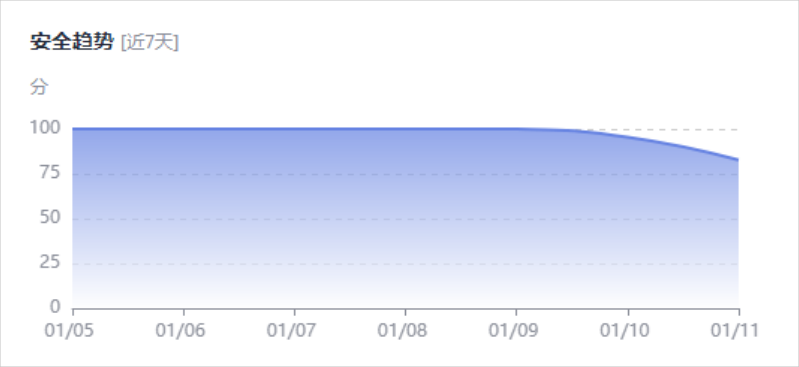
 版权所有 © 华为云计算技术有限公司

参数名称	参数说明
合规检查	展示您资产中**近30天内**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。 ● 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。

图 7-4 安全趋势



7.2 安全大屏

7.2.1 综合态势感知大屏

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

版权所有 © 华为云计算技术有限公司

安全云脑默认提供一个**综合态势感知大屏**，可以还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力，实现一屏全面感知。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-5 工作空间页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击“综合态势感知”图片，进入综合态势感知大屏信息页面。

页面中各个模块的功能介绍和使用方法详见下述内容。

----结束

安全评分

展示当前资产安全健康得分。

- 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”。

告警统计情况

展示已接入服务的告警统计情况。

- 新增告警：呈现**当天**新增的告警总数。
- 威胁告警：呈现**近7天内**威胁告警数量。
- 待解决告警：呈现**近7天内**待解决的告警数量。
- 已解决告警：呈现**近7天内**已解决的告警数量。

资产防护率

展示主机和网站的防护情况，包含已防护和未防护资产的比例。将鼠标悬停在对应模块上，可以查看已防护/未防护资产数量。

版权所有 © 华为云计算技术有限公司

基线合规

展示当前资产基线配置和漏洞修复情况、基线扫描后的风险资源分布情况和近7天内漏洞修复的趋势。

- **配置基线**：呈现**最近一次**执行基线检查后，基线配置情况统计情况，即基线配置通过和不通过的配置项目数量。
- **漏洞处理**：呈现**近7天内**已接入服务在基线检查中的漏洞修复统计情况，包括已修复、未修复漏洞的数量。
- **风险资源分布**：呈现**最近一次**执行基线检查的风险资产分布情况以及风险资产的数量。风险等级分为：致命、高危、中危、低危、提示几个级别。
- **漏洞趋势**：呈现**近7天内**已接入服务在基线检查中的漏洞分布趋势。

威胁态势

展示**近7天内**每日受到威胁的资产的数量和日志访问量，威胁态势的横坐标表示时间，左侧纵坐标表示受威胁资产的数量，右侧纵坐标表示受威胁访问的日志量。将鼠标箭头置于某个日期上，可以看到该日受威胁的资产总数和日志量大小。

待办工单

展示当前工作空间内的待办事项。

响应闭环

展示告警处置情况、近7天内SLA和MTTR达成率和近7天内事件自动处置统计情况。

- **告警总数**：呈现已接入服务的告警总数。
- **处置数**：呈现**近7天内**已关闭的告警总数。
- **及时处置数**：呈现及时处理了的告警总数，即在告警设置的SLA时间内完成了处理的告警总数。
- **自动处置数**：呈现被剧本自动处理并关闭了的告警总数。
- **7天SLA和MTTR**：呈现**近7天内**告警处理的SLA统计分析情况和MTTR平均响应时间。
  - **SLA（计划关闭时间）统计分析情况**：呈现**近7天内**告警处理的时效满足情况。计算方法如下：

    已设置了SLA字段的告警，当告警关闭事件-告警产生时间≤设置的SLA时间时，则表示满足，反之则表示不满足。
  - **MTTR（平均恢复时间）平均响应时间**：表示**近7天内**平均告警关闭时间。计算方法如下：

    MTTR=每个告警的处理时间总和/告警总数，其中，每个告警的处理时间=关闭时间-创建时间。
- **7天事件自动处置统计**：呈现**近7天内**告警被剧本自动处理了的告警统计总数。

7.2.2 值班响应大屏

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

 版权所有 © 华为云计算技术有限公司

安全云脑默认提供一个**值班响应大屏**，可以查看未处理告警、事件、漏洞、基线的总览情况，实现一屏全面感知。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-6 工作空间页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击“值班响应大屏”图片，进入值班响应大屏信息页面。

页面中各个模块的功能介绍和使用方法详见下述内容。

----结束

值班响应大屏总览

展示未处理告警、事件、漏洞、基线的总数。

未处理告警

列表呈现TOP5的未处理威胁告警事件的信息，包括告警发现时间、威胁告警描述信息、告警等级、告警所属的类型。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

未处理事件

列表呈现TOP5的未处理事件的信息，包括事件发现时间、事件描述、事件等级、事件所属类型。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

未处理漏洞

列表呈现TOP5的未处理漏洞的信息，包括漏洞发现时间、漏洞描述、漏洞类别、漏洞等级、受影响资产数。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

版权所有 © 华为云计算技术有限公司

未处理基线

列表呈现TOP5的未处理基线的信息，包括基线发现时间、基线描述、基线检查项目的检查方式、受影响的资源总数。

TOP5是根据创建时间降序来排序的，即最新的时间排在最前，以此往下进行排序。

7.2.3 资产大屏

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**资产大屏**，可以查看资产总数、受攻击资产数、未防护资产数等总览情况，实现一屏全面感知。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-7 工作空间页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击“资产大屏”图片，进入资产大屏信息页面。

页面中各个模块的功能介绍和使用方法详见下述内容。

----结束

资产大屏总览

展示资产、受攻击资产、未防护资产、漏洞和弱配置资产的总数。

- 资产总数：当前帐号当前工作空间内的资产总数。
- 受攻击资产数：当前帐号当前工作空间内存在告警的资产总数。
- 未防护资产数：当前帐号当前工作空间内的资产中未进行防护资产的总数。例如，ECS资产未开启主机防护功能。
- 漏洞和弱配置资产数：当前帐号当前工作空间内存在漏洞、待处理基线检查问题或未进行防护资产总数（重复资产不会重复统计）。

版权所有 © 华为云计算技术有限公司

资产分布情况

呈现资产类型的分布情况、资产防护率统计情况、资产变化趋势和TOP5受攻击资产所在区域分布情况。

- 资产类型分布：当前帐号当前工作空间内不同资产类型的分布情况。
- 资产防护率统计：当前帐号当前工作空间内不同资产类型的防护率统计情况。
- 资产变化趋势：近7天当前帐号当前工作空间内资产变化趋势和脆弱性资产变化趋势。
- TOP5 受攻击资产：当前帐号当前工作空间内TOP5受攻击资产及其被攻击次数。

TOP5 漏洞数最多资产和 TOP5 资产防护率

列表呈现当前时间TOP5漏洞数量最多的资产和TOP5部门名下的资产防护率。

- TOP5 漏洞数最多资产：当前时间，漏洞数TOP5的资产，包含资产IP、所属部门和漏洞个数统计。
- TOP5 资产防护率：当前时间，TOP5部门名下的资产防护率，包括不同部门资产防护率、WAF防护率、主机防护率、漏洞修复率。

  TOP5是根据资产防护率排序的，即防护率最低排在最前，以此往下进行排序

7.2.4 威胁态势大屏

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**威胁态势大屏**，可以查看网络攻击次数、应用拦截次数、主机层拦截次数等总览情况，实现一屏全面感知。

操作步骤

步骤1 单击“威胁态势大屏”图片，进入威胁态势大屏信息页面。

页面中各个模块的功能介绍和使用方法详见下述内容。

----结束

威胁态势大屏总览

展示当前帐号内资产的网络日志攻击次数、应用日志攻击次数和主机日志攻击次数。

- 网络日志攻击次数：近7天网络攻击次数总量。另外，还展示了近7天每日网络攻击次数，以及近7天网络攻击次数总量较上一个7天的变化。
- 应用日志攻击次数：近7天应用攻击次数总量。另外，还展示了近7天每日应用攻击次数，以及近7天应用攻击次数总量较上一个7天的变化。
- 主机日志攻击次数：近7天主机攻击次数总量。另外，还展示了近7天每日主机攻击次数，以及近7天主机攻击次数总量较上一个7天的变化。

 版权所有 © 华为云计算技术有限公司

攻击来源分布情况

列表呈现TOP5的网络攻击和应用攻击来源的分布情况，包括被攻击的资产IP、所属部门以及个数。

- TOP5网络日志攻击来源分布：近7天告警次数Top5的网络攻击源IP、攻击源地区、告警次数。
- TOP5应用告警攻击来源分布：近7天告警次数Top5的应用攻击源IP、攻击源地区、告警次数。

攻击类型分布

呈现TOP5的网络攻击类型、TOP5的应用攻击类型、主机类型分布情况。

- TOP5网络告警攻击类型：近7天告警次数Top5的网络攻击类型。
- TOP5应用告警攻击类型：近7天告警次数Top5的应用攻击类型。
- TOP5主机告警攻击类型：近7天告警次数Top5的主机攻击类型。

威胁态势统计

当前帐号内资产的告警统计情况、日志分析总量及分布情况、模型检测总量及分布情况。

- 告警统计：
  - 日志条数：近7天日志流入总条数。
  - 威胁攻击数：近7天DDOS攻击次数、网络攻击次数、应用攻击次数和主机攻击次数的总和。
  - 告警数：近7天告警数总量。
  - 事件数：近7天事件数总量。
- 日志分析
  - 总日志量：当前总日志存储量，单位KB、MB、GB等。
  - 总日志量同上周环比：当前总日志存储量与七天前同一时间总日志存储量的环比。计算方法：（本期数-上期数）/上期数×100%。
  - 日志分析：近7天日志流入存储量Top5的日志源，在这七天每天的存储量。
- 模型监测统计：
  - 模型总数：全部告警模型数量。
  - 模型监测统计：近7天告警次数Top10的告警模型、及其对应告警数量。

7.2.5 脆弱性大屏

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将安全云脑服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**安全大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

安全云脑默认提供一个**脆弱性大屏**，可以查看脆弱性资产、漏洞、基线、未防护资产等总览情况，实现一屏全面感知。

 版权所有 © 华为云计算技术有限公司

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-8 工作空间页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

步骤5 单击“脆弱性大屏”图片，进入脆弱性大屏信息页面。

页面中各个模块的功能介绍和使用方法详见下述内容。

----结束

脆弱性大屏总览

展示脆弱性资产、漏洞、不合格基线、未防护资产的总数。

脆弱性资产表示当前时间存在未处理的漏洞、不合格的基线或未防护的资产。

TOP5 部门脆弱性统计

列表呈现脆弱性统计TOP5的部门，包括部门名称，该部门的脆弱性风险资产数量、未修复漏洞数和未防护资产数。

TOP5 部门未防护统计

列表呈现TOP5的部门未覆盖防护策略情况，包括部门的名称、未覆盖策略数、DBSS、WAF、DDoS、HSS、CFW。

TOP5是从部门索引取值，按未防护资产数降序排序。

漏洞修复率

展示漏洞修复率、TOP5 漏洞类型分布情况和漏洞趋势变化情况。

- 漏洞修复率：高危、中危、低危、提示漏洞修复率。
- TOP5 漏洞类型分布：TOP 5类型漏洞的具体分类及其数量。
- 漏洞趋势变化：高危、中危、低危、提示漏洞的变化趋势。

 版权所有 © 华为云计算技术有限公司

基线检查通过率

呈现基线检查通过率、基线自动检查不通过资源统计情况、基线检查不通过类型及其数量、基线检查总数等。

7.3 安全报告

7.3.1 创建/复制安全报告

安全云脑提供安全报告功能。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。

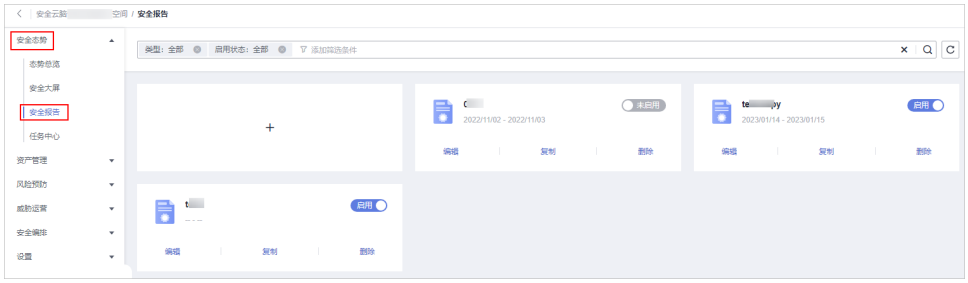
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-9 工作空间页面

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 7-10 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。

版权所有 © 华为云计算技术有限公司

表 7-4 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。
报告类型	选择报告类型。 • 日报：默认统计前一天0:00~24:00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。
报告周期	根据选择的报告类型自动生成报告的周期。

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。

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。

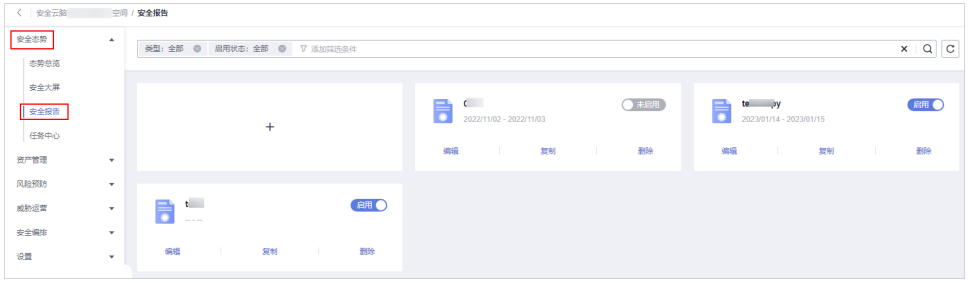
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-11 工作空间页面

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 7-12 进入安全报告页面



版权所有 © 华为云计算技术有限公司

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。

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

7.3.2 查看安全报告

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。

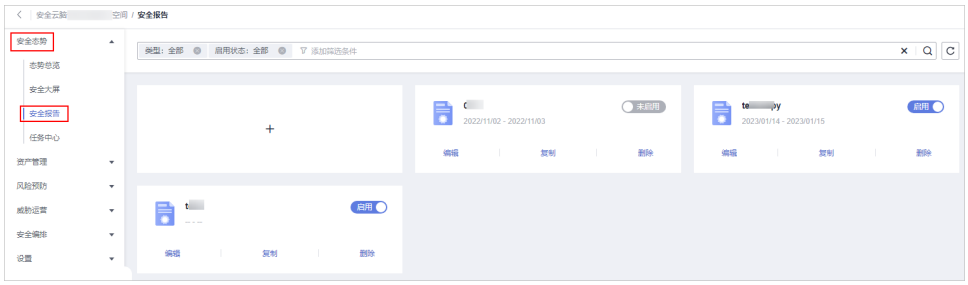
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-13 工作空间页面

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 7-14 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

版权所有 © 华为云计算技术有限公司

模板日报展示内容

- **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**

  根据您的安全云脑的威胁检测能力，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。

- **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。

- **安全响应**

 版权所有 © 华为云计算技术有限公司

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。

7.3.3 下载安全报告

安全云脑创建并生成报告后，可以将历史报告（PDF或.jpg格式）下载至本地。

操作步骤

步骤1 登录管理控制台。

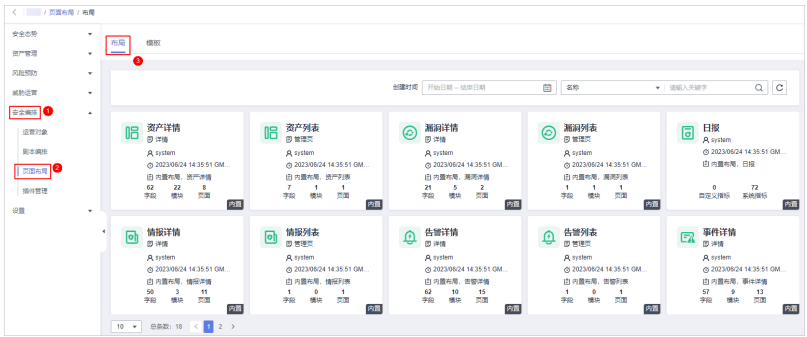
步骤2 单击页面左上方的 ，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-15 工作空间页面

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 7-16 进入布局管理页面



步骤5 在布局管理页面，将鼠标悬停在日报布局上，并单击布局右上角 ，进入布局配置页面。

步骤6 在布局编辑页面中，单击下载按钮。

系统将自动下载.jpg格式的安全报告到本地。

----结束

版权所有 © 华为云计算技术有限公司

7.3.4 管理安全报告

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。

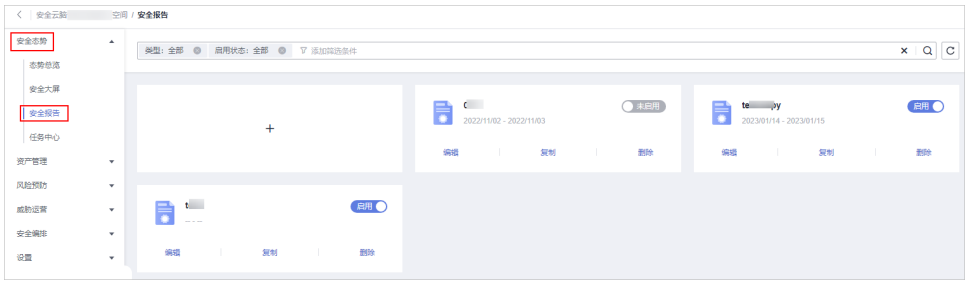
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-17 工作空间页面

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 7-18 进入安全报告页面



步骤5 管理安全报告。

表 7-5 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。

版权所有 © 华为云计算技术有限公司

操作名称	执行步骤
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

7.4 任务中心

7.4.1 查看待办任务

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-19 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 7-20 我的待办

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”或“任务名称”，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 7-6 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。
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

7.4.2 处理待办任务

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。

 版权所有 © 华为云计算技术有限公司

操作步骤

步骤1 登录管理控制台。

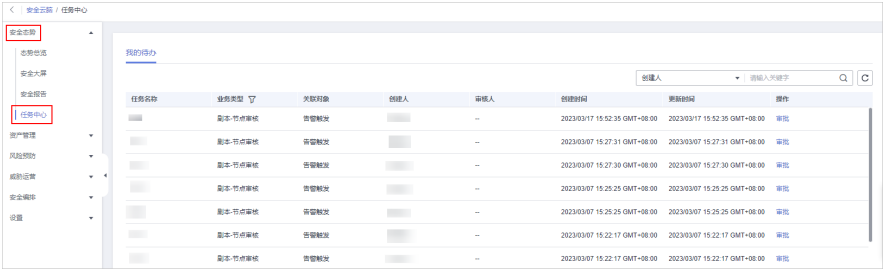
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 7-21 工作空间页面

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。

图 7-22 我的待办



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

版权所有 © 华为云计算技术有限公司

8 资产管理

8.1 资产管理简介

安全云脑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。

资产来源及对应的防护产品

表 8-1 资产来源及对应的防护产品

参数名称	来源	对应的安全防护产品
主机资产	弹性云服务器（Elastic Cloud Server，ECS）	企业主机安全（Host Security Service，HSS）
网站	Web应用防火墙（Web Application Firewall，WAF）	Web应用防火墙（Web Application Firewall，WAF）
数据库	云数据库（Relational Database Service，RDS）	数据库安全服务（Database Security Service，DBSS）
VPC	虚拟私有云（Virtual Private Cloud，VPC）	云防火墙（Cloud Firewall，CFW）
EIP	弹性公网IP（Elastic IP，EIP）	DDoS原生基础防护服务（Anti-DDoS流量清洗，Anti-DDoS）
设备	用户线下设备资产	--
说明： 如果在安全云脑控制台中的对应资产的“防护状态”显示“未防护”，表示未购买对应安全防护产品，且未开启防护；如果“防护状态”显示为“-”，表示对应的安全防护产品在该region不支持使用。		

版权所有 © 华为云计算技术有限公司

8.2 修改资产信息同步策略

新创建的工作空间资产同步策略**已自动开启**，资产相关信息会自动同步到安全云脑中（默认一小时同步一次）。

如果需要同步策略，请参照本章节进行处理。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

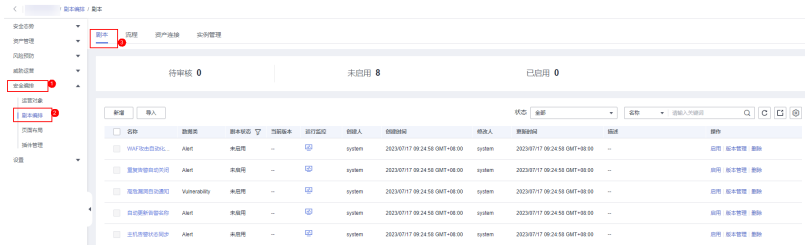
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 8-2 流程管理页面

步骤5 在“RDS资产连接器”、“VPC资产连接器”、“WebSite资产连接器”、“ECS资产连接器”、“EIP资产连接器”流程所在行“操作”列，单击“启用”，启用资产相关流程。

步骤6 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 8-3 进入剧本管理页面



版权所有 © 华为云计算技术有限公司

步骤7 新增剧本版本。

1. 在“资产连接器”剧本所在行“操作”列，单击“版本管理”，进入版本管理页面。
2. 在版本管理页面的“版本信息”模块中，单击v1版本所在行操作列的“复制”，并在弹出的确认框中单击“确认”。

图 8-4 复制版本

3. 单击新生成的草稿版本所在行操作列的“编辑”，右侧弹出编辑页面。
4. 在编辑页面的版本信息栏中，单击“触发条件”后的“新增条件”，弹出触发条件设置页面。

图 8-5 新增条件

5. 在触发条件页面中，设置需要调整的资产同步时间。

表 8-2 触发条件参数说明

参数名称	参数说明
开始时间	- 配置结束立即生效：剧本创建完成后立即生效。 - 选定时间：自定义剧本触发时间。
执行频率	- 只执行一次：在时间范围内，只执行一次，执行完成即结束。 - 重复执行：设置重复执行策略。设置执行时间每xx分钟/小时/天/周执行一次。 - 定时执行：在指定时间执行。设置执行时间为每天/每周的xx时xx分xx秒。
结束条件：	当“执行频率”设置为“重复执行”或“定时执行”时，需要配置该参数。 - 一直执行：该剧本任务无结束时间，创建完成后，将按照设置时间点一直执行。 - 选定时间：自定义剧本结束时间。

6. 单击页面右下角“确认”。
7. 确认无误后，单击页面右下角“确定”。

 版权所有 © 华为云计算技术有限公司

步骤8 提交剧本版本。

在“资产连接器”剧本的版本管理页面中，单击草稿版本所在行操作列的“提交”，并在弹出提交审核确认框中，单击“确认”。

步骤9 审核剧本版本。

在“资产连接器”剧本的版本管理页面中，单击草稿版本所在行操作列的“审核”，并在审核剧本版本页面，填写审核信息为通过后，单击页面右下角“确定”。

步骤10 启用剧本。

在剧本页面中，单击“资产连接器”剧本所在行“操作”列的“启用”，并在弹出启用确认信息框中单击“确认”。

启用成功后，系统将按照最新设置的同步策略进行同步。

----结束

8.3 查看资产信息

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。

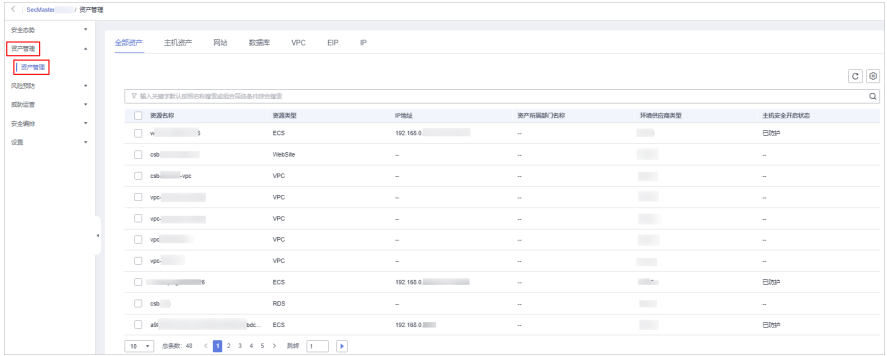
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 8-6 工作空间页面

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。

图 8-7 资产管理



 版权所有 © 华为云计算技术有限公司

步骤5 查看资源详细信息。

支持查看**全部资产**、**主机资产**、**网站**、**数据库**、**VPC**、**EIP**、**IP**资产的详细信息。

- 全部资产

  查看全部资产安全状态，相关说明如下所示：

  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。

  表 8-3 全部资产参数说明

参数名称	参数说明
资源名称	资源的名称。
资源类型	呈现资源所属的类型。例如：云服务器、磁盘、实例等。
IP地址	资源的IP地址。
资产所属部门名称	资源所在部门的名称。
环境供应商类型	资源的环境供应商所属的类型。
主机安全开启状态	资源是否开启主机安全防护。

- 主机资产

  查看主机资产信息，相关说明如下所示：

  表 8-4 主机资产参数说明

参数名称	参数说明
资源名称	主机的名称。
镜像名称	主机镜像的名称。
IP地址	主机的IP地址。
资产所属部门名称	主机所在部门的名称。
环境供应商类型	主机的环境供应商所属的类型。
主机安全开启状态	是否开启主机安全防护。
描述信息	主机描述信息。

- 网站

  查看网站资产信息，相关说明下所示：

 版权所有 © 华为云计算技术有限公司

表 8-5 网站参数说明

参数名称	参数说明
资源名称	网站名称。
域名服务器列表	域名所在服务器列表信息。
资产所属部门名称	域名所在部门的名称。
环境供应商类型	域名的环境供应商所属的类型。
WAF开启状态	域名是否开启WAF防护。

- 数据库
  查看数据库资产信息，相关说明如下所示：

  表 8-6 数据库参数说明

参数名称	参数说明
资源名称	数据库名称。
数据库引擎	数据库引擎类型。
外网IP地址	数据库的外网IP地址。
资产所属部门名称	数据库资源所在部门的名称。
环境供应商类型	数据库资源的环境供应商所属的类型。
开启状态	数据库资源是否开启数据库安全防护。
描述	数据库相关描述信息

- VPC
  查看VPC资产信息，相关说明如下所示：

  表 8-7 VPC 参数说明

参数名称	参数说明
资源名称	VPC的名称。
资源类型	VPC所属的类型。
子网范围	VPC子网的范围。
资产所属部门名称	VPC所在部门的名称。
环境供应商类型	VPC的环境供应商所属的类型。
保护状态	VPC资源是否开启保护。
描述	VPC的描述信息。

 版权所有 © 华为云计算技术有限公司

- EIP

  查看EIP资产信息，相关说明如下所示：

  表 8-8 EIP 参数说明

参数名称	参数说明
资源名称	EIP的名称。
公网IP地址	EIP的公网IP地址。
资产所属部门名称	EIP资源所在部门的名称。
环境供应商类型	EIP资源的环境供应商所属的类型。
状态	EIP的状态。
描述	EIP的描述信息

- IP

  查看IP资产信息，相关说明如下所示：

  表 8-9 IP 参数说明

参数名称	参数说明
资源名称	IP的名称。
资源类型	IP的类型。
资产值	IP的资产值
资产所属部门名称	IP资源所在部门的名称。
环境供应商类型	IP资源的环境供应商所属的类型。
资产备注	IP的备注信息。

----结束

8.4 导入/导出资产

安全云脑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，且文件大小不超过20MB。

 版权所有 © 华为云计算技术有限公司

导入资产

步骤1 登录管理控制台。

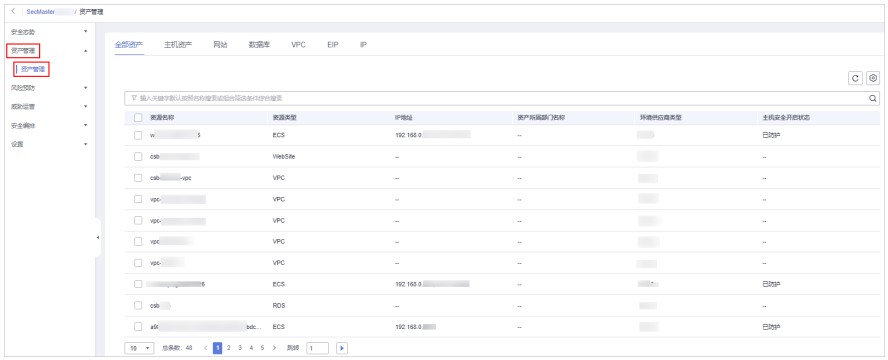
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 8-8 工作空间页面

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。

图 8-9 资产管理



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。

⚠ 注意

- 填写要求：请按照模板填写待导入资产信息，填写说明请参见**资产导入模板参数说明**。
- 文件格式：须为.xlsx。

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

版权所有 © 华为云计算技术有限公司

资产导入模板参数说明

导入资产需按照模板要求进行操作，资产导入模板参数说明请根据资产类型进行选择：

- **主机资产**
- **网站**
- **数据库**
- **VPC**
- **EIP**
- **IP**

说明

填写时，请勿修改表头。

表 8-10 主机资产

参数名称	类型	是否必填	参数说明
id	String	是	资产ID，长度要求为2-36个字符。
name	String	是	资产名称，长度要求为2-512个字符。
protected_status	String	否	选择主机安全开启状态。 • OPEN：已开启。 • CLOSE：未开启。
description	String	否	弹性云服务器的描述信息。
status	String	否	弹性云服务器状态。 取值范围如下： ACTIVE、BUILD、ERROR、HARD_REBOOT、MIGRATING、REBOOT、REBUILD、RESIZE、REVERT_RESIZE、SHUTOFF、VERIFY_RESIZE、DELETED。
host_id	String	否	弹性云服务器所在主机的主机ID。
host_name	String	否	弹性云服务器所在主机的主机名称。
host_status	String	否	云服务器所在主机状态。可填写以下状态： • UP：服务正常。 • UNKNOWN：状态未知。 • DOWN：服务异常。 • MAINTENANCE：维护状态。 • 空字符串：弹性云服务器无主机信息。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
version	String	否	IP地址版本。 ● 4：代表IPv4。 ● 6：代表IPv6。
addr	String	否	IP地址。
type	String	否	IP地址类型。 fixed：代表私有IP地址。 floating：代表浮动IP地址
mac_addr	String	否	MAC地址。
port_id	String	否	IP地址对应的端口ID。
vpc_id	String	否	所属虚拟私有云的ID。
image_type	String	否	镜像类型，目前支持以下类型： ● 公共镜像：gold ● 私有镜像：private ● 共享镜像：shared
image_name	String	否	云服务器操作系统对应的镜像名称。
os_type	String	否	操作系统类型，取值为：Linux、Windows。
os_bit	String	否	操作系统位数，一般取值为“32”或者“64”。
resource_spec_code	String	否	云服务器对应的资源规格。
vendor_type	String	是	环境供应商。
domain_id	String	是	资产归属租户ID。
region_id	String	是	资产归属区域。
project_id	String	是	资产归属工程ID。
ep_id	String	否	资产归属的企业项目id。
ep_name	String	否	资产归属的企业项目名称。
vendor_name	String	是	包含资产探针或资产提供商。
idc_id	String	是	线下机房id。
idc_name	String	是	线下机房名称。
department_name	String	否	资产所属部门名称。
business_name	String	否	业务系统名称。

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
business_owner	String	否	业务系统责任人。
governance_user_type	String	否	资产治理责任人类型。
governance_user_name	String	否	资产治理责任人名称。

表 8-11 网站

参数名称	类型	是否必填	参数说明
value	String	是	网站名称。
domain_name	String	是	域名名称。
name_server	String	否	域名服务器列表。以英文逗号（","）分割，如：192.168.25.106,192.168.25.124
protected_status	String	否	WAF开启状态： ● OPEN：开启 ● CLOSE：关闭 如果不填，默认为CLOSE。
idc_id	String	是	线下机房ID。
idc_name	String	是	线下机房名称。
vendor_name	String	是	资产提供商。
department_name	String	否	资产所属部门名称。
business_name	String	否	业务系统名称。
business_owner	String	否	业务系统责任人。
governance_user_type	String	否	资产治理责任人类型。
governance_user_name	String	否	资产治理责任人名称。

 版权所有 © 华为云计算技术有限公司

表 8-12 数据库

参数名称	类型	是否必填	参数说明
id	String	是	实例ID。
name	String	是	创建的实例名称。
status	String	是	实例状态。取值如下： ● BUILD：实例正在创建。 ● ACTIVE：实例正常。 ● FAILED：实例异常。 ● FROZEN：实例冻结。 ● MODIFYING：实例正在扩容。 ● REBOOTING：实例正在重启。 ● RESTORING：实例正在恢复。 ● MODIFYING INSTANCE TYPE：实例正在转主备。 ● SWITCHOVER：实例正在主备切换。 ● MIGRATING：实例正在迁移。 ● BACKING UP：实例正在进行备份。 ● MODIFYING DATABASE PORT：实例正在修改数据库端口。 ● STORAGE FULL：实例磁盘空间满。
private_ips	String	是	实例内网IP地址列表。以英文逗号（","）分割，如：192.168.25.106,192.168.25.124
port	Integer	是	数据库端口号。 ● RDS for MySQL数据库端口设置范围为1024～65535（其中12017和33071被RDS系统占用不可设置）。 ● RDS for PostgreSQL数据库端口修改范围为2100～9500。 ● RDS for SQL Server实例的端口设置范围为1433和2100~9500（其中5355和5985不可设置。对于2017 EE、2017 SE、2017 Web版，5050、5353和5986不可设置）。
enable_ssl	Boolean	是	实例开启SSL标志。 ● true：表示实例已开启SSL。 ● false：表示实例未开启SSL。

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
type	String	是	实例类型，取值如下： ● Single：单机实例 ● Ha：主备实例 ● Replica：只读实例 ● Enterprise：分布式实例（企业版）
region	String	是	资产所属region。
db_user_name	String	是	默认用户名。
vpc_id	String	是	虚拟私有云ID。
subnet_id	String	是	子网的网络ID信息。
cpu	String	是	CPU大小，例如，1表示1U。
mem	String	是	内存大小（单位：GB）。
vendor_type	String	是	环境供应商。
domain_id	String	是	资产归属租户ID。
region_id	String	是	资产归属区域。
project_id	String	是	资产归属工程ID。
ep_id	String	否	资产归属的企业项目id。
ep_name	String	否	资产归属的企业项目名称。
vendor_name	String	是	包含资产探针或资产提供商。
idc_id	String	是	线下机房id。
idc_name	String	是	线下机房名称。
department_name	String	否	资产所属部门名称。
business_name	String	否	业务系统名称。
business_owner	String	否	业务系统责任人。
governance_user_type	String	否	资产治理责任人类型。
governance_user_name	String	否	资产治理责任人名称。

 版权所有 © 华为云计算技术有限公司

表 8-13 VPC

参数名称	类型	是否必填	参数说明
id	String	是	VPC的ID。
name	String	是	VPC名称。
protected_status	String	否	安全开启状态：OPEN或CLOSE。
description	String	否	虚拟私有云的描述信息。
cidr	String	是	VPC下可用子网的范围。
status	String	是	VPC对应的状态。取值范围： ● PENDING：创建中 ● ACTIVE：创建成功
vendor_type	String	是	环境供应商。
domain_id	String	是	资产归属租户ID。
region_id	String	是	资产归属区域。
project_id	String	是	资产归属工程ID。
ep_id	String	否	资产归属的企业项目id。
ep_name	String	否	资产归属的企业项目名称。
vendor_name	String	是	包含资产探针或资产提供商。
idc_id	String	是	线下机房id。
idc_name	String	是	线下机房名称。
department_name	String	否	资产所属部门名称。
business_name	String	否	业务系统名称。
business_owner	String	否	业务系统责任人。
governance_user_type	String	否	资产治理责任人类型。
governance_user_name	String	否	资产治理责任人名称。

表 8-14 EIP

参数名称	类型	是否必填	参数说明
id	String	是	唯一标识，UUID。

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
alias	String	否	弹性公网IP名称。
description	String	否	弹性公网描述。
protected_status	String	否	DDoS或CFW开启状态：OPEN或CLOSE。
project_id	String	是	项目id。
ip_version	Integer	是	IP版本信息。枚举值： ● 4 ● 6
public_ip_address	String	是	ip地址。
publicip_pool_name	String	是	弹性公网IP的网络类型，包括：公共池类型（如5_bgp/5_sbgp...）和用户购买的专属池。
status	String	是	弹性公网IP的状态。取值范围： ● FREEZED：冻结 ● BIND_ERROR：绑定失败 ● BINDING：绑定中 ● PENDING_DELETE：释放中 ● PENDING_CREATE：创建中 ● NOTIFYING：创建中 ● NOTIFY_DELETE：释放中 ● PENDING_UPDATE：更新中 ● DOWN：未绑定 ● ACTIVE：绑定 ● ELB：绑定ELB ● VPN：绑定VPN ● ERROR：失败
associate_instance_type	String	是	公网IP绑定的实例类型。取值范围： ● PORT ● NATGW ● ELB ● ELBV1 ● VPN ● null
associate_instance_id	String	是	公网IP绑定的实例ID。

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
create_time	String	是	资源创建UTC时间。 格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone
vendor_type	String	是	环境供应商。
domain_id	String	是	资产归属租户ID、
region_id	String	是	资产归属区域。
project_id	String	是	资产归属工程ID。
ep_id	String	否	资产归属的企业项目id。
ep_name	String	否	资产归属的企业项目名称。
vendor_name	String	是	包含资产探针或资产提供商
idc_id	String	是	线下机房id。
idc_name	String	是	线下机房名称。
department_name	String	否	资产所属部门名称。
business_name	String	否	业务系统名称。
business_owner	String	否	业务系统责任人。
governance_user_type	String	否	资产治理责任人类型。
governance_user_name	String	否	资产治理责任人名称。

表 8-15 IP

参数名称	类型	是否必填	参数说明
value	String	是	资产值。
version	String	是	资产类型： • ipv4 • ipv6
relative_value	String	否	相对值，如资产为ipv4，则为对应的ipv6。
network_public	Boolean	是	外网或内网。
network_partition	String	否	网络分区：OM/PSZ/DMZ。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
network_partition	String	否	网络平面（线下有自己的代号）。
network_vxlan_id	String	否	虚拟网络ID。
remark	String	否	资产备注。
name	String	否	资产名称，默认为资产值。
latitude	Float	否	纬度。
longitude	Float	否	经度。
city_code	String	是	城市编码，请按照标准城市编码填写。
country_code	String	是	国家编码，按照国际标准国家代码填写。
server_room	String	是	机房。
server_rack	String	是	机柜。
mac_addr	String	否	MAC地址。
important	String	是	重要等级。 ● 0：不重要 ● 1：重要。
idc_id	String	是	线下机房ID。
idc_name	String	是	线下机房名称。
vendor_name	String	是	资产提供商。
department_name	String	否	资产所属部门名称。
business_name	String	否	业务系统名称。
business_owner	String	否	业务系统责任人。
governance_user_type	String	否	资产治理责任人类型。
governance_user_name	String	否	资产治理责任人名称。

导出资产

步骤1 登录管理控制台。

 版权所有 © 华为云计算技术有限公司

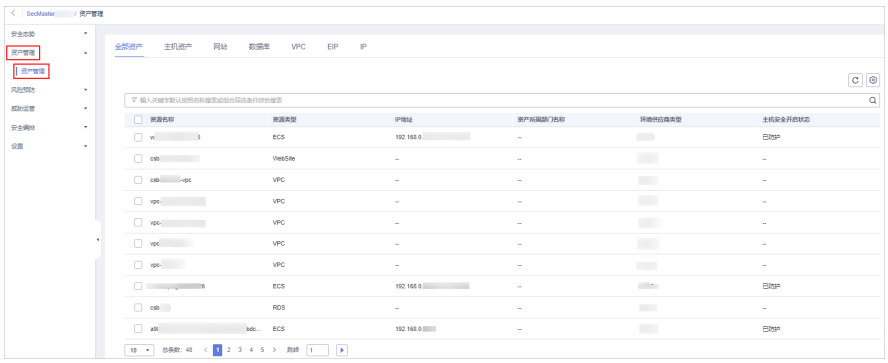
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 8-10 工作空间页面

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。

图 8-11 资产管理



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 8-16 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

版权所有 © 华为云计算技术有限公司

8.5 删除资产

如果不再需要在安全云脑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。

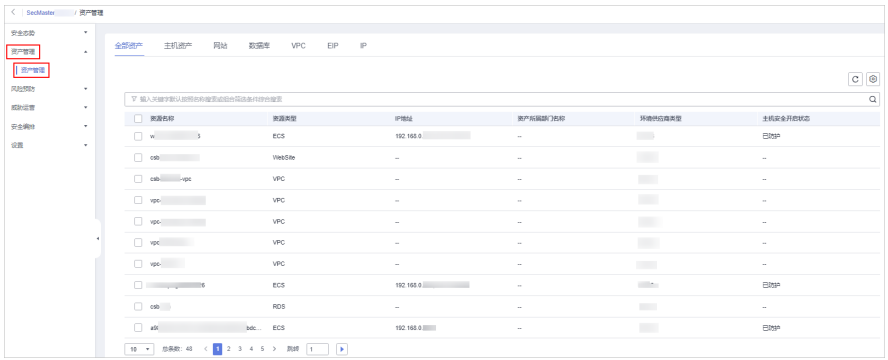
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 8-12 工作空间页面

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。

图 8-13 资产管理



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

版权所有 © 华为云计算技术有限公司

9 风险预防

9.1 基线检查

9.1.1 云服务基线简介

安全云脑提供云服务基线检查功能。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。

9.1.2 设置基线检查计划

安全云脑支持根据基线检查计划检查您的服务器基线配置是否存在风险。

本文档介绍了如何新增基线检查计划。

背景信息

开通基线检查服务后，安全云脑将使用默认检查计划对所有资产进行检查。默认检查计划的自动检查时间、检查对象如下：

- 自动检查时间：每隔3天检查一次，每次在00:00~06:00进行检查。
- 检查对象：您帐号下当前区域的所有资产。

约束与限制

创建检查计划是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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

 版权所有 © 华为云计算技术有限公司

图 9-1 工作空间页面

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 9-2 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9-1所示。

表 9-1 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，SecMaster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。

 版权所有 © 华为云计算技术有限公司

- 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”。

9.1.3 执行基线检查计划

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SecMaster为您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。默认检查计划每隔3天在0点的时候自动执行基线检查。
- 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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

版权所有 © 华为云计算技术有限公司

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“设置检查规范”，系统弹出选择检查规范窗口。

图 9-4 基线检查页面

步骤5 在弹出的选择规范窗口中，选择检查规范，并单击“确定”。

步骤6 在页面右上角单击“立即检查”，立即执行扫描任务。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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。

图 9-6 进入检测设置页面

版权所有 © 华为云计算技术有限公司

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

9.1.4 执行手动检查

基线检查项目分为“自动检查”和“手动检查”项目两种，本章节介绍手动检查项目执行检查的操作。

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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-7 工作空间页面

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 9-8 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”。

版权所有 © 华为云计算技术有限公司

图 9-9 反馈结果

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

9.1.5 查看基线检查结果

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-10 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 9-11 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 9-12 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。

   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。

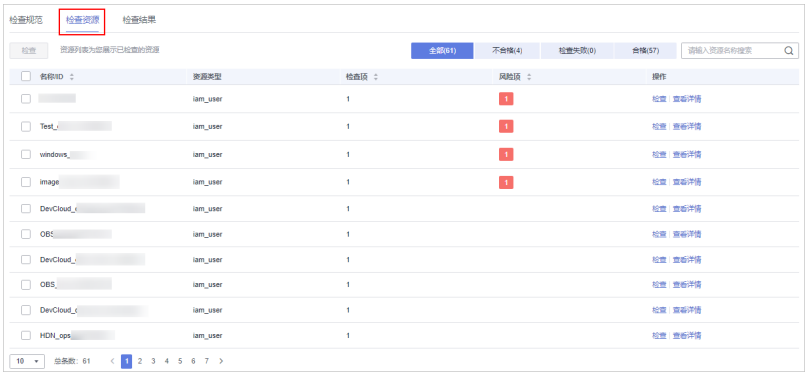
 版权所有 © 华为云计算技术有限公司

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 9-13 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。

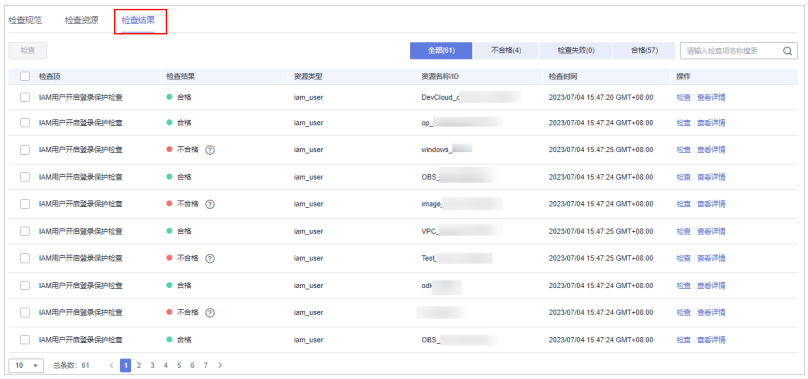
   在资源详情页面，查看资源的检查项、检查状态、检查方式、最近检查时间等详细信息。

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 9-14 全部检查结果



----结束

9.1.6 处理基线检查结果

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。

版权所有 © 华为云计算技术有限公司

- **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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-15 工作空间页面

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 9-16 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 9-2 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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。
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

安全云脑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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-17 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 9-18 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”。

图 9-19 反馈结果

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，SecMaster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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

版权所有 © 华为云计算技术有限公司

图 9-20 工作空间页面

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 9-21 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”。

图 9-22 确认忽略操作示例

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

9.2 漏洞管理

版权所有 © 华为云计算技术有限公司

9.2.1 漏洞管理概述

背景介绍

安全云脑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。

安全云脑支持以下类型的漏洞：

- **主机漏洞**
  包括Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞。

主机漏洞

安全云脑支持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 9-3 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。
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。

9.2.2 查看漏洞详情

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

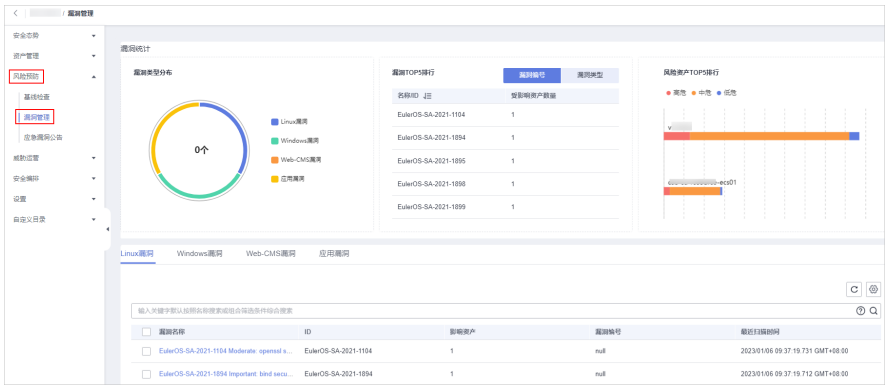
版权所有 © 华为云计算技术有限公司

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 9-23 工作空间页面

步骤4 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

图 9-24 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 9-25 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。

 版权所有 © 华为云计算技术有限公司

表 9-4 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。
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。
最近扫描时间	最近一次扫描的时间。
等级	按照漏洞的危险程度分为：“高危”、“中危”、“低危”、“提示”。

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

9.2.3 修复漏洞

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 9-5 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： ● 使用安全云脑控制台上的“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	

 版权所有 © 华为云计算技术有限公司

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。

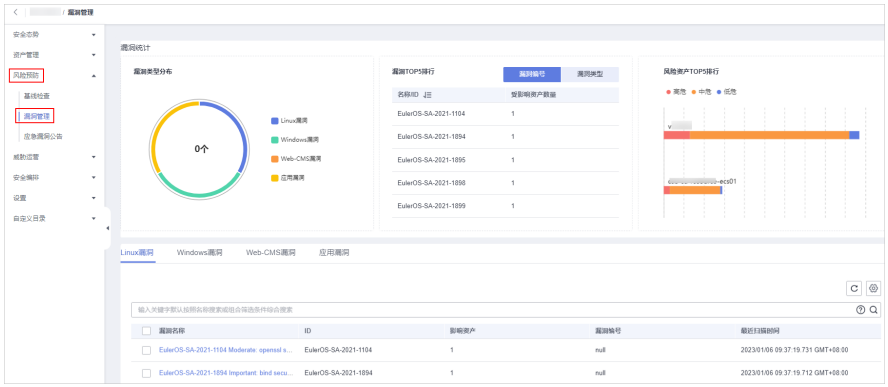
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-26 工作空间页面

步骤4 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

图 9-27 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。

版权所有 © 华为云计算技术有限公司

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。

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9-6。

  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 9-6 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。

 版权所有 © 华为云计算技术有限公司

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 9-7 修复验证

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。

9.2.4 导入/导出漏洞

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20MB。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

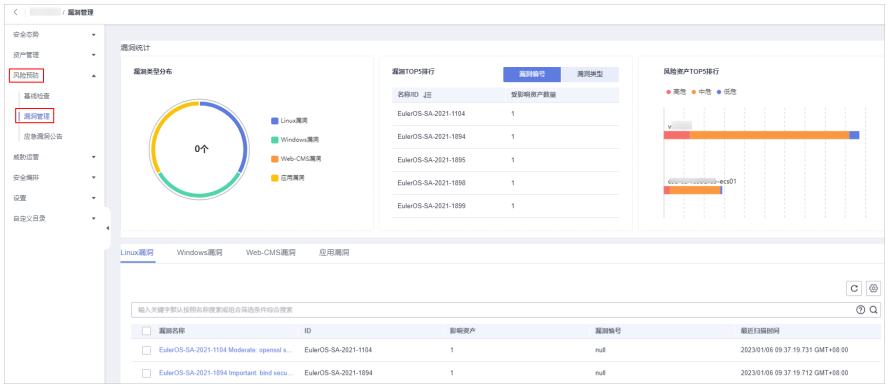
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 9-28 工作空间页面

步骤4 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

图 9-29 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。

注意

- 填写要求：请按照模板填写待导入漏洞信息，填写说明请参见**漏洞导入模板参数说明**。
- 文件格式：须为.xlsx。

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

漏洞导入模板参数说明

导入漏洞需按照模板要求进行操作，参数说明如**表9-8**所示。

版权所有 © 华为云计算技术有限公司

表 9-8 漏洞导入模板参数说明

参数名称		类型	是否必填	参数说明
vul_name_zh		String	是	漏洞中文名称，最大为255字符。
vul_name_en		String	是	漏洞英文名称，最大为255字符。
vul_name		String	是	漏洞名称，最大为255字符。

resource		Object	是	受影响资源。填写示例：
				{
				"domain_id":"f9d7bacbfd2c49e892532ba3f62ab75d",
				"provider":"ecs",
				"project_id":"f69081793d9e4ea8a2f479dcef961989",
				"name":"WAF_12345678-T5Q3",
				"region_id":"xxx",
				"id":"964b692a-8a89-488c-bf65-2bd6fd6f36f7",
				"type":"cloudservers",
				"ep_id":null,
				"tags":{
				"ip":"192.168.0.116",
				"high_risk_port":"20" }}

resource	id	String	是	云服务资源ID。
	name	String	是	资源名称，最大长度255个字符。
	type	String	是	资源类型。
	provider	String	是	云服务名称。
	region_id	String	否	区域ID。
	domain_id	String	是	资源所属帐号ID。
	project_id	String	否	资源所属项目ID。
	ep_id	String	否	企业项目id。
	ep_name	String	否	企业项目名称。
	tags	Object	否	资源标签。 • 最多50个key/values对。 • values：最大255字符，取值范围：字母数字,空格,+, -, =, ., _, :, /,@

 版权所有 © 华为云计算技术有限公司

参数名称		类型	是否必填	参数说明

remediation		Object	否	补救措施。填写示例：
				{
				"recommendation":"The official advisory for this vulnerability has been released, please click the following links to fix it according to the suggestions：\nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\nThe patch for this vulnerability can be referred to:\nhttps://go.googlesource.com/crypto//b7391e95e576cacdcdd422573063bc057239113d\nThe third party advisory for this vulnerability can be referred to:\nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\nThe exploit/POC for this vulnerability has been exposed, for verification please refer to:\nhttps://github.com/Live-Hack-CVE/CVE-2019-11840\n"
				}

remediation	recommendation	String	否	推荐处理方法。
	url	String	否	链接，指向该漏洞的一般修复信息。该URL必须可以从公网访问，不需要提供凭证。
environment		Object	是	漏洞产生的环境坐标信息。
environment	vendor_type	string	是	环境供应商。
	domain_id	string	是	帐号ID。
	region_id	string	是	区域ID。
	project_id	string	否	项目ID，全局服务默认null。
data_source		Object	是	首次上报数据源。
data_source	source_type	Int	是	数据源类型
	domain_id	String	是	数据源产品所属帐号的ID，最大36个字符。
	project_id	String	是	数据源产品所属项目的ID，最大36个字符。
	region_id	String	是	数据源产品所在区域

 版权所有 © 华为云计算技术有限公司

参数名称		类型	是否必填	参数说明
	company_name	String	是	数据源产品所属公司的名称，最大16个字符。
	product_name	String	是	数据源产品的名称，最大24个字符。
	product_feature	String	是	产品功能特性名称，最大24个字符。
	product_module	String	否	检测模块列表。
workspace_id		String	是	工作空间ID。
arrive_time		Timestamp	是	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为漏洞接收时区，无法解析时区的时间，默认时区填东八区。示例： 2023-03-30T12:14:50.472Z+0800
source_url		String	否	漏洞URL链接，指向数据源产品中有关当前漏洞说明的页面。
description_zh		String	是	漏洞中文描述信息，最大1024个字符。
description_en		String	是	漏洞英文描述信息，最大1024个字符。
description		String	是	漏洞描述信息，最大1024个字符。
close_reason		String	否	关闭原因。可填写：误检、已解决、重复或其他。
close_comment		String	否	关闭评论。
create_time		Timestamp	是	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为漏洞记录时区，无法解析时区的时间，默认时区填东八区。示例： 2023-03-30T12:14:50.473Z+0800

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
close_time	Timestamp	否	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。 时区信息为漏洞关闭时区，无法解析时区的时间，默认时区填东八区。示例： 2023-03-30T12:14:50.472Z+0800
update_time	Timestamp	否	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。 时区信息为漏洞更新时区，无法解析时区的时间，默认时区填东八区。示例： 2023-03-30T12:14:50.472Z+0800
criticality	Int	否	关键性，是指漏洞涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源。
close_method	String	否	关闭方式，取值范围如下： ● soc_auto：自动处理修复 ● soc_manual：云脑通过剧本触发 ● hss_manual：hss触发 ● csb_manual：云脑直接触发
batch_number	String	是	批次号，标记比对漏洞使用。
history_observed_source	List<String>	否	历史上报数据源，追加新的上报数据源：HSS、VSS。
count	Int	是	漏洞发生次数。

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
first_observed_time	Timestamp	是	首次发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为漏洞首次发现时区，无法解析时区的时间，默认时区填东八区。示例： 2023-03-30T12:14:50.473+08:00
last_observed_time	Timestamp	是	最近发现时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为漏洞最近发现时区，无法解析时区的时间，默认时区填东八区。示例： 2023-03-30T12:14:50.473Z+0800
id	String	是	漏洞唯一标识，UUID格式，最大36个字符。
version	String	是	漏洞对象的版本。
handled	String	是	是否处理。
domain_id	String	是	资源所属帐号ID。
region_id	String	是	区域ID。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
vulnerability	Object	是	漏洞信息，填写示例如下： { "reason":"Offline Processing", "solution_en":"The official advisory for this vulnerability has been released, please click the following links to fix it according to the suggestions：\nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\nThe patch for this vulnerability can be referred to:\nhttps://go.googlesource.com/crypto//b7391e95e576cacdcdd422573063bc057239113d\nThe third party advisory for this vulnerability can be referred to:\nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\nThe exploit/POC for this vulnerability has been exposed, for verification please refer to:\nhttps://github.com/Live-Hack-CVE/CVE-2019-11840\n", "last_observed_time":"2023-03-23T14:31:41.42108:00", "level":"Medium", "type":3, "url":"[\"https://go.googlesource.com/crypto//b7391e95e576cacdcdd422573063bc057239113d\"]", "repair_severity":2, "related":["CVE-2019-11840"], "solution":"针对该漏洞的官方修复建议已发布，您可单击链接按照建议进行修复：\nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\n针对该漏洞的补丁可参考：\nhttps://go.googlesource.com/crypto//b7391e95e576cacdcdd422573063bc057239113d\n针对该漏洞的非官方修复建议可参考：\nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\n针对该漏洞的漏洞利用/POC已曝光，可参考下方链接进行验证：\nhttps://github.com/Live-Hack-CVE/CVE-2019-11840\n", "solution_zh":"针对该漏洞的官方修复建议已发布，您可单击链接按照建议进行修复：\nhttps://bugzilla.redhat.com/show_bug.cgi?id=1691529\n针对该漏洞的补丁可参考：\nhttps://go.googlesource.com/crypto//b7391e95e576cacdcdd422573063b

 版权所有 © 华为云计算技术有限公司

参数名称		类型	是否必填	参数说明
				c057239113d\n针对该漏洞的非官方修复建议可参考：\nhttps://groups.google.com/forum/#!msg/golang-announce/tjyNcJxb2vQ/n0NRBziSCAAJ\nhttps://github.com/golang/go/issues/30965\n针对该漏洞的漏洞利用/POC已曝光，可参考下方链接进行验证：\nhttps://github.com/Live-Hack-CVE/CVE-2019-11840\n", "comment":null, "id":"HCVD-APP-CVE-2019-12345", "status":4 }
vulnerability	id	String	是	漏洞id。 **注意** ID须为全局唯一，不能与其他漏洞ID相同。
	type	Int	是	漏洞类型。 ● 0：linux ● 1：windows ● 2：web-cms ● 3：应用 ● 4：网站 ● 5：其他
	level	String	是	漏洞等级，High/Medium/Low/Hint。
	tags	List<String>	否	漏洞标签。
	solution	String	否	漏洞修复方案。
	url	String	否	链接信息。
	related	List<String>	是	关联cve_ids。
	repair_severity	Int	是	修复紧急度。 ● 0：high ● 1：medium ● 2：low ● 3：hint

版权所有 © 华为云计算技术有限公司

参数名称			类型	是否必填	参数说明
	status		Int	是	修复状态。 ● 0：unfix ● 1：ignored ● 2：verified ● 3：fixing ● 4：fixed ● 5：reboot ● 6：failed
	reason		String	否	状态修改原因。
	comment		String	否	状态修改其他备注。
	apps		List<Object>	否	涉及软件列表。
	apps	name	String	是	软件名字。
		version	String	是	软件版本。
		image_name	String	否	镜像。
		upgrade_version	String	是	修复版本.
		path	String	否	软件所在路径。
		match_detail	String	否	命中详细信息.
		match_rule	String	否	命中规则。
		pid	String	否	进程id。
	repair_cmd		String	否	修复命令。
	need_boot		int	否	是否需要重启。 ● 1：true ● 0：false
	domain		Object	否	网站漏洞信息。
	domain	url	String	是	url。
		poc	String	否	命中详情，攻击字段，告警信息。

 版权所有 © 华为云计算技术有限公司

参数名称			类型	是否必填	参数说明
		request	String	否	测试请求报文。
		response	String	否	测试返回报文。
playbook_name			String	否	剧本名称。
resource_num			int	是	资产数量。

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。

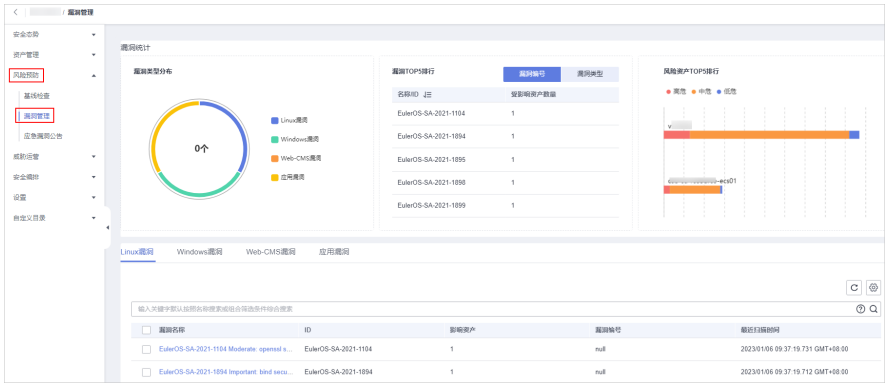
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-30 工作空间页面

步骤4 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

图 9-31 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。

版权所有 © 华为云计算技术有限公司

表 9-9 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

9.2.5 忽略/取消忽略漏洞

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。

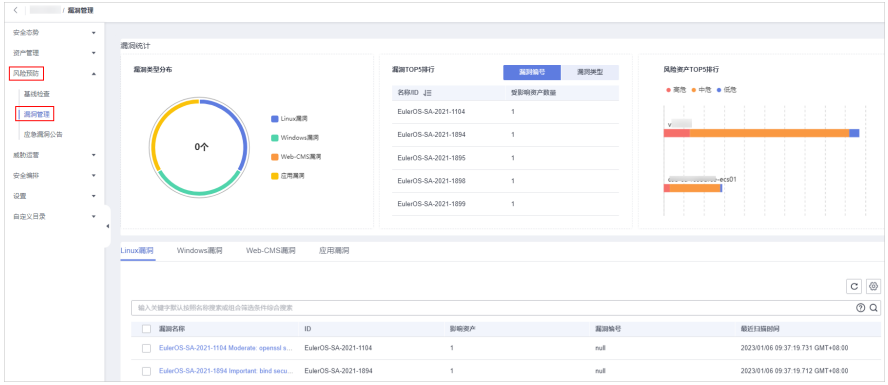
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 9-32 工作空间页面

步骤4 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

图 9-33 进入漏洞管理页面



版权所有 © 华为云计算技术有限公司

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

 版权所有 © 华为云计算技术有限公司

10 威胁运营

10.1 事件管理

10.1.1 查看事件信息

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

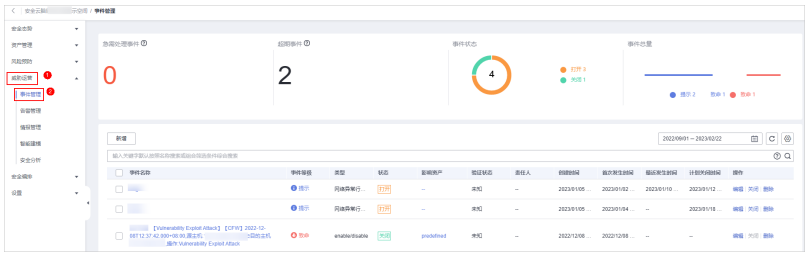
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-1 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 10-2 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 10-3 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，参数说明如**查看事件信息**所示。

页面最多可查看9999条事件信息。

表 10-1 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。
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。

版权所有 © 华为云计算技术有限公司

参数	说明
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细信息，可单击事件名称，页面右侧将展示事件的详细信息。

----结束

10.1.2 新增/编辑事件

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。

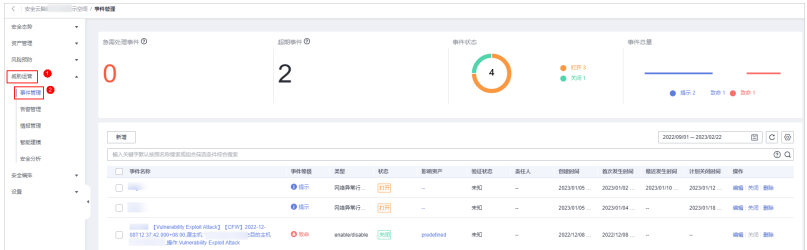
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 10-5 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10-2所示。

 版权所有 © 华为云计算技术有限公司

表 10-2 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。
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。

版权所有 © 华为云计算技术有限公司

参数名称		参数说明
	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。

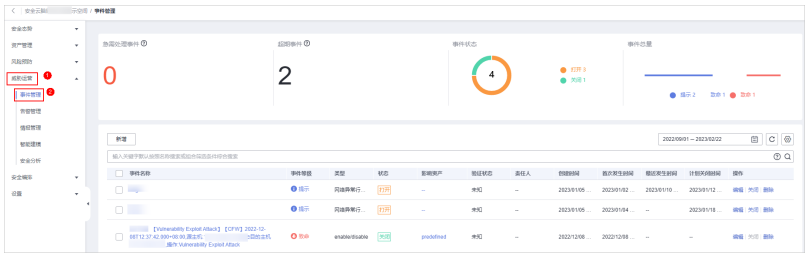
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 10-7 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。

 版权所有 © 华为云计算技术有限公司

表 10-3 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。
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。

 版权所有 © 华为云计算技术有限公司

步骤7 单击“确认”，完成事件编辑。

----结束

10.1.3 导入/导出事件

本章节主要介绍如何导入事件。

约束与限制

仅支持导入.xlsx格式的文件，且文件大小不超过20MB。

导入事件

步骤1 登录管理控制台。

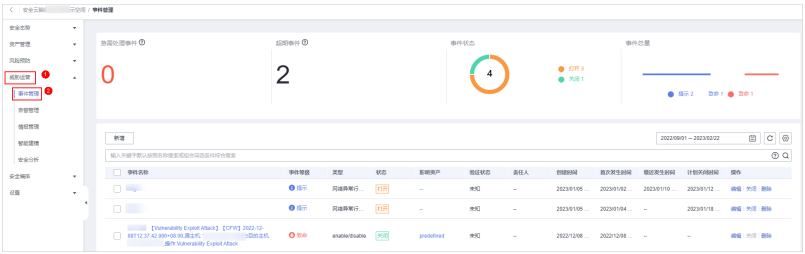
步骤2 单击页面左上方的 ，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 10-9 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。

 版权所有 © 华为云计算技术有限公司

⚠ 注意

- 填写要求：请按照模板填写待导入事件信息，填写说明请参见**导入事件模板参数说明**。
- 文件格式：须为.xlsx。

步骤8 选择完成后，单击“确定”，完成导入。

----结束

导入事件模板参数说明

导入事件需按照模板要求进行操作，事件导入模板参数说明如**表10-4**所示。

表 10-4 导入事件模板参数说明

参数名称	类型	是否必填	参数说明
extend_properties	Object	否	事件的扩展属性。
ttr	Int	否	事件的响应时间。
ttd	Int	否	事件的检测时间。
ref_order_id	String	否	事件业务ID（工单号），最大128个字符。
region_id	String	是	事件对象所属的租户region id。
domain_id	String	是	事件对象所属的租户domain id。
origin_id	String	否	事件原始来源id，最大128个字符。
file_info	List<object>	否	文件信息。
user_info	List<object>	否	用户信息。
process	List<object>	否	进程信息。
incident_type	Object	是	事件类型。填写示例： {"incident_type":"demo","id":"demo"}
network_list	List[Object]	否	网络信息。
resource_list	List[Object]	否	影响资产。
malware	Object	否	恶意软件。
system_info	Object	否	系统信息。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
data_source	Object	是	数据源。填写示例： {"REGION_ID":"demo","product_feature":"demo","project_id":"demo","product_module":"demo","company_name":"demo","DOMAIN_ID":"demo","source_type":445428683,"product_name":"demo"}
remediation	Object	否	补救措施。
is_deleted	Boolean	否	是否删除。
environment	Object	是	事件产生的环境坐标信息。
workspace_id	String	是	事件对象所属工作空间id。
sla	Int	否	计划关闭时间：单位：小时设置风险接受持续时间。
close_time	Timestamp	否	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件关闭时区，无法解析时区的时间，默认时区填东八区。
owner	String	否	责任人、服务责任人。
close_comment	String	否	关闭评论。
count	Int	是	事件发生次数。
close_reason	String	否	关闭原因。 ● 误检 ● 已解决 ● 重复 ● 其他
handle_status	String	是	事件处理状态，可选类型如下： ● Open：打开 ● Block：阻塞 ● Closed：关闭 默认填写Open
update_time	Timestamp	否	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件更新时区，无法解析时区的时间，默认时区填东八区。
create_time	Timestamp	是	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件记录时区，无法解析时区的时间，默认时区填东八区。示例：2023-04-13T10:36:20.580Z+0800

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
first_observed_time	Timestamp	是	首次发生时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
arrive_time	Timestamp	是	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件接收时区，无法解析时区的时间，默认时区填东八区。
last_observed_time	Timestamp	否	最近发生时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为事件发生时区，无法解析时区的时间，默认时区填东八区。
description	String	是	事件描述信息，最大1024个字符。
ipdrr_phase	String	否	周期/处置阶段编号。
title	String	是	事件名称，最大255字符。
confidence	Int	否	事件的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100。 ● 0：表示事件的置信度为0% ● 100：表示事件的置信度为100%
verification_state	String	是	验证状态，标识事件的准确性。 ● Unknown：未知 ● True_Positive：确认 ● False_Positive：误报 默认填写Unknown
version	String	是	事件对象的版本。
actor	String	否	事件调查员。
creator	String	否	创建人。
simulation	Boolean	否	调试字段。
severity	String	是	事件等级，取值范围： ● Tips：未发现任何问题。 ● Low：无需针对问题执行任何操作。 ● Medium：问题需要处理，但不紧急。 ● High：问题必须优先处理。 ● Fatal：问题必须立即处理，以防止产生进一步的损害。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
criticality	Int	否	关键性，是指事件涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源。
source_url	String	否	事件URL链接，指向数据源产品中有关当前事件说明的页面。
id	String	是	事件唯一标识，UUID格式，最大36个字符。
labels	String	否	标签。

导出事件

步骤1 登录管理控制台。

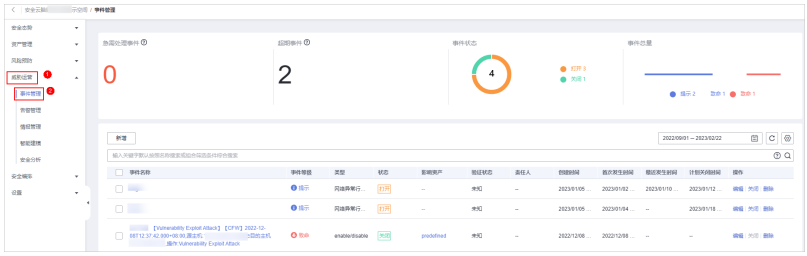
步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-10 工作空间页面

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 10-11 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。

 版权所有 © 华为云计算技术有限公司

表 10-5 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

10.1.4 关闭/删除事件

本章节主要介绍如何执行**关闭事件**、**删除事件**操作。

关闭事件

步骤1 登录管理控制台。

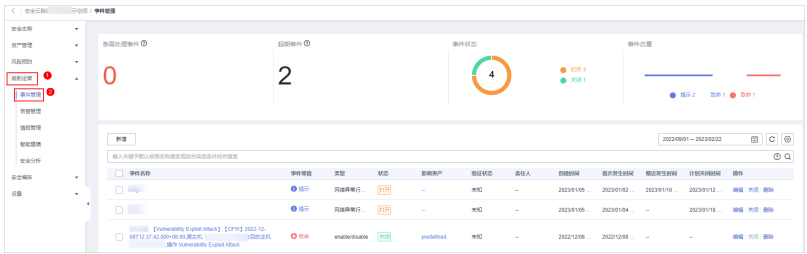
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-12 工作空间页面

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 10-13 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“关闭”，弹出关闭事件确认框。

步骤6 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”。

----结束

版权所有 © 华为云计算技术有限公司

删除事件

步骤1 登录管理控制台。

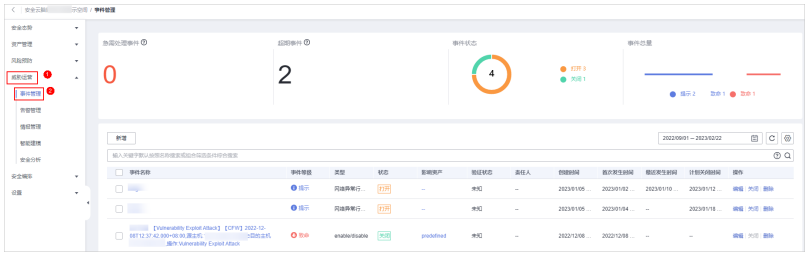
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 10-15 事件管理页面



步骤5 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。

步骤6 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

10.2 告警管理

10.2.1 查看告警信息

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。

 版权所有 © 华为云计算技术有限公司

操作步骤

步骤1 登录管理控制台。

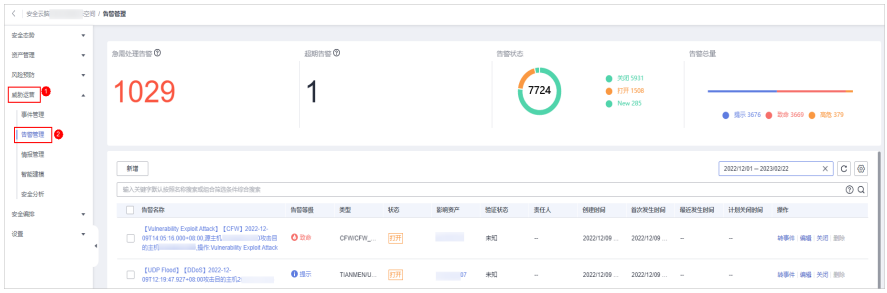
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 10-17 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 10-18 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10-6所示。

页面最多可查看9999条告警信息。

 版权所有 © 华为云计算技术有限公司

表 10-6 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，还可以查看受影响资产相关信息。

----结束

10.2.2 告警转事件

本章节主要介绍如何将告警转为事件。

告警转事件

步骤1 登录管理控制台。

 版权所有 © 华为云计算技术有限公司

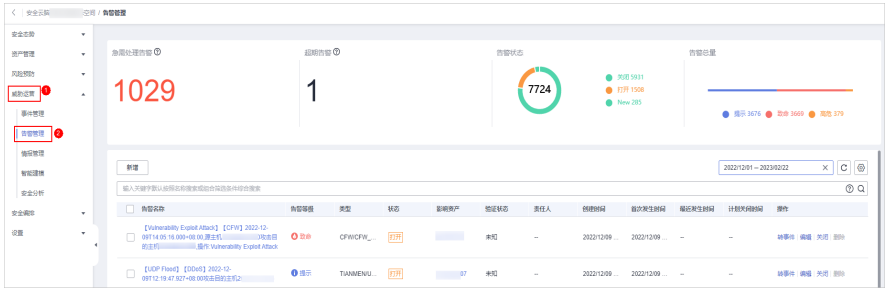
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-19 工作空间页面

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 10-20 告警管理页面

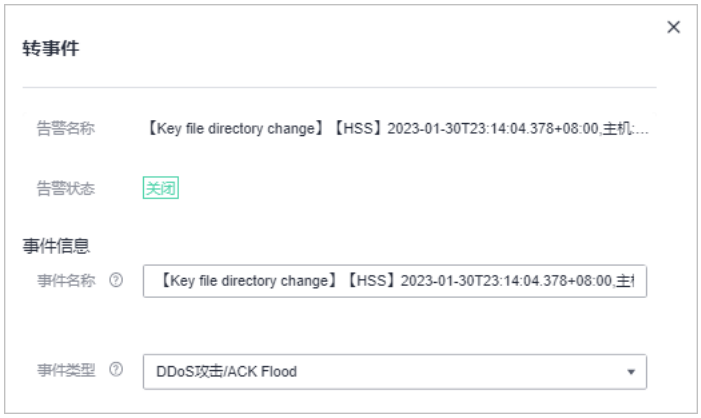


步骤5 在告警管理列表中，单击目标告警所在行“操作”列的“转事件”，右侧弹出转事件配置页面。

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。

图 10-21 告警转事件配置



步骤7 设置完成后，单击“确认”。

----结束

版权所有 © 华为云计算技术有限公司

10.2.3 新增/编辑告警

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。

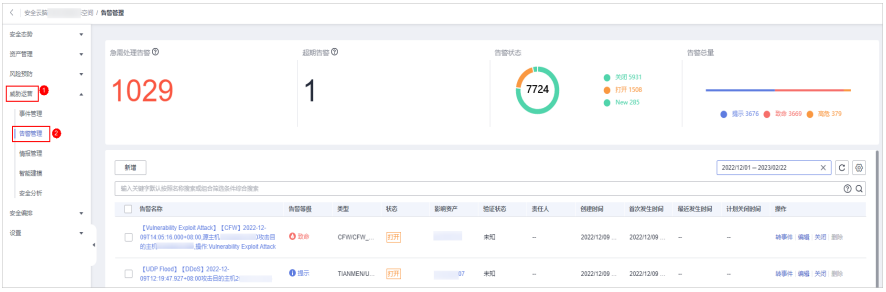
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 10-23 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10-7所示。

表 10-7 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。

版权所有 © 华为云计算技术有限公司

参数名称		参数说明
	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。
	（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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

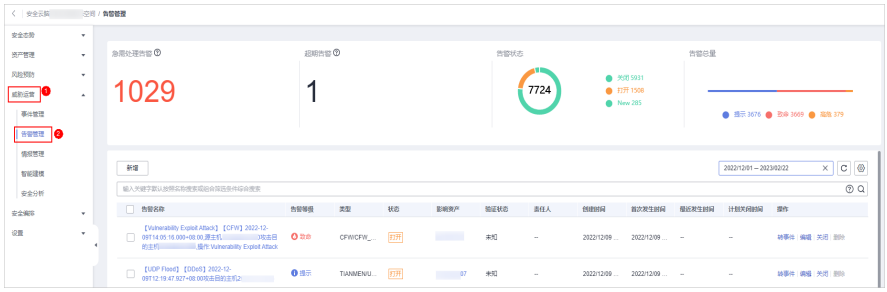
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 10-24 工作空间页面

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 10-25 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10-8所示。

表 10-8 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。

版权所有 © 华为云计算技术有限公司

参数名称		参数说明
	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。
	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

10.2.4 导入/导出告警

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20MB。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

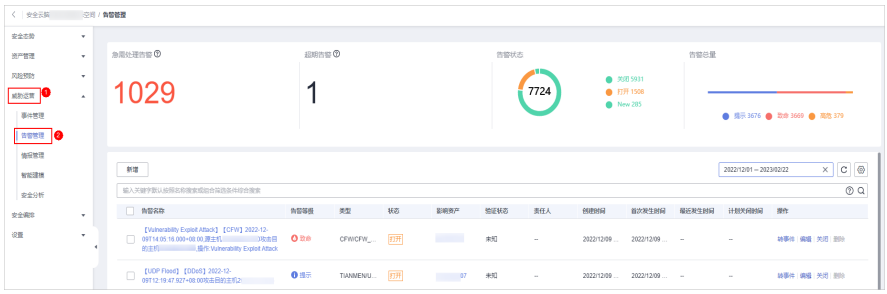
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 10-26 工作空间页面

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 10-27 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。

注意

- 填写要求：请按照模板填写待导入告警信息，填写说明请参见**导入告警模板参数说明**。
- 文件格式：须为.xlsx。

步骤8 选择完成后，单击“确定”，完成导入。

----结束

导入告警模板参数说明

导入告警需按照模板要求进行操作，告警导入模板参数说明如**表10-9**所示。

表 10-9 导入告警模板参数说明

参数名称	类型	是否必填	参数说明
extend_properties	Object	否	扩展属性。
ttr	Int	否	响应时间。
ttd	Int	否	检测时间。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
ref_order_id	String	否	业务ID（工单号），最大128个字符。
origin_id	String	否	告警原始来源id，最大128个字符。
file_info	list<object>	否	文件信息。
user_info	list<object>	否	用户信息。
process	list<object>	否	进程信息。
network_list	List[Object]	否	网络信息。
resource_list	List[Object]	否	影响资产。
system_info	object	否	系统信息。
alert_type	Object	是	告警类型。填写示例： {"id":"demo","alert_type":"demo"}
malware	Object	否	恶意软件。
remediation	Object	否	补救措施。
environment	Object	是	告警产生的环境坐标信息。
data_source	Object	是	数据源。填写示例： {"domain_id":"demo","product_feature":"demo","project_id":"demo","product_module":"demo","company_name":"demo","region_id":"demo","source_type":-827196037,"product_name":"demo"}
workspace_id	String	是	告警对象所属工作空间id。
is_deleted	Boolean	否	是否删除。
arrive_time	Timestamp	是	接收时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警接收时区，无法解析时区的时间，默认时区填东八区。
source_url	String	否	告警URL链接，指向数据源产品中有关当前事件说明的页面。
description	String	是	告警描述信息，最大1024个字符。
sla	Int	否	计划关闭时间，单位：小时,设置风险接受持续时间。
ipdrr_phase	String	否	周期/处置阶段编号。
actor	String	否	告警调查员。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
close_reason	String	否	关闭原因。 ● 误检 ● 已解决 ● 重复 ● 其他
close_comment	String	否	关闭评论。
create_time	Timestamp	是	记录时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警记录时区，无法解析时区的时间，默认时区填东八区。
close_time	Timestamp	否	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警关闭时区，无法解析时区的时间，默认时区填东八区。
update_time	Timestamp	否	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为告警更新时区，无法解析时区的时间，默认时区填东八区。
severity	String	是	告警等级，取值范围： ● Tips：未发现任何问题。 ● Low：无需针对问题执行任何操作。 ● Medium：问题需要处理，但不紧急。 ● High：问题必须优先处理。 ● Fatal：问题必须立即处理，以防止产生进一步的损害。
confidence	Int	否	告警的置信度。置信度的定义旨在说明识别的行为或问题的可能性。 取值范围：0-100。 ● 0：表示告警的置信度为0% ● 100：表示告警的置信度为100%
criticality	Int	否	关键性，是指告警涉及的资源的重要性级别。 取值范围：0-100，0表示资源不关键，100表示最关键资源。
count	Int	是	告警发生次数。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
handle_status	String	是	告警处理状态，可选类型如下： ● Open：打开 ● Block：阻塞 ● Closed：关闭 默认填写Open
first_observed_time	Timestamp	是	告警首次发生时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms +timezone。时区信息为告警发生时区，无法解析时区的时间，默认时区填东八区。
last_observed_time	Timestamp	否	告警最近发生时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms +timezone。时区信息为告警发生时区，无法解析时区的时间，默认时区填东八区。
creator	String	否	创建人。
verification_state	String	是	验证状态，标识告警的准确性。可选类型如下： ● Unknown：未知 ● True_Positive：确认 ● False_Positive：误报 默认填写Unknown
id	String	是	告警唯一标识，UUID格式，最大36个字符。
version	String	是	告警对象的版本。
domain_id	String	是	告警对象所属的租户domain id。
title	String	是	告警名称，最大255字符。
region_id	String	是	告警对象所属的租户region id。
simulation	Boolean	否	调试字段。
owner	String	否	责任人、服务责任人。
labels	String	否	标签。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

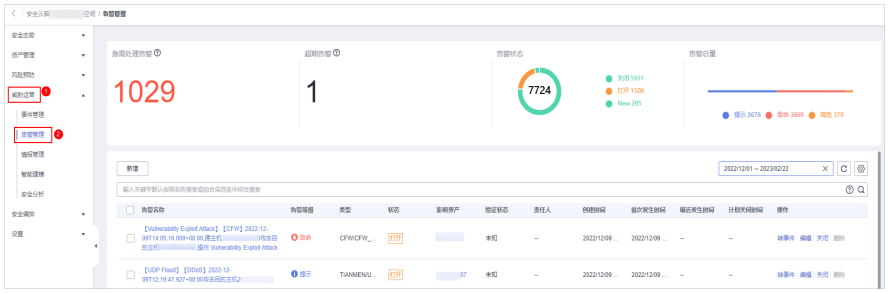
 版权所有 © 华为云计算技术有限公司

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 工作空间页面

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 10-29 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 10-10 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

10.2.5 关闭/删除告警

本章节主要介绍如何执行关闭告警、删除告警操作。

关闭告警

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

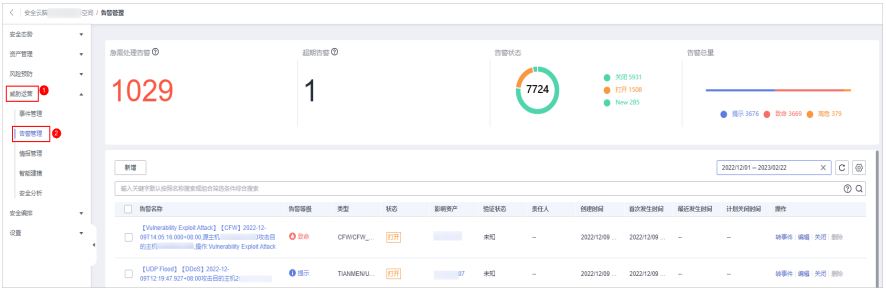
 版权所有 © 华为云计算技术有限公司

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 工作空间页面

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 10-31 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“更多 > 关闭”，弹出关闭告警确认框。

步骤6 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”。

----结束

删除告警

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

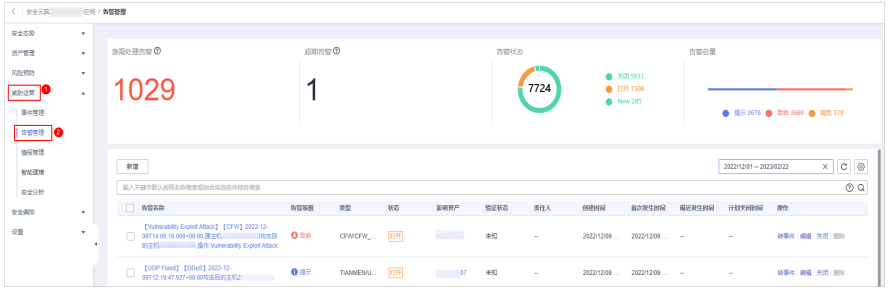
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-32 工作空间页面

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。

 版权所有 © 华为云计算技术有限公司

图 10-33 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“更多 > 删除”，弹出删除告警确认框。

步骤6 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

10.3 情报管理

10.3.1 新增情报指标

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-34 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 10-35 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 10-11 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。
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、邮箱帐户、地区等信息。

版权所有 © 华为云计算技术有限公司

步骤6 单击“确认”，完成指标创建。

----结束

10.3.2 关闭情报指标

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-36 工作空间页面

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 10-37 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

10.3.3 导入/导出情报指标

本章节主要介绍如何导入情报指标。

约束与限制

- 仅支持导入.xlsx格式的文件，且文件大小不超过20MB。
- 最多支持导出9999条情报指标信息。

版权所有 © 华为云计算技术有限公司

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-38 工作空间页面

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 10-39 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。

注意

- 填写要求：请按照模板填写待导入情报指标信息，填写说明请参见**导入情报指标模板参数说明**。
- 文件格式：须为.xlsx。

步骤8 选择完成后，单击“确定”，完成导入。

----结束

导入情报指标模板参数说明

导入情报指标需按照模板要求进行操作，情报指标导入模板参数说明如**表10-12**所示。

版权所有 © 华为云计算技术有限公司

表 10-12 导入情报指标模板参数说明

参数名称	类型	是否必填	参数说明
data_source	Object	是	数据源。填写示例： {"domain_id":"demo","product_feature":"demo","project_id":"demo","product_module":"demo","company_name":"demo","region_id":"demo","source_type":892339122,"product_name":"demo"}
environment	Object	是	指标产生的环境坐标信息。填写示例： {"domain_id":"demo","project_id":"demo","region_id":"demo","vendor_type":"demo"}
email	Object	否	邮件。
url	Object	否	URL地址。
domain	Object	否	域名。
is_deleted	string	是	是否删除标记。
workspace_id	String	是	工作空间ID。
weak_password	String	否	弱口令。
vulnerability	String	否	漏洞。
start_time	Timestamp	否	开始时间。
information_source	String	是	来源渠道。
confidence	Numeric	否	指标的置信度，取值范围是80-100。
close_comment	String	否	关闭评论。
labels	String	否	标签，如“矿池”、“外联”等。
inactive_time	Timestamp	否	失效时间。
file	Object	否	文件。
close_reason	String	否	关闭原因。
first_report_time	Timestamp	是	首次发生时间。
create_time	Timestamp	是	威胁平台收集到情报的创建时间。
suggested_of_coa	String	否	建议。
valid_from	Timestamp	否	有效期开始时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为指标有效期开始所在时区，无法解析时区的时间，默认时区填东八区。

版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
kill_chain_phases	String	否	比较重要的信息，应该保留。
verdict	String	是	标志黑白灰，自定义枚举转换（black、white、gray）。
pattern	String	否	保留字段。
external_references	String	否	扩展字段。
status	String	是	指标状态。 ● Open：打开 ● Closed：关闭 ● Revoked：作废
revoked	Boolean	否	是否作废，默认否。
creator	String	否	创建人。
granular_marking	Numeric	是	粒度（保密等级），由高到低：1（首次发现）、2（自产数据）、3（需购买）、4（外网直接查询）。
id	String	是	唯一值（生成规则）：md5（indicator_type + value + information_source + label）
owner	String	否	所有者。
ip	Object	否	ip地址。
indicator_type	Object	是	类别(值域)：ipv4、ipv6，domain、email、url、hash，un_classified。填写示例： {"indicator_type":"demo","id":"demo","category":"demo"}
close_time	String	否	关闭时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为指标发生时区，无法解析时区的时间，默认时区填东八区。
inactive_set_time	Timestamp	否	设定失效时间。
update_time	String	否	更新时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms+timezone。时区信息为指标更新时区，无法解析时区的时间，默认时区填东八区。
verdict_set_time	Timestamp	否	判定时间。

 版权所有 © 华为云计算技术有限公司

参数名称	类型	是否必填	参数说明
severity	Numeric	否	严重程度，不同渠道定义值不一样（取值范围是80-100）。
valid_until	Timestamp	否	有效期截止时间，格式ISO8601：YYYY-MM-DDTHH:mm:ss.ms +timezone。时区信息为指标有效期截止时区，无法解析时区的时间，默认时区填东八区。
last_report_time	Timestamp	是	最近发生时间。
value	String	是	值，如：ip，url，domain等。
defanged	Boolean	是	是否失效默认否。
extensions	String	否	扩展。
count	Numeric	否	发生次数。
description	String	否	描述。
name	String	是	情报名称。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-40 工作空间页面

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 10-41 情报管理页面

版权所有 © 华为云计算技术有限公司

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 10-13 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

10.3.4 管理情报指标

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-42 工作空间页面

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 10-43 情报管理页面

版权所有 © 华为云计算技术有限公司

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 10-44 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10-14所示。

页面最多可查看9999条情报指标信息。

表 10-14 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。
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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

版权所有 © 华为云计算技术有限公司

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 10-45 工作空间页面

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 10-46 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 10-15 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。

版权所有 © 华为云计算技术有限公司

参数	说明
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。
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、邮箱帐户、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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-47 工作空间页面

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 10-48 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。

版权所有 © 华为云计算技术有限公司

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

10.4 智能建模

10.4.1 查看已有模型模板

安全云脑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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-49 工作空间页面

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 10-50 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。

版权所有 © 华为云计算技术有限公司

- **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

10.4.2 新建/编辑模型

安全云脑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
- 自定义告警模型
- 编辑模型

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-51 工作空间页面

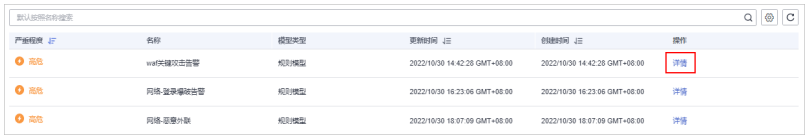
步骤4 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

图 10-52 模型模板页面

版权所有 © 华为云计算技术有限公司

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。

图 10-53 模型模板详情



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10-16所示。

图 10-54 基础配置

表 10-16 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。

版权所有 © 华为云计算技术有限公司

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10-17所示。

表 10-17 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。

 版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-55 工作空间页面

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 10-56 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10-18所示。

 版权所有 © 华为云计算技术有限公司

图 10-57 基础配置

表 10-18 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10-19所示。

 版权所有 © 华为云计算技术有限公司

表 10-19 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

 版权所有 © 华为云计算技术有限公司

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 10-58 工作空间页面

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 10-59 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10-20所示。

图 10-60 基础配置

表 10-20 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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。

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10-21**所示。

表 10-21 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。

 版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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

10.4.3 查看已有模型

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-61 工作空间页面

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 10-62 可用模型页面

版权所有 © 华为云计算技术有限公司

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

10.4.4 管理模型

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-63 工作空间页面

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 10-64 可用模型页面

步骤5 管理模型。

 版权所有 © 华为云计算技术有限公司

表 10-22 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

10.5 安全分析

10.5.1 安全分析概述

安全云脑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。

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。

10.5.2 使用流程

安全分析功能使用具体流程如**表10-23**所示。

 版权所有 © 华为云计算技术有限公司

表 10-23 使用流程

子流程	说明
新增工作空间	新增工作空间，用于资源隔离和控制。
数据集成	配置需要接入的数据。 安全云脑支持集成存储、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）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）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。
配置索引	配置索引条件，缩小查询范围。
查询与分析	对接入的数据进行查询、分析。
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。
图表统计查询分析结果	当您执行了查询分析语句后，安全云脑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。

10.5.3 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

 版权所有 © 华为云计算技术有限公司

图 10-65 工作空间页面

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 10-66 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。

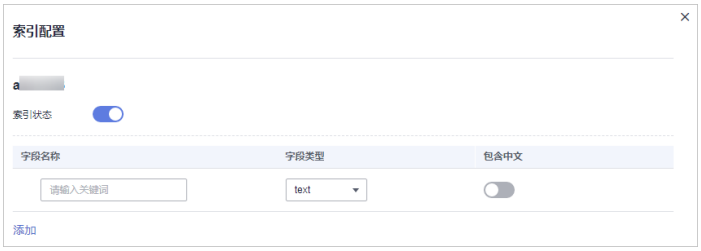
图 10-67 管道数据页面

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10-24所示。

图 10-68 索引配置



 版权所有 © 华为云计算技术有限公司

表 10-24 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

10.5.4 查询与分析

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

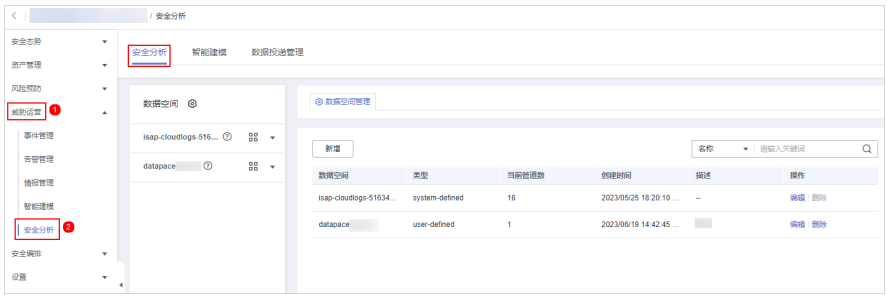
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 10-69 工作空间页面

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 10-70 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 10-71 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**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 10-72 查询与分析

版权所有 © 华为云计算技术有限公司

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。

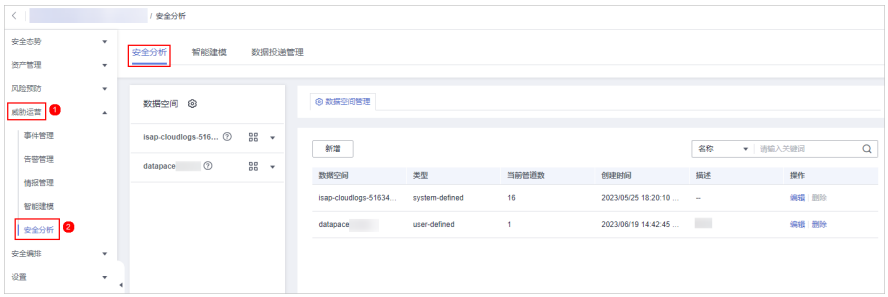
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-73 工作空间页面

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 10-74 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 10-75 管道数据页面

版权所有 © 华为云计算技术有限公司

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。
- 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。

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

安全云脑通过**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。

- **原始日志**

  在“原始日志”页签将展示当前查询结果。

  - 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。
    - 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。
    - 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。
      - 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。
      - 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。
  - 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。

 版权所有 © 华为云计算技术有限公司

图表统计是安全云脑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**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**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**快速查询**。

10.5.5 下载日志

安全云脑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**数据集成**。

操作步骤

步骤1 登录管理控制台。

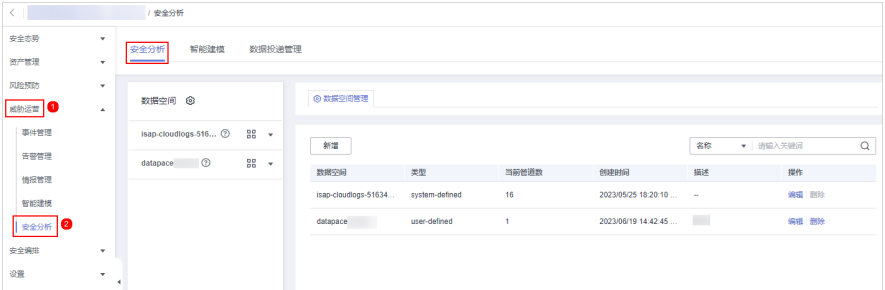
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-76 工作空间页面

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。

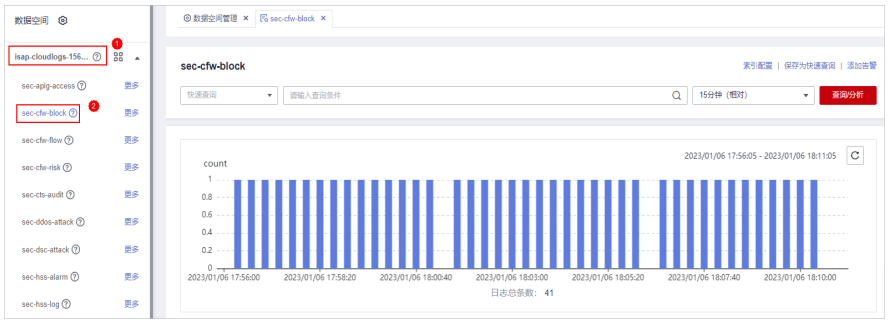
图 10-77 进入安全分析页面



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。

版权所有 © 华为云计算技术有限公司

图 10-78 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

10.5.6 查询与分析语法

10.5.6.1 SQL 语法

10.5.6.1.1 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 10-25 基本语法

语句类型	说明
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。
分析语句	分析语句用于对查询结果进行计算和统计。

10.5.6.1.2 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。

本章节将介绍查询语句以及使用示例。

 版权所有 © 华为云计算技术有限公司

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 10-26 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。
>	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 10-27 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'

版权所有 © 华为云计算技术有限公司

查询需求	查询语句
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

10.5.6.1.3 分析语句

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]
```

SELECT

指定查询的字段。

使用*查询所有字段

```
SELECT *
```

表 10-28 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

版权所有 © 华为云计算技术有限公司

查询指定字段

```
SELECT firstname, lastname
```

表 10-29 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 10-30 使用 AS 给字段定义别名

num
1
16
13
18

使用 DISTINCT 去重

```
SELECT DISTINCT age
```

表 10-31 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
```

 版权所有 © 华为云计算技术有限公司

表 10-32 使用 SQL 函数

len	firstname
4	Amber
6	Hattie
7	Nanette
4	Dale

GROUP BY

按值分组。

按字段的值分组

```
SELECT age GROUP BY age
```

表 10-33 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 10-34 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
```

 版权所有 © 华为云计算技术有限公司

表 10-35 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 10-36 使用 SQL 函数

len	count
4	2
5	2

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 10-37 HAVING

age	MAX(balance)
28	32838
32	39225

ORDER BY

按字段值排序。

使用字段值排序

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

 版权所有 © 华为云计算技术有限公司

表 10-38 使用字段值排序

age
28
32
32
36

LIMIT

指定返回数据的条数。

指定返回的条数

```
SELECT * LIMIT 1
```

表 10-39 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 10-40 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

 版权所有 © 华为云计算技术有限公司

函数

数学类

表 10-41 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
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

版权所有 © 华为云计算技术有限公司

函数	作用	定义	示例
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 10-42 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

版权所有 © 华为云计算技术有限公司

函数	作用	定义	示例
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 10-43 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
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

版权所有 © 华为云计算技术有限公司

函数	作用	定义	示例
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 10-44 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
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

版权所有 © 华为云计算技术有限公司

其他

表 10-45 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

聚合函数

表 10-46 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
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

10.5.6.1.4 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。

版权所有 © 华为云计算技术有限公司

10.5.6.2 快速查询

快速查询为安全云脑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**配置索引**。

创建快速查询

步骤1 登录管理控制台。

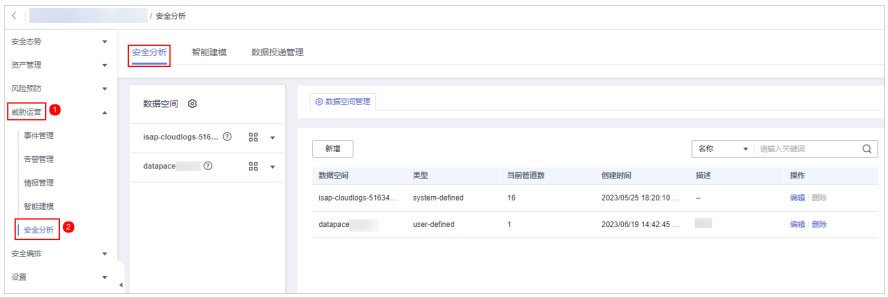
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-79 工作空间页面

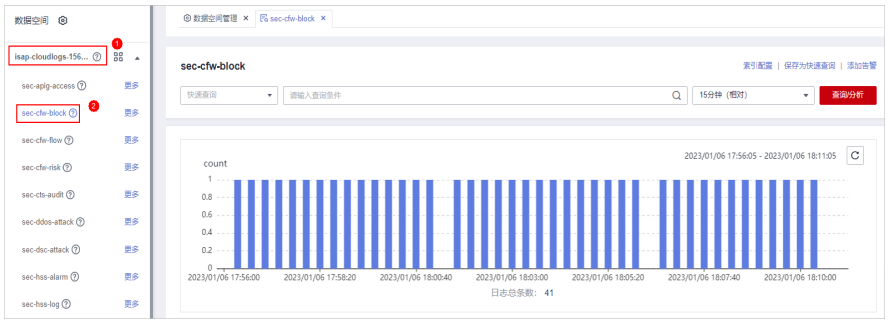
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-80 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 10-81 管道数据页面



版权所有 © 华为云计算技术有限公司

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**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。

图 10-82 快速查询

表 10-47 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

10.5.7 快速添加日志告警模型

安全云脑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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

版权所有 © 华为云计算技术有限公司

图 10-83 工作空间页面

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 10-84 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 10-85 管道数据页面

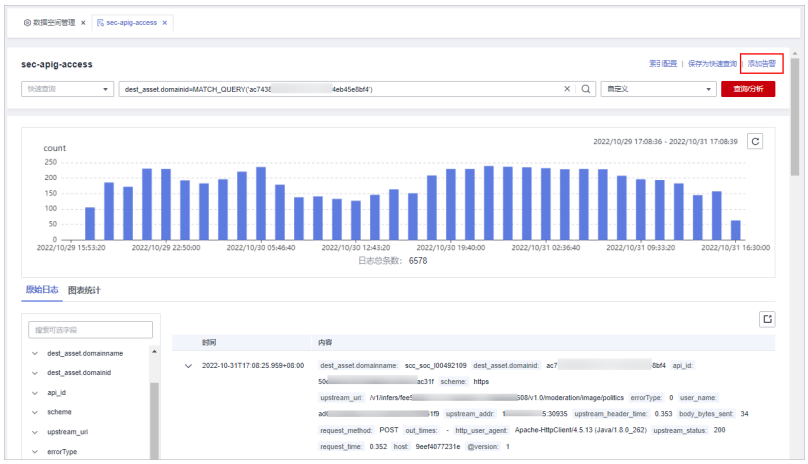
步骤6 输入查询分析语句，设置时间范围，并单击“查询分析”，显示查询分析结果。

更多查询分析详细操作请参见**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。

 版权所有 © 华为云计算技术有限公司

图 10-86 添加告警



步骤8 配置告警基础信息，参数说明如**表10-48**所示。

图 10-87 基础配置

表 10-48 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。

版权所有 © 华为云计算技术有限公司

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10-49所示。

表 10-49 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。

 版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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

10.5.8 图表统计

10.5.8.1 图表统计概述

当您执行了查询分析语句后，安全云脑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：

- 表格
- 折线图
- 柱状图
- 饼图

10.5.8.2 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。在安全云脑中，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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

 版权所有 © 华为云计算技术有限公司

图 10-88 工作空间页面

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 10-89 进入安全分析页面

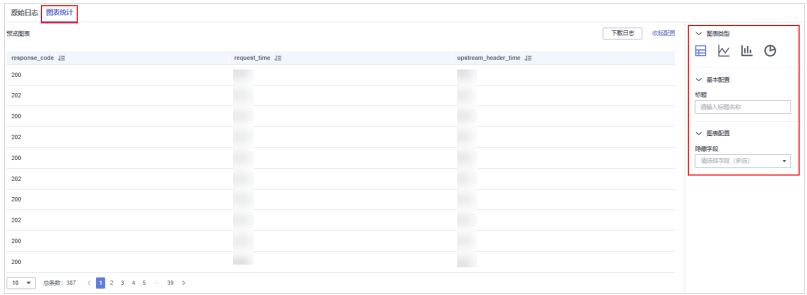
步骤5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 10-90 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 。

图 10-91 表格统计



步骤8 配置表格参数。

版权所有 © 华为云计算技术有限公司

表 10-50 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。
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”。

10.5.8.3 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-92 工作空间页面

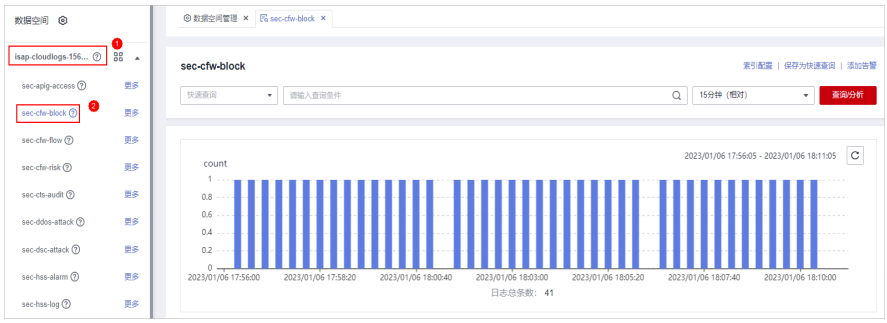
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

版权所有 © 华为云计算技术有限公司

图 10-93 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。

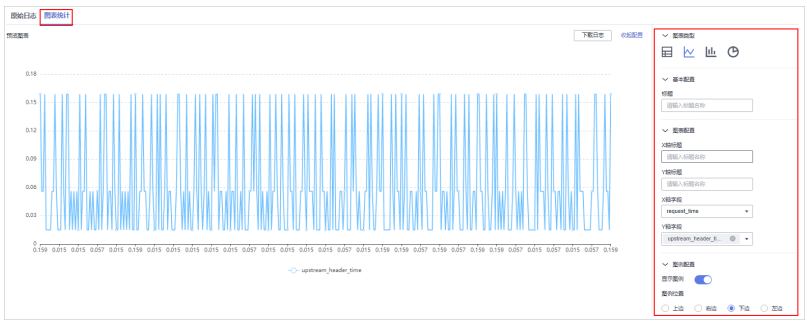
图 10-94 管道数据页面



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  。

图 10-95 折线图统计



步骤8 配置折线图参数。

表 10-51 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。

版权所有 © 华为云计算技术有限公司

参数类别	参数名称	参数说明
	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”。

10.5.8.4 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。安全云脑中，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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

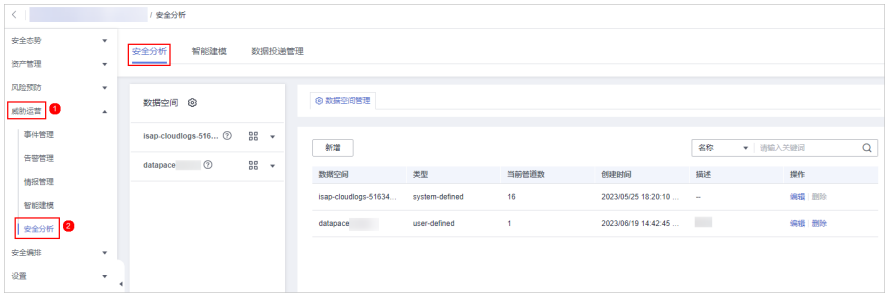
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-96 工作空间页面

版权所有 © 华为云计算技术有限公司

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 10-97 进入安全分析页面



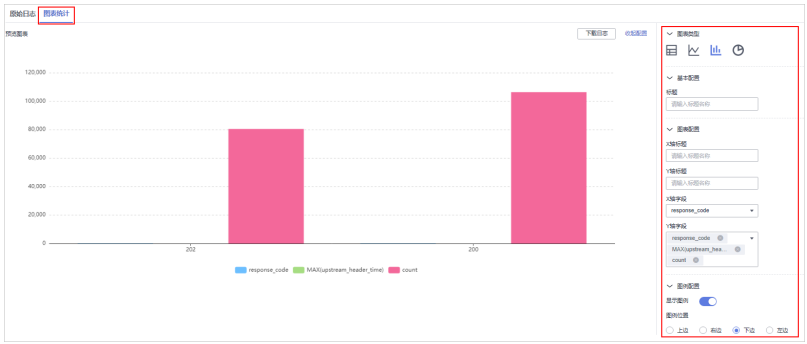
步骤5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击管道名称，右侧将显示管道数据的检索页面。

图 10-98 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  。

图 10-99 柱状图统计



步骤8 配置柱状图参数。

表 10-52 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。

版权所有 © 华为云计算技术有限公司

参数类别	参数名称	参数说明
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”。

10.5.8.5 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

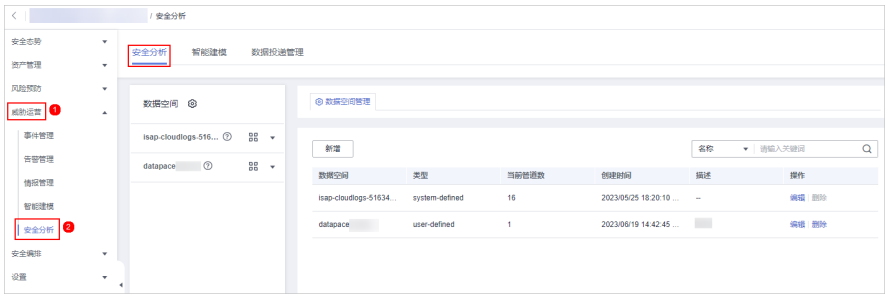
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-100 工作空间页面

版权所有 © 华为云计算技术有限公司

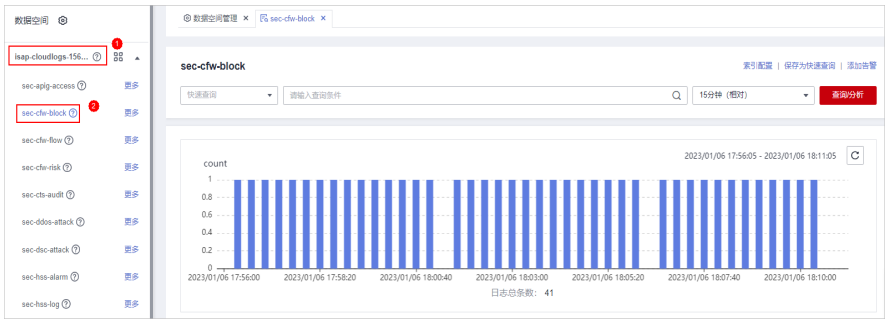
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-101 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。

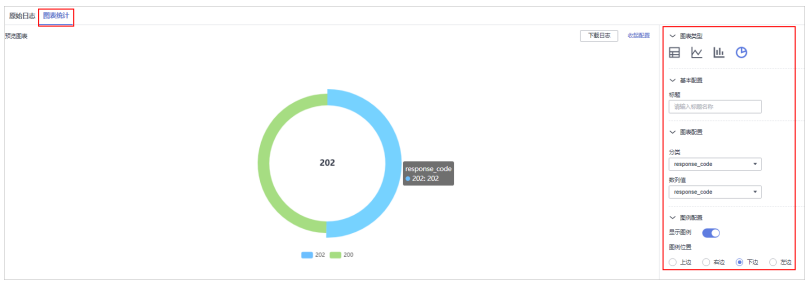
图 10-102 管道数据页面



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  。

图 10-103 饼图统计



步骤8 配置饼图参数。

表 10-53 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。

版权所有 © 华为云计算技术有限公司

参数类别	参数名称	参数说明
	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”。

10.5.9 管理数据空间

10.5.9.1 新增数据空间

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。

当您需要使用安全云脑提供的**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**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。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-104 工作空间页面

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 10-105 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 10-106 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10-54所示。

表 10-54 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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

10.5.9.2 查看数据空间详情

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。

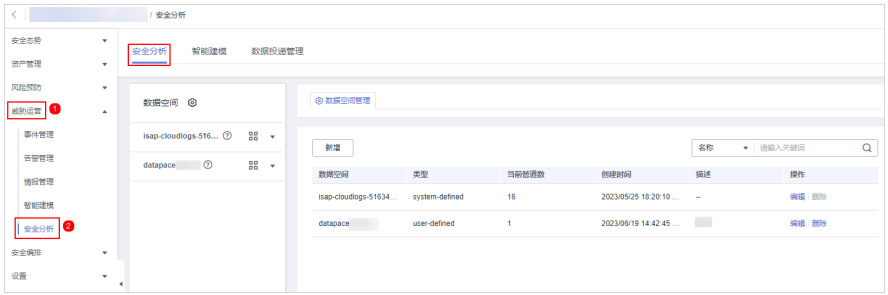
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-107 工作空间页面

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 10-108 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10-55所示。

版权所有 © 华为云计算技术有限公司

表 10-55 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 10-109 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10-56**所示。

表 10-56 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

10.5.9.3 编辑数据空间

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。

版权所有 © 华为云计算技术有限公司

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-110 工作空间页面

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 10-111 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”。

图 10-112 编辑数据空间

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

10.5.9.4 删除数据空间

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。

版权所有 © 华为云计算技术有限公司

- 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-113 工作空间页面

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 10-114 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”。

图 10-115 删除数据空间

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

版权所有 © 华为云计算技术有限公司

10.5.10 管理管道

10.5.10.1 创建管道

数据传输消息主题和存储索引组合为数据管道。

当您需要使用安全云脑提供的**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**新增工作空间**。
- 已新增数据空间，具体操作请参见**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。

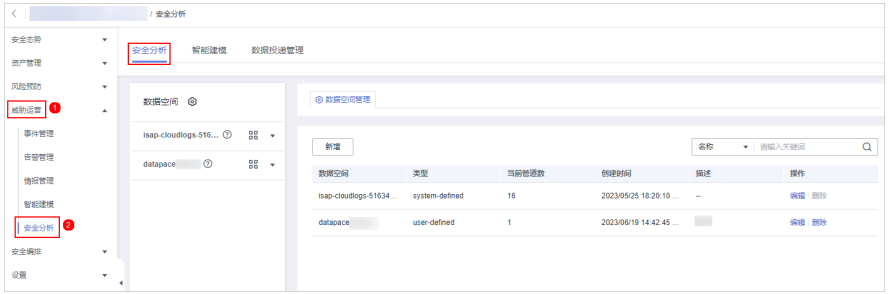
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-116 工作空间页面

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 10-117 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。

版权所有 © 华为云计算技术有限公司

图 10-118 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10-57所示。

表 10-57 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。
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

10.5.10.2 查看管道详情

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

版权所有 © 华为云计算技术有限公司

图 10-119 工作空间页面

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 10-120 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 10-121 查看管道

步骤6 单击待查看管道名称后的⑦，右侧将显示管道的详细信息。

表 10-58 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
创建时间	管道的创建时间。
描述	管道的描述信息。

----结束

10.5.10.3 编辑管道

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

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。

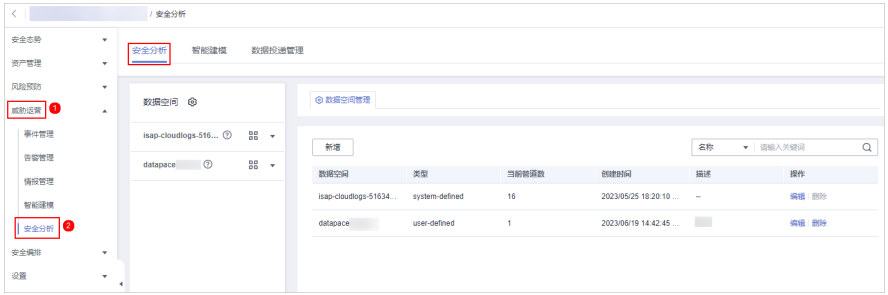
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-122 工作空间页面

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 10-123 进入安全分析页面



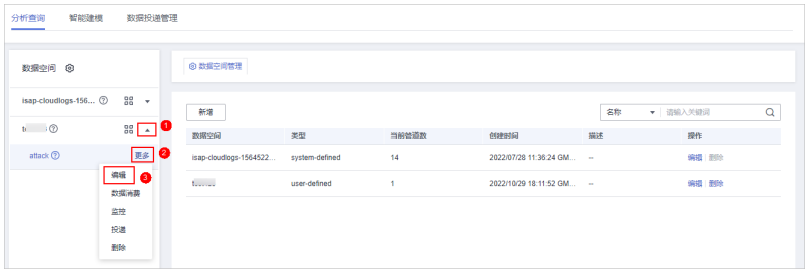
步骤5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的 ▼，展开已创建的管道。

版权所有 © 华为云计算技术有限公司

图 10-124 查看管道

步骤6 单击管道名称后的“更多 > 编辑”。

图 10-125 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10-59所示。

表 10-59 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

10.5.10.4 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。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

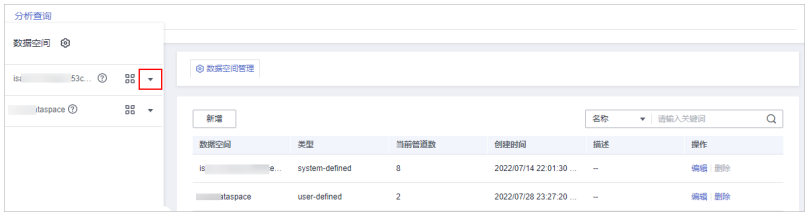
图 10-126 工作空间页面

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 10-127 进入安全分析页面

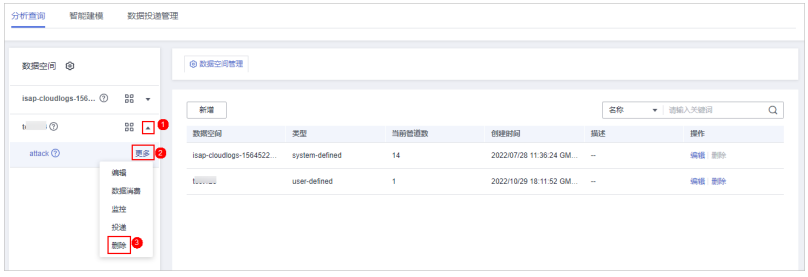
步骤5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的 ▼，展开已创建的管道。

图 10-128 查看管道



步骤6 单击管道名称后的“更多 > 删除”。

图 10-129 删除管道



版权所有 © 华为云计算技术有限公司

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

10.6 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。

安全云脑提供数据消费功能，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。

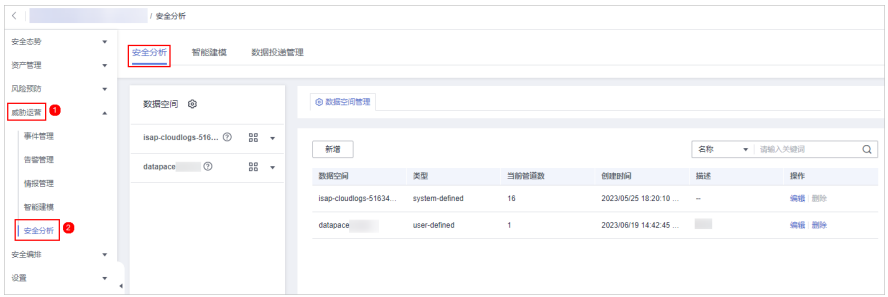
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-130 工作空间页面

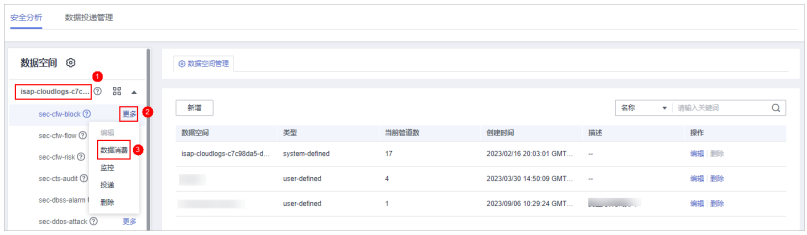
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-131 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 10-132 进入数据消费页面



版权所有 © 华为云计算技术有限公司

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10-60**所示。

表 10-60 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。

10.7 数据投递

10.7.1 新增数据投递

安全云脑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，安全云脑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）。

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

跨帐号投递仅支持投递到其他帐号管道中，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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

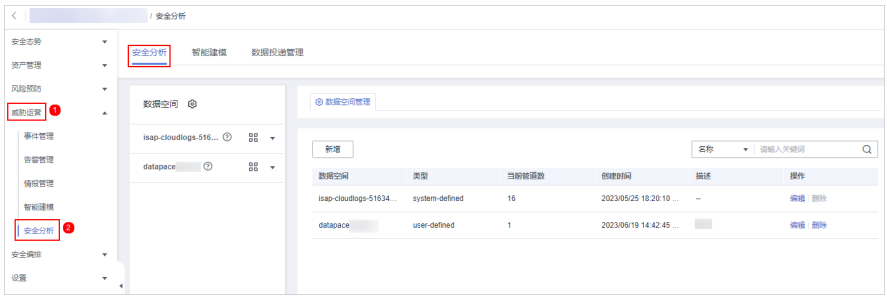
版权所有 © 华为云计算技术有限公司

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 10-133 工作空间页面

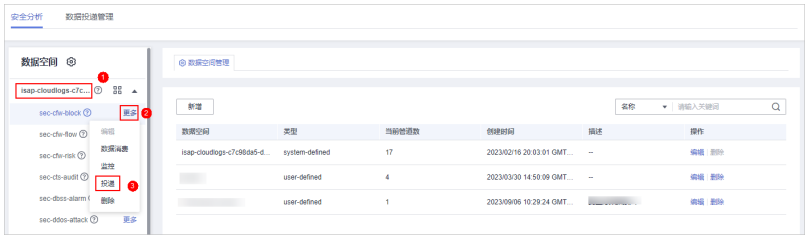
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-134 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 10-135 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 10-61 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**。

版权所有 © 华为云计算技术有限公司

表 10-62 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。
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帐号其他管道或其他帐号的管道中，请根据您的需要进行选择配置。
     - 本帐号投递：将当前管道数据投递到本帐号的其他管道中，参数配置说明如表10-63所示。

       表 10-63 配置数据目的-本帐号 PIPE

参数名称	参数说明
帐号类型	选择数据投递目的地的帐号类型，此处选择“本帐号”。
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。

     - 跨帐号投递：将当前管道数据投递到其他帐号的管道中，参数配置说明如表10-64所示。

       表 10-64 配置数据目的-跨帐号 PIPE

参数名称	参数说明
帐号类型	选择数据投递目的地的帐号类型，此处选择“跨帐号”。
投递类型	选择投递类型，此处选择PIPE。
帐号ID	输入目的PIPE所在帐号的ID。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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**。
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10-65**所示。
  投递到LTS中，需要已有可用的日志组和日志流。

  表 10-65 配置数据目的-LTS

参数名称	参数说明
帐号类型	选择数据投递目的地的帐号类型。投递到LTS服务仅支持选择“本帐号”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10-66**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 10-66 配置数据目的-OBS

参数名称	参数说明
帐号类型	选择数据投递目的地的帐号类型。投递到OBS服务仅支持选择“本帐号”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。

步骤8 单击“确定”。

----结束

 版权所有 © 华为云计算技术有限公司

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**数据投递授权**。

10.7.2 数据投递授权

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。

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帐号投递，则需要登录目的帐号进行授权操作。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-136 工作空间页面

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 10-137 数据投递授权

版权所有 © 华为云计算技术有限公司

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**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 10-67 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”。

10.7.3 查看数据投递情况

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

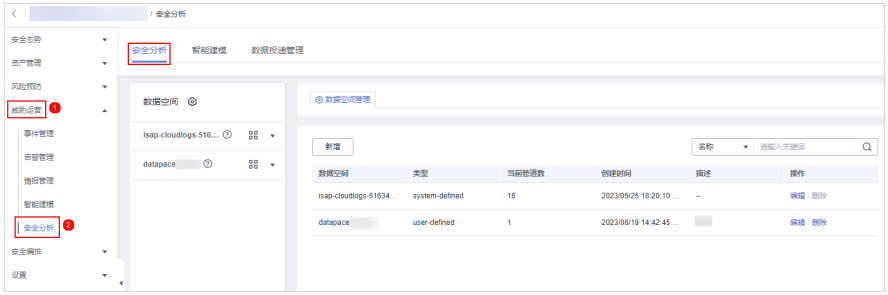
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 10-138 工作空间页面

版权所有 © 华为云计算技术有限公司

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 10-139 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 10-140 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。

版权所有 © 华为云计算技术有限公司

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

10.7.4 管理数据投递任务

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-141 工作空间页面

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 10-142 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。

版权所有 © 华为云计算技术有限公司

表 10-68 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-143 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 10-144 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-145 工作空间页面

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 10-146 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”。

挂起后，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

 版权所有 © 华为云计算技术有限公司

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 10-147 工作空间页面

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 10-148 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

10.8 数据监控

安全云脑数据监控功能支持监控安全云脑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：用于订阅安全云脑管道消息，一个管道可由多个订阅器进行订阅，安全云脑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，负责通过订阅器把安全云脑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。

版权所有 © 华为云计算技术有限公司

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

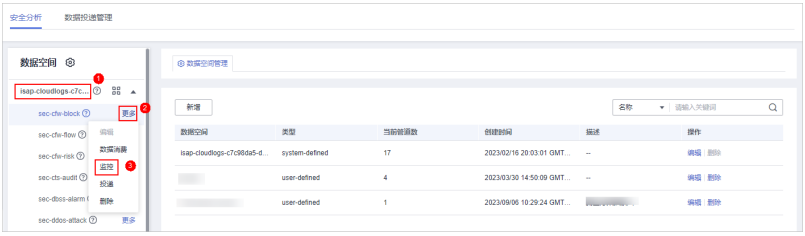
图 10-149 工作空间页面

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 10-150 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。

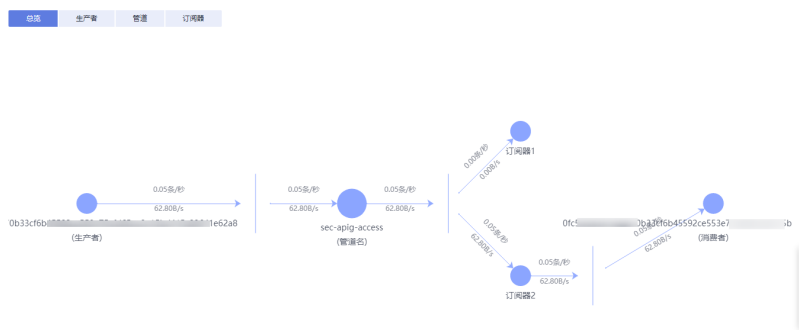
图 10-151 进入数据监控页面



步骤6 在数据管道的监控页面，查看监控指标。

版权所有 © 华为云计算技术有限公司

图 10-152 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

版权所有 © 华为云计算技术有限公司

11 安全编排

11.1 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（incidence）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。

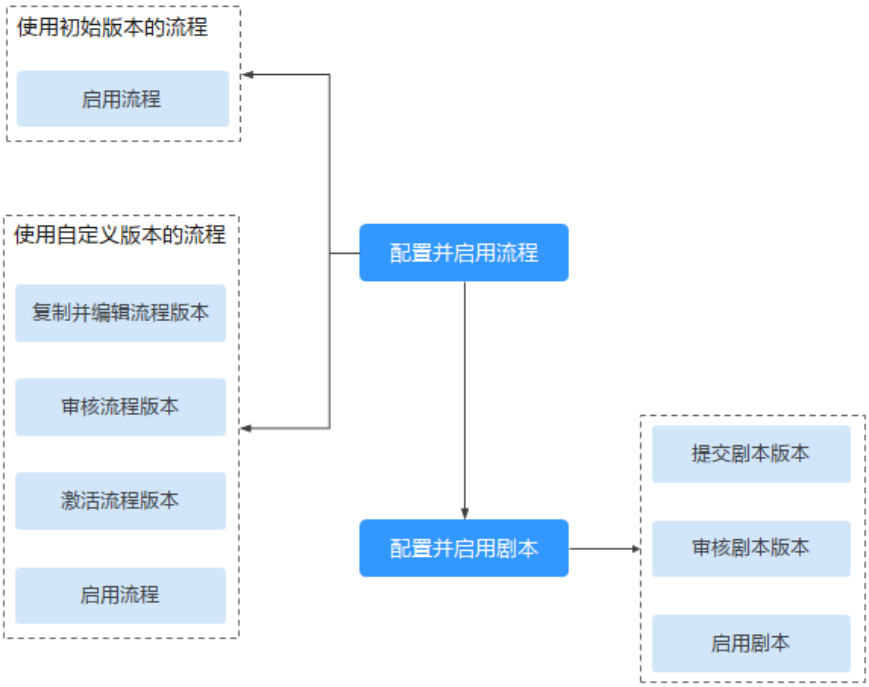
  它是将系统内部不同组件的安全功能通过可编程接口（API）封装后形成的安全能力（即应用）和人工检查点按照一定的逻辑关系组合到一起，以完成某个特定的安全运营过程和规程。

11.2 安全编排使用流程

安全编排的使用流程如下：

 版权所有 © 华为云计算技术有限公司

图 11-1 安全编排使用流程



1. **配置并启用流程**：启用需要的安全云脑内置的流程。

   安全云脑默认提供了“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）也已激活，只需要启用就可以在剧本中进行使用。

   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. **配置并启用剧本**：启用需要的安全云脑内置的剧本。

   安全云脑默认提供了“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，如需使用某个剧本，需要启用对应剧本。

   剧本支持存在多个剧本版本，您先需要提交并审核需要的剧本版本，才能启用对应的剧本。

11.3 配置并启用流程

安全云脑默认提供了“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）也已激活，如需使用某个流程的初始版本，仅需要启用对应流程即可。

同时，还支持对已有流程进行自定义编辑，使用自定义流程。

本章节主要介绍如何配置并启用流程。

- **启用初始版本的流程**
- **启用自定义版本的流程**

启用初始版本的流程

步骤1 登录管理控制台。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

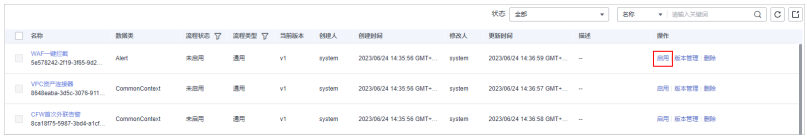
图 11-2 工作空间页面

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 11-3 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 11-4 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

启用自定义版本的流程

进入流程管理页面

步骤1 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。

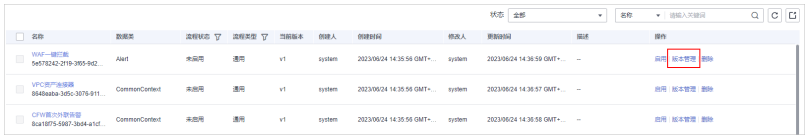
版权所有 © 华为云计算技术有限公司

图 11-5 流程管理页面

复制流程版本

步骤2 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 11-6 进入流程版本管理页面



步骤3 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4 在弹出的确认框中，单击“确认”，完成复制流程版本。

编辑并提交流程版本

步骤5 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6 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 11-1 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。
		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**任务中心**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11-2**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。

版权所有 © 华为云计算技术有限公司

参数名称			参数说明
	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 11-2 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。
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帐号中的IAM用户。设置后如有流程需审批，仅设置的责任人可在任务中心页面进行处理，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7 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”。

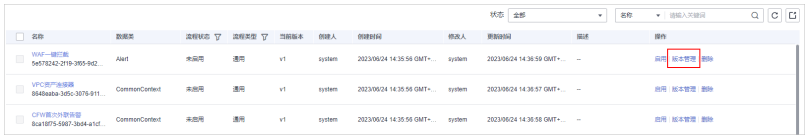
如果流程校验失败，请根据失败提示进行检查。

审核流程版本

 版权所有 © 华为云计算技术有限公司

步骤8 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 11-7 进入流程版本管理页面



步骤9 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10 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”，完成审核流程版本。

激活流程版本

步骤11 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12 在弹出确认框中，单击“确认”，完成激活操作。

启用流程

步骤13 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14 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

11.4 配置并启用剧本

安全云脑默认提供了“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，如需使用某个剧本，需要启用对应剧本。

本章节主要介绍配置并启用剧本。

前提条件

已启用对应流程，具体操作请参见**配置并启用流程**。

步骤一：提交剧本版本

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

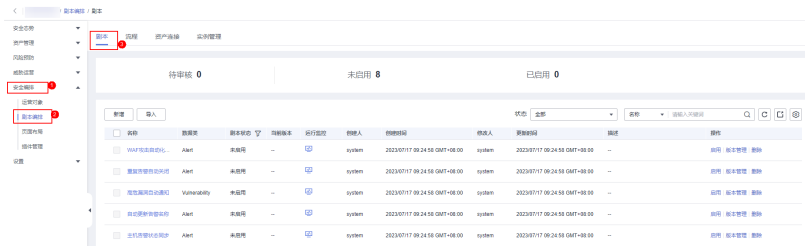
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 11-8 工作空间页面

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 11-9 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。

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

步骤二：审核剧本版本

步骤1 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤2 在版本管理页面中，单击“审核”，弹出审核剧本版本页面。

步骤3 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11-3所示。

表 11-3 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）。

版权所有 © 华为云计算技术有限公司

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4 单击“确定”，完成审核剧本版本。

----结束

步骤三：启用剧本

步骤1 在剧本管理页面中，单击待启用剧本所在行“操作”列的“启用”，弹出启用确认信息框。

步骤2 选择启用的剧本版本后，单击“确认”，完成剧本启用。

----结束

11.5 运营对象管理

11.5.1 数据类

11.5.1.1 查看已有数据类

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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

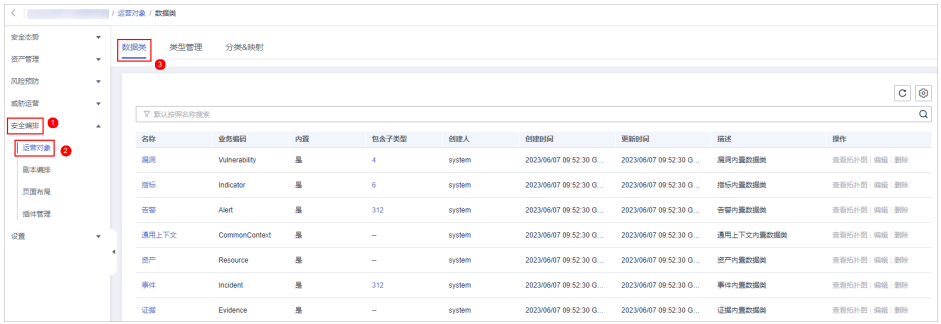
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-10 工作空间页面

步骤4 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。

版权所有 © 华为云计算技术有限公司

图 11-11 进入数据类管理页面



步骤5 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 11-4 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6 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

11.5.2 类型管理

11.5.2.1 管理告警类型

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。

版权所有 © 华为云计算技术有限公司

- **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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-13 进入类型管理页面

步骤5 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6 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11-5**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。

版权所有 © 华为云计算技术有限公司

图 11-14 查看告警类型

表 11-5 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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-15 工作空间页面

步骤4 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。

版权所有 © 华为云计算技术有限公司

图 11-16 进入类型管理页面

步骤5 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6 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 11-6 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。名称需遵循大驼峰命名规范，例如TypeName。
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。名称需遵循大驼峰命名规范，例如SubType。
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。
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7 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

 版权所有 © 华为云计算技术有限公司

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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-18 进入类型管理页面

步骤5 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6 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7 在绑定布局编辑框中，选择需要关联的布局。

步骤8 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 登录管理控制台。

版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-20 进入类型管理页面

步骤5 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6 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7 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8 在编辑告警类型页面中，修改告警类型的参数信息。

表 11-7 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。

版权所有 © 华为云计算技术有限公司

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。

步骤9 在页面右下角单击“确认”。

----结束

管理已有告警类型

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-22 进入类型管理页面

步骤5 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6 在告警类型管理页面中，对告警类型进行管理。

版权所有 © 华为云计算技术有限公司

表 11-8 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

11.5.2.2 管理事件类型

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 登录管理控制台。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-24 进入类型管理页面

步骤5 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6 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11-9所示。

图 11-25 查看事件类型

表 11-9 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-26 工作空间页面

步骤4 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 11-27 进入类型管理页面

步骤5 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6 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。

版权所有 © 华为云计算技术有限公司

表 11-10 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7 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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-28 工作空间页面

版权所有 © 华为云计算技术有限公司

步骤4 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 11-29 进入类型管理页面

步骤5 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6 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7 在绑定布局编辑框中，选择需要关联的布局。

步骤8 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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-30 工作空间页面

步骤4 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。

 版权所有 © 华为云计算技术有限公司

图 11-31 进入类型管理页面

步骤5 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6 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7 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8 在编辑事件类型页面中，编辑参数信息。

表 11-11 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。
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9 在页面右下角单击“确认”。

----结束

管理已有事件类型

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

版权所有 © 华为云计算技术有限公司

图 11-32 工作空间页面

步骤4 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 11-33 进入类型管理页面

步骤5 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6 在事件类型管理页面中，对事件类型进行管理。

表 11-12 管理已有事件类型

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

版权所有 © 华为云计算技术有限公司

11.5.2.3 管理威胁情报

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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-34 工作空间页面

步骤4 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 11-35 进入类型管理页面

步骤5 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。

版权所有 © 华为云计算技术有限公司

步骤6 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11-13所示。

图 11-36 查看威胁情报

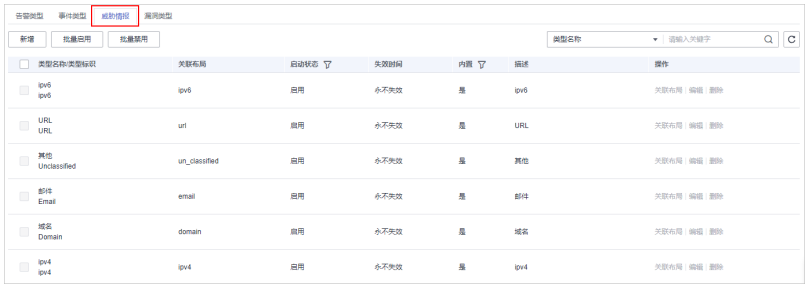


表 11-13 威胁情报参数说明

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。
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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

版权所有 © 华为云计算技术有限公司

步骤4 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 11-38 进入类型管理页面

步骤5 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6 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 11-14 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7 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

 版权所有 © 华为云计算技术有限公司

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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-40 进入类型管理页面

步骤5 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6 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7 在绑定布局编辑框中，选择需要关联的布局。

步骤8 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 登录管理控制台。

版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-41 工作空间页面

步骤4 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 11-42 进入类型管理页面

步骤5 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6 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7 在编辑页面中，编辑对应类型的参数信息。

表 11-15 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。

版权所有 © 华为云计算技术有限公司

步骤8 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 登录管理控制台。

步骤2 单击页面左上方的 ，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-43 工作空间页面

步骤4 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 11-44 进入类型管理页面

步骤5 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6 在威胁情报类型管理页面中，对威胁情报类型进行管理。

表 11-16 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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。
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

11.5.2.4 管理漏洞类型

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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-45 工作空间页面

 版权所有 © 华为云计算技术有限公司

步骤4 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 11-46 进入类型管理页面

步骤5 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6 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11-17所示。

图 11-47 查看漏洞类型

表 11-17 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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

 版权所有 © 华为云计算技术有限公司

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 工作空间页面

步骤4 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 11-49 进入类型管理页面

步骤5 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6 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 11-18 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7 在页面右下角单击“确认”，完成新增操作。

 版权所有 © 华为云计算技术有限公司

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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-51 进入类型管理页面

步骤5 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6 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7 在绑定布局编辑框中，选择需要关联的布局。

步骤8 单击“确认”。

----结束

 版权所有 © 华为云计算技术有限公司

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 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-53 进入类型管理页面

步骤5 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6 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7 在编辑页面中，编辑对应类型的参数信息。

表 11-19 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**。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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8 在页面右下角单击“确认”。

----结束

管理已有漏洞类型

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-55 进入类型管理页面

步骤5 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6 在漏洞类型管理页面中，对漏洞类型进行管理。

版权所有 © 华为云计算技术有限公司

表 11-20 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。
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

11.5.3 分类&映射

11.5.3.1 创建分类映射

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分类映射。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

版权所有 © 华为云计算技术有限公司

步骤4 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 11-57 进入分类&映射管理页面

步骤5 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6 在创建分类映射页面中，配置分类映射参数信息。

图 11-58 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11-21所示。

   表 11-21 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。
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。

版权所有 © 华为云计算技术有限公司

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

11.5.3.2 管理分类映射

本章节介绍如何执行**查看已创建的分类映射**、**删除分类映射**等操作。

约束与限制

- 系统内置分类映射默认处于启用状态，且暂**不支持**进行编辑、删除操作。
- 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。
- 非内置分类映射暂不支持启用/禁用操作。

查看已创建的分类映射

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-59 工作空间页面

步骤4 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 11-60 进入分类&映射管理页面

步骤5 在分类映射管理页面中，查看已创建分类映射的详细信息。

版权所有 © 华为云计算技术有限公司

表 11-22 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6 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

复制已创建的分类映射

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-62 进入分类&映射管理页面

版权所有 © 华为云计算技术有限公司

步骤5 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6 在弹出的确认框中，编辑复制项名称，并单击“确认”。

----结束

启用分类映射

说明

自定义新增的分类映射暂不支持启用操作。

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-63 工作空间页面

步骤4 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 11-64 进入分类&映射管理页面

步骤5 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。

----结束

禁用分类映射

说明

自定义新增的分类映射暂不支持禁用操作。

步骤1 登录管理控制台。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

步骤4 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 11-66 进入分类&映射管理页面

步骤5 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。

----结束

删除分类映射

说明

暂不支持删除系统内置分类映射。

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-67 工作空间页面

版权所有 © 华为云计算技术有限公司

步骤4 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 11-68 进入分类&映射管理页面

步骤5 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”。

步骤6 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

11.6 剧本编排管理

11.6.1 剧本

11.6.1.1 提交剧本版本

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

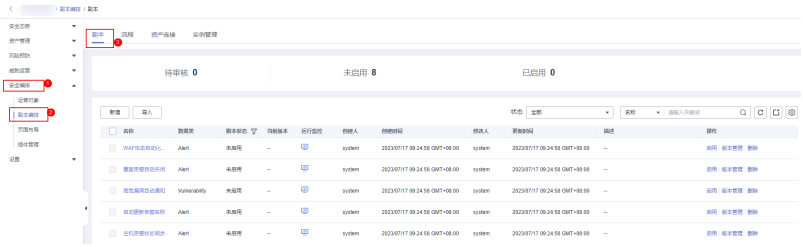
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-69 工作空间页面

版权所有 © 华为云计算技术有限公司

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 11-70 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。

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**审核剧本版本**。

11.6.1.2 审核剧本版本

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

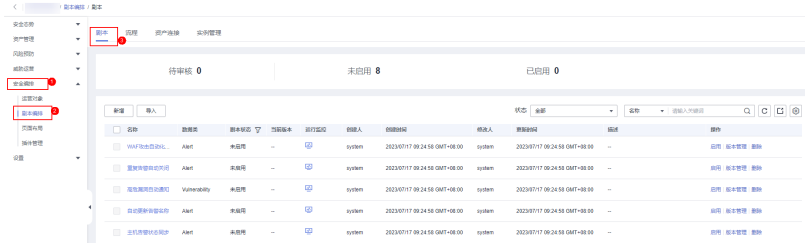
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-71 工作空间页面

版权所有 © 华为云计算技术有限公司

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 11-72 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。

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11-23所示。

表 11-23 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**启用剧本**。

11.6.1.3 启用剧本

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**。

版权所有 © 华为云计算技术有限公司

操作步骤

步骤1 登录管理控制台。

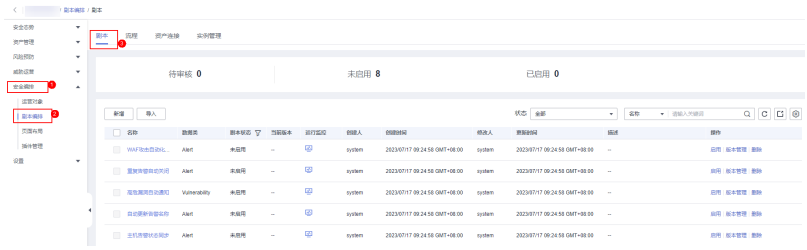
步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-73 工作空间页面

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 11-74 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

11.6.1.4 管理剧本

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 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

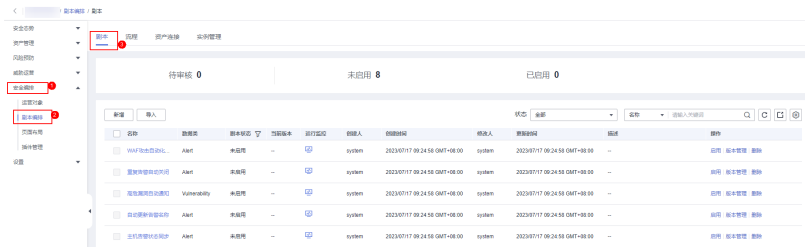
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 11-75 工作空间页面

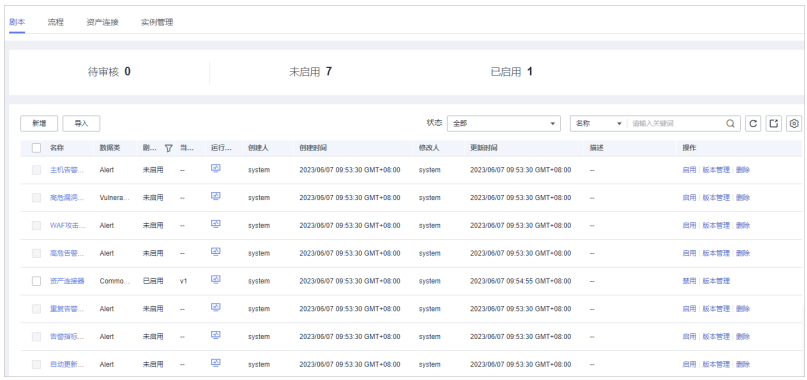
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-76 进入剧本管理页面



步骤5 在剧本管理页面，查看剧本的信息。

图 11-77 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 11-24 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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6 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 登录管理控制台。

步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

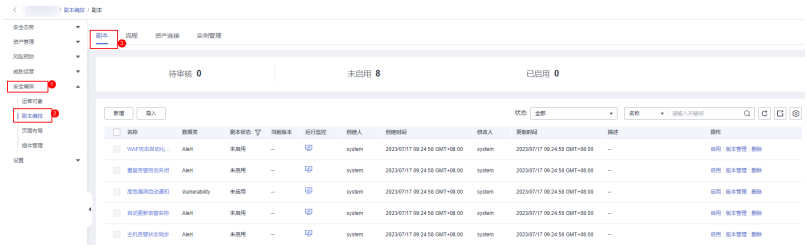
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-78 工作空间页面

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。

 版权所有 © 华为云计算技术有限公司

图 11-79 进入剧本管理页面



步骤5 在剧本管理列表右上角单击“导入”，弹出导入剧本窗口。

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

导出剧本信息

说明

安全云脑支持导出“剧本状态”为“已启用”的剧本。

步骤1 登录管理控制台。

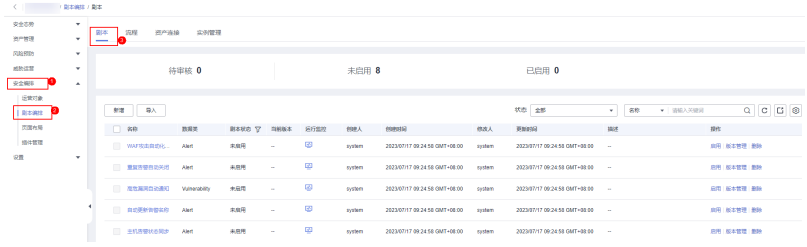
步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 11-81 进入剧本管理页面



步骤5 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6 在弹出的确认框中，单击“确认”，导出剧本信息到本地。

----结束

版权所有 © 华为云计算技术有限公司

禁用剧本

步骤1 登录管理控制台。

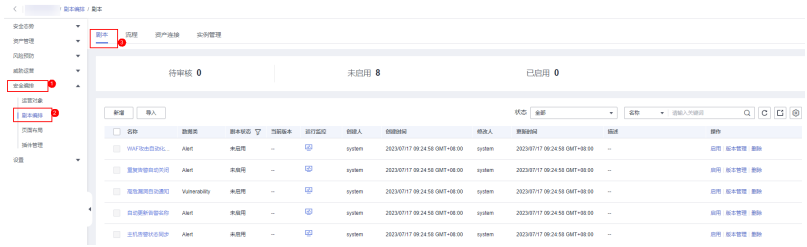
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-82 工作空间页面

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 11-83 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

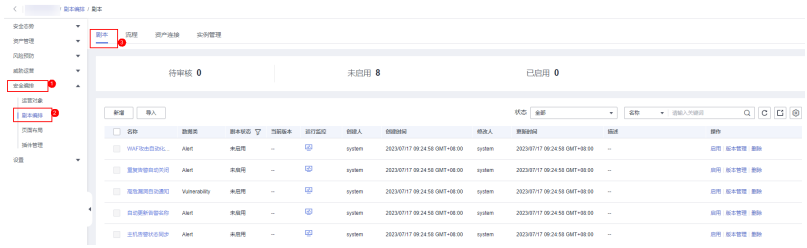
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

版权所有 © 华为云计算技术有限公司

图 11-84 工作空间页面

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 11-85 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

11.6.1.5 管理剧本版本

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

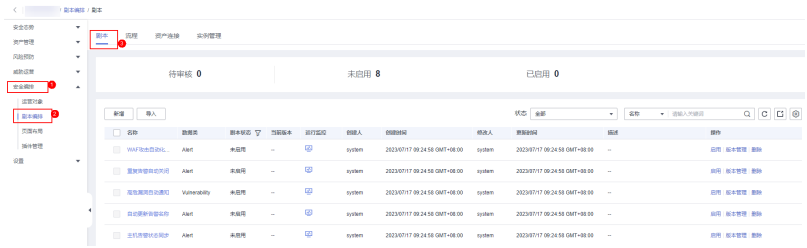
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-86 工作空间页面

版权所有 © 华为云计算技术有限公司

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 11-87 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。

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

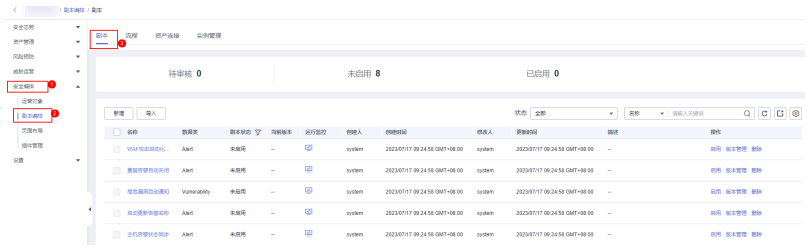
仅支持对版本状态为“未提交”的剧本版本进行编辑。

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

步骤3 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 11-88 进入剧本管理页面



步骤4 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

步骤5 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6 在剧本版本编辑页面，编辑版本信息。

步骤7 单击“确定”，完成剧本的编辑。

----结束

版权所有 © 华为云计算技术有限公司

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。

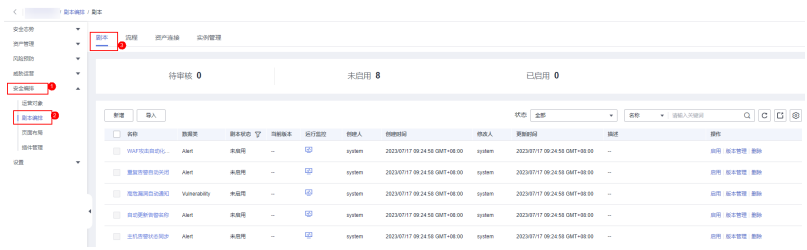
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-89 工作空间页面

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 11-90 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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

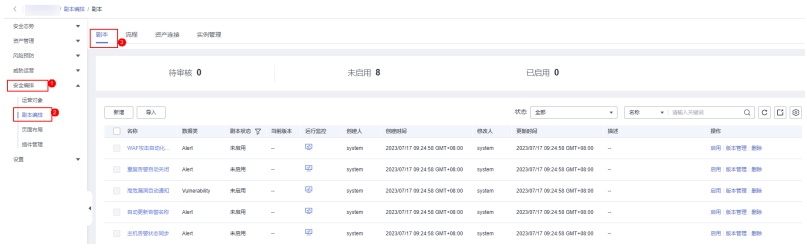
 版权所有 © 华为云计算技术有限公司

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 11-91 工作空间页面

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 11-92 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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

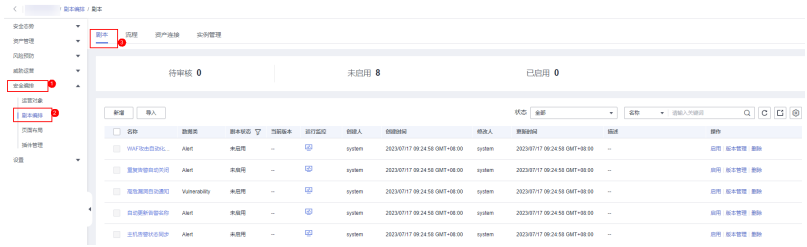
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-93 工作空间页面

版权所有 © 华为云计算技术有限公司

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 11-94 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。

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

11.6.2 流程

11.6.2.1 审核流程版本

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

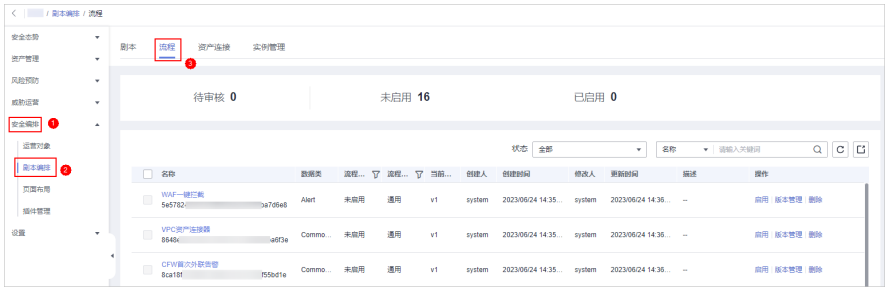
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-95 工作空间页面

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。

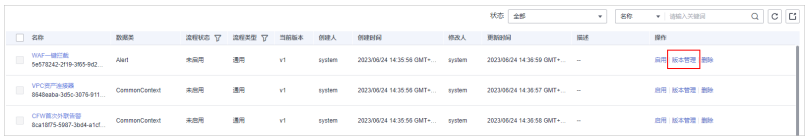
版权所有 © 华为云计算技术有限公司

图 11-96 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 11-97 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11-25**所示。

表 11-25 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**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**启用流程**。

11.6.2.2 启用流程

本章节主要介绍如何启用流程。

 版权所有 © 华为云计算技术有限公司

前提条件

已激活流程版本，具体操作请参见**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

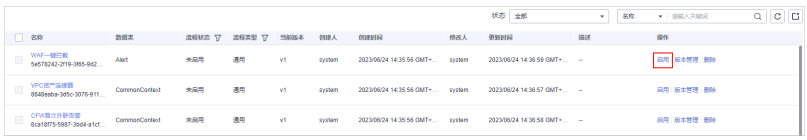
图 11-98 工作空间页面

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 11-99 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 11-100 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

11.6.2.3 管理流程

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**。

版权所有 © 华为云计算技术有限公司

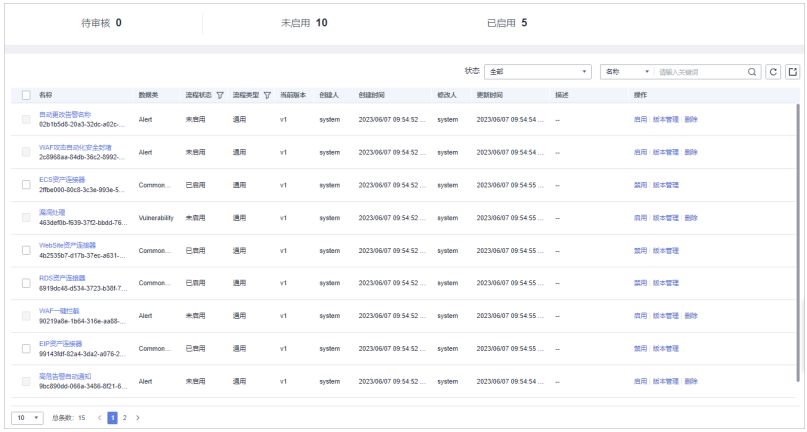
查看流程

步骤1 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 11-101 流程管理页面

步骤2 在流程管理页面中，查看已创建流程的信息。

图 11-102 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 11-26 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。
创建人	创建该流程的用户。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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3 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。

----结束

导入流程

步骤1 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 11-103 流程管理页面

步骤2 在流程管理列表右上角单击“导入”，弹出导入流程窗口。

步骤3 单击“添加文件”，并选择待导入文件。

步骤4 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 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。

版权所有 © 华为云计算技术有限公司

图 11-104 流程管理页面

步骤2 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3 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

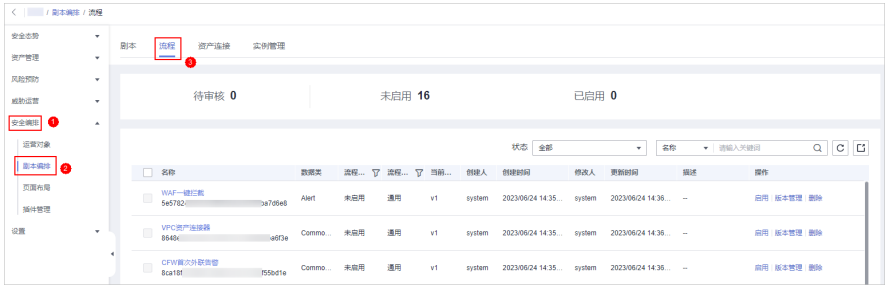
说明

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 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 11-105 流程管理页面



步骤2 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3 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 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。

版权所有 © 华为云计算技术有限公司

图 11-106 流程管理页面

步骤2 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3 在弹出的确认框中，单击“确认”，完成流程禁用。

----结束

11.6.2.4 管理流程版本

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**。

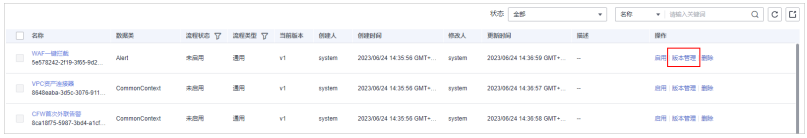
复制流程版本

步骤1 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 11-107 流程管理页面

步骤2 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 11-108 进入流程版本管理页面



步骤3 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4 在弹出的确认框中，单击“确认”，完成复制流程版本。

----结束

版权所有 © 华为云计算技术有限公司

编辑流程版本

说明

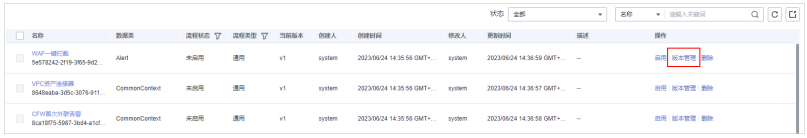
支持对“版本状态”为“待提交”或“审核驳回”的流程版本进行编辑。

步骤1 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 11-109 流程管理页面

步骤2 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 11-110 进入流程版本管理页面



步骤3 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4 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 11-27 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。
		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**任务中心**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11-28**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。

版权所有 © 华为云计算技术有限公司

参数名称			参数说明
	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 11-28 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。
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帐号中的IAM用户。设置后如有流程需审批，仅设置的责任人可在任务中心页面进行处理，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5 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

 版权所有 © 华为云计算技术有限公司

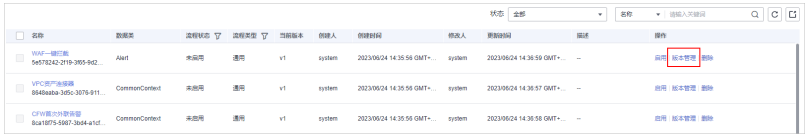
提交流程版本

步骤1 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 11-111 流程管理页面

步骤2 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 11-112 进入流程版本管理页面



步骤3 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 11-113 提交流程版本

步骤4 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

版权所有 © 华为云计算技术有限公司

激活/失活流程版本

说明

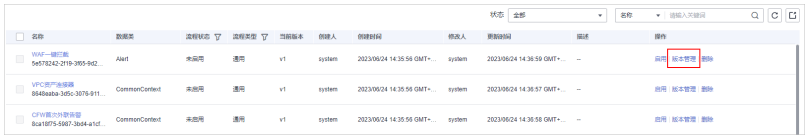
- 只有版本状态为未激活的流程版本才能激活。
- 每个流程只允许存在一个激活版本。
- 激活当前版本后，之前激活的版本将会失活。例如，此次激活V2版本，则处于已激活状态的V1版本将被取消激活，更新为未激活状态。

步骤1 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 11-114 流程管理页面

步骤2 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 11-115 进入流程版本管理页面



步骤3 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 11-116 取消激活示例

步骤4 在弹出确认框中，单击“确认”，完成激活/失活操作。

----结束

版权所有 © 华为云计算技术有限公司

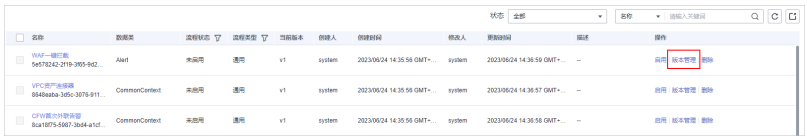
删除流程版本

步骤1 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 11-117 流程管理页面

步骤2 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 11-118 进入流程版本管理页面



步骤3 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

11.6.3 资产连接

11.6.3.1 新增资产连接

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**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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

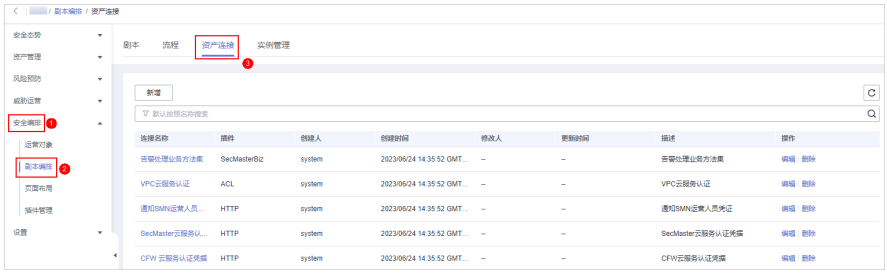
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

版权所有 © 华为云计算技术有限公司

图 11-119 工作空间页面

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 11-120 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11-29**所示。

表 11-29 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**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

11.6.3.2 管理资产连接

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

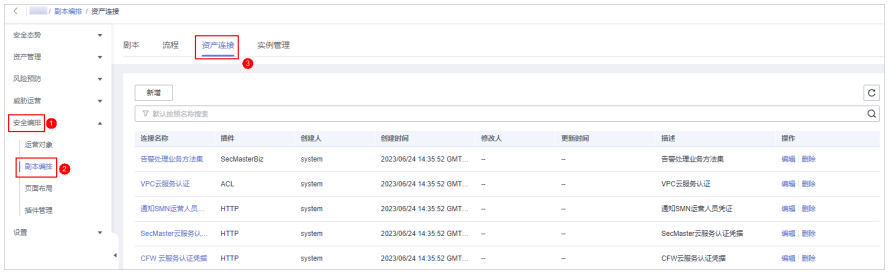
版权所有 © 华为云计算技术有限公司

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 11-121 工作空间页面

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 11-122 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 11-123 查看资产连接信息

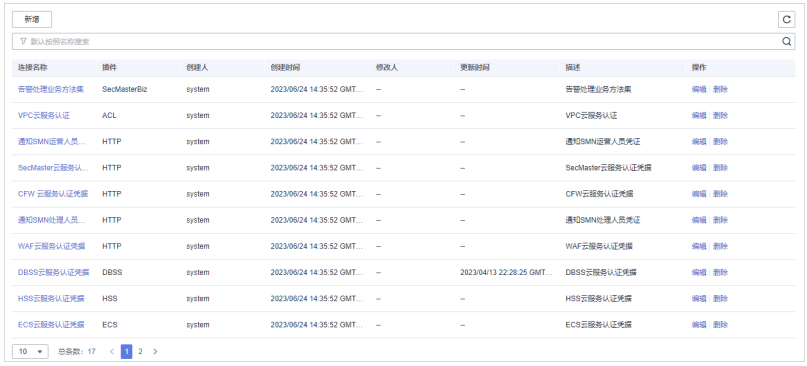


表 11-30 资产连接参数说明

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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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。

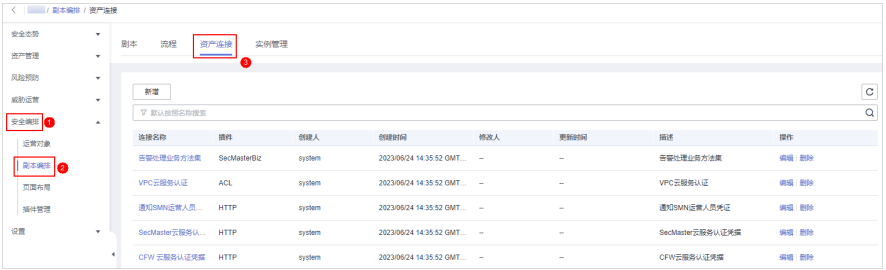
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-124 工作空间页面

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 11-125 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11-31所示。

版权所有 © 华为云计算技术有限公司

表 11-31 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**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。

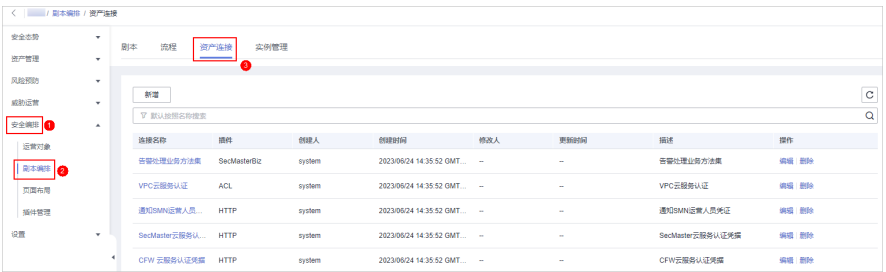
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 11-127 资产连接管理页面



版权所有 © 华为云计算技术有限公司

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

11.6.4 实例管理

11.6.4.1 查看剧本实例监控

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

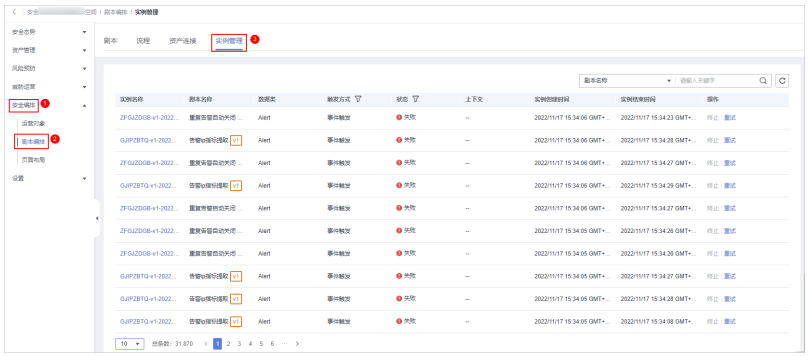
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 11-128 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 11-129 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11-32所示。

图 11-130 实例信息

表 11-32 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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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

11.7 页面布局管理

11.7.1 查看已有布局模板

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。

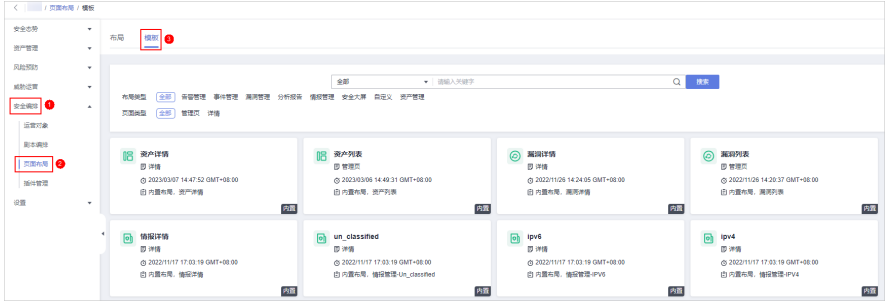
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 工作空间页面

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 11-132 进入布局模板页面



版权所有 © 华为云计算技术有限公司

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

11.7.2 管理已有布局

本章节将介绍如何**查看已有布局**、**删除布局**。

查看已有布局

步骤1 登录管理控制台。

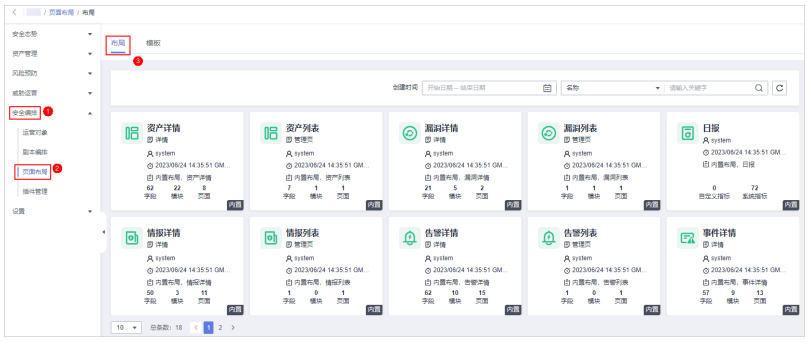
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-133 工作空间页面

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 11-134 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

版权所有 © 华为云计算技术有限公司

删除布局

步骤1 登录管理控制台。

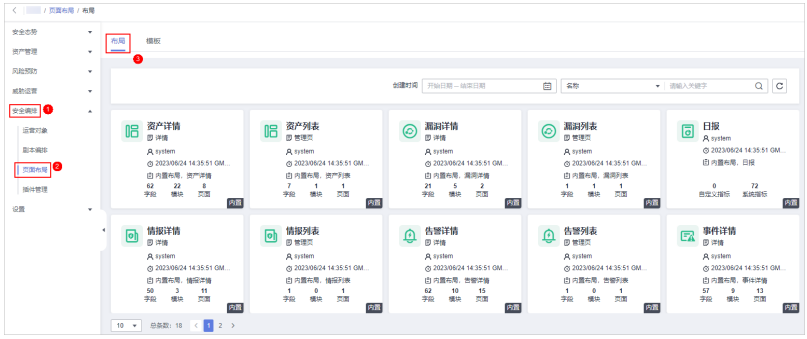
步骤2 单击页面左上方的 ，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-135 工作空间页面

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 11-136 进入布局管理页面



步骤5 在布局管理页面，将鼠标放在目标布局上，并单击布局右上角 ，弹出删除确认页面。

步骤6 单击“确认”，删除布局。

----结束

11.8 插件管理

11.8.1 概述

安全云脑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。

 版权所有 © 华为云计算技术有限公司

- **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安全云脑，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。

11.8.2 查看插件详情

本章节介绍如何查看安全云脑内置插件及详细信息。

操作步骤

步骤1 登录管理控制台。

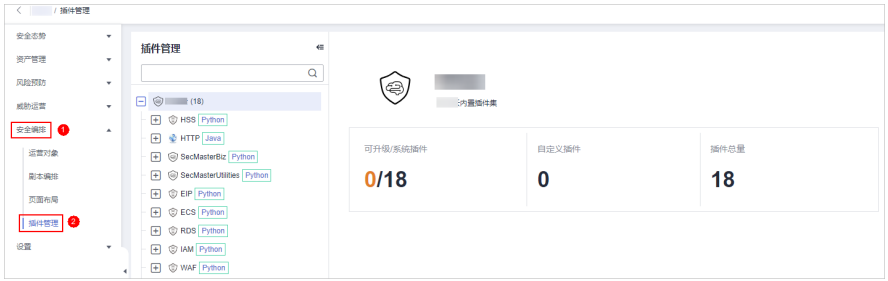
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 11-137 工作空间页面

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 11-138 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

版权所有 © 华为云计算技术有限公司

12 设置

12.1 数据采集

12.1.1 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帐号登录。

使用流程

表 12-1 数据采集使用流程

操作步骤		说明
1	**购买ECS**	购买指定版本的ECS主机。
2	**安装Agent**	在主机上安装Agent。
3	**新增节点**	新增采集管理节点。
4	**配置组件**	配置组件相关信息。
5	**新增数据连接**	新增数据连接来源和目的。
6	**（可选）配置解析器**	配置解析器，将数据通过自定义解析方式进行采集。
7	**新增采集通道**	新增数据采集通道。

版权所有 © 华为云计算技术有限公司

支持的操作系统

数据采集的Agent目前仅支持运行在EulerOS的Linux系统x86_64架构的主机上。支持版本如表12-2所示：

表 12-2 支持的 EulerOS 版本

版本	购买ECS时，可选择的版本
EulerOS 2.5	EulerOS 2.5 64bit for Tenant 20210227(40GB) EulerOS 2.5 64bit for Tenant 20220321 base 2.5.11(40GB) EulerOS 2.5 64bit for Tenant 20220906 base 2.5.12(40GB) EulerOS 2.5 64bit for Tenant 20221130 base 2.5.13(40GB) Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.11-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.12-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.13-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.14-x86_64-Standard（制作资源专用不支持密码注入）(20GB)
EulerOS 2.9	Public-CAD-EulerOS-BaseTemplate-2.9.6-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.7-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.8-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.9-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.10-x86_64-Standard（制作资源专用不支持密码注入）(20GB)
EulerOS 2.10	Public-CAD-EulerOS-BaseTemplate-2.10.5-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.10.6-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.10.7-x86_64-Standard（制作资源专用不支持密码注入）(20GB)

12.1.2 购买 ECS

本章节介绍如何购买支持安装数据采集Agent对应版本的ECS主机。

版权所有 © 华为云计算技术有限公司

前提条件

已获取登录管理控制台的IAM帐号、用户名和密码。

操作步骤

购买弹性云服务器，详细操作请参见《 弹性云服务器用户指南 》。

版权所有 © 华为云计算技术有限公司

注意

数据采集的Agent目前仅支持运行在EulerOS的Linux系统x86_64架构的主机上。购买时，需注意操作系统和版本的选择，支持的版本说明如表12-3所示。

图 12-1 选择操作系统版本

表 12-3 支持的 EulerOS 版本

版本	购买ECS时，可选择的版本
EulerOS 2.5	EulerOS 2.5 64bit for Tenant 20210227(40GB) EulerOS 2.5 64bit for Tenant 20220321 base 2.5.11(40GB) EulerOS 2.5 64bit for Tenant 20220906 base 2.5.12(40GB) EulerOS 2.5 64bit for Tenant 20221130 base 2.5.13(40GB) Public-CAD-EulerOS-BaseTemplate-2.5.9-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.11-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.12-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.13-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.5.14-x86_64-Standard（制作资源专用不支持密码注入）(20GB)
EulerOS 2.9	Public-CAD-EulerOS-BaseTemplate-2.9.6-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.7-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.8-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.9-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.9.10-x86_64-Standard（制作资源专用不支持密码注入）(20GB)
EulerOS 2.10	Public-CAD-EulerOS-BaseTemplate-2.10.5-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.10.6-x86_64-Standard（制作资源专用不支持密码注入）(20GB) Public-CAD-EulerOS-BaseTemplate-2.10.7-x86_64-Standard（制作资源专用不支持密码注入）(20GB)

版权所有 © 华为云计算技术有限公司

后续处理

ECS购买完成后，需要安装Agent，详细操作请参见**安装Agent**。

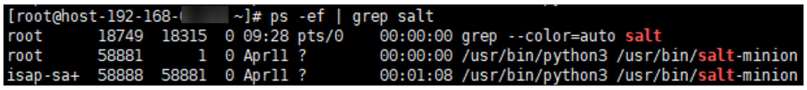
12.1.3 安装 Agent

本章节介绍如何安装Agent。

前提条件

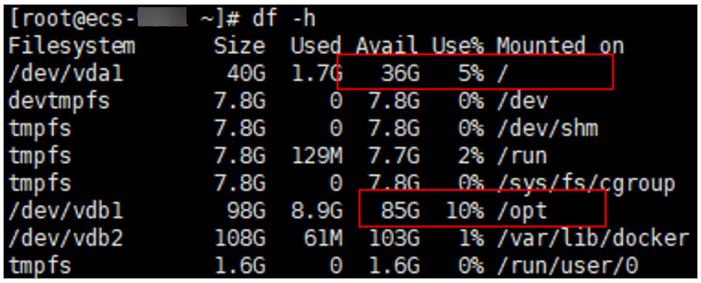
- 已购买ECS。
- 已获取登录管理控制台的IAM帐号、用户名和密码。
- 安装Agent前预检查：
  a. 安装Agent前，执行**ps -ef | grep salt**命令，检查主机之前的salt-minion进程是否残留。
     - 如果有，请先关闭。
     - 如果没有，请继续执行**b**。

     图 12-2 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 12-3 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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

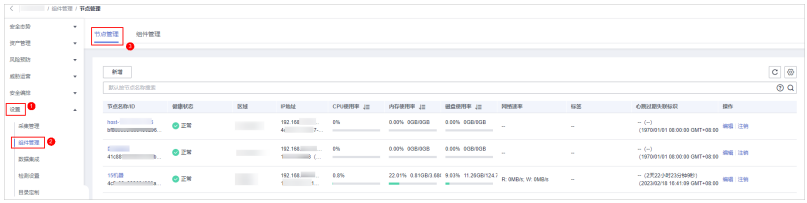
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

 版权所有 © 华为云计算技术有限公司

图 12-4 工作空间页面

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。

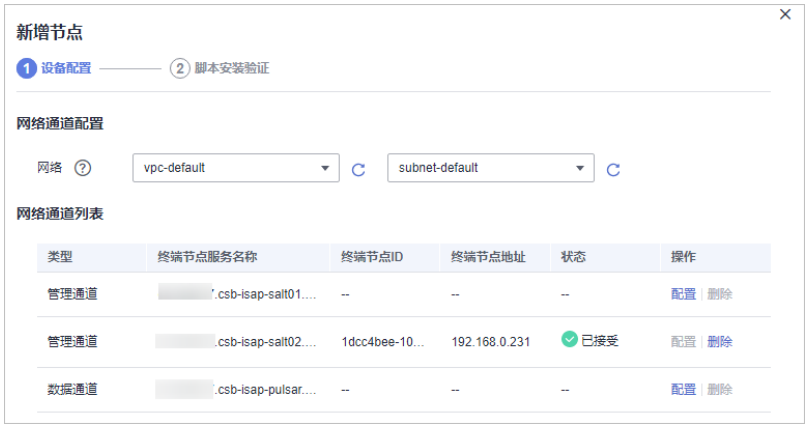
图 12-5 进入节点管理页面



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 在新增节点页面中，配置设备。

图 12-6 新增节点



1. 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。
2. 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”。

步骤7 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。

步骤8 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帐号在主机中安装Agent。

步骤9 执行**cd /opt/cloud**命令，进入安装目录。

 版权所有 © 华为云计算技术有限公司

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。

步骤10 粘贴复制的**步骤7**复制的安装命令，以root权限执行，在ECS中安装Agent。

步骤11 根据界面提示，输入登录控制台的IAM帐号和密码。

步骤12 若界面回显信息与如下信息类似，则表示Agent安装成功。

```
install isap-agent successfully
```

----结束

后续处理

Agent安装完成后，需要在控制台中新增节点，详细操作请参见**新增节点**。

相关操作

Agent安装失败问题排查

12.1.4 新增节点

本章节将介绍如何新增节点。

前提条件

已在主机上安装Agent。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

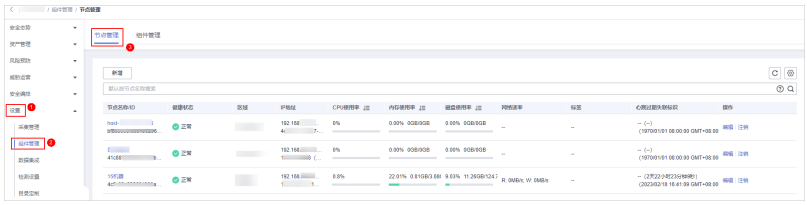
步骤3 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-7 工作空间页面

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。

 版权所有 © 华为云计算技术有限公司

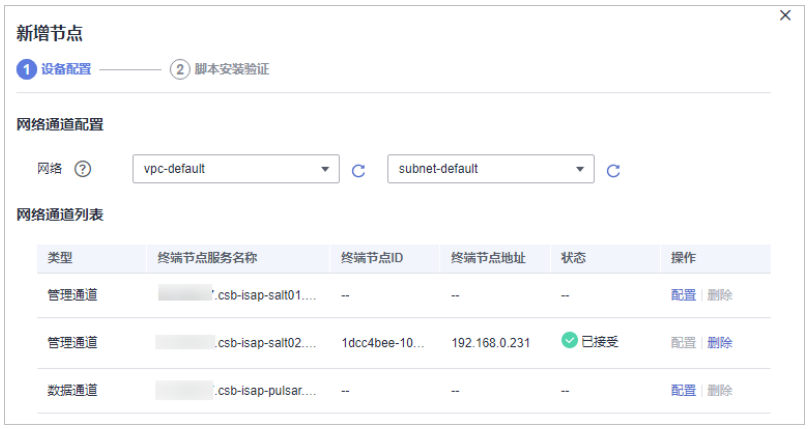
图 12-8 进入节点管理页面



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 在新增节点页面中，配置设备。

图 12-9 新增节点



1. 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。
2. 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”。

步骤7 单击页面右下角“下一步”，进入“脚本安装验证”页面。

步骤8 确认已安装后，单击页面右下角“确认”。

如未安装请参照**安装Agent**进行处理。

----结束

12.1.5 配置组件

本章节将介绍如何配置组件相关信息。

前提条件

已新增节点。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

版权所有 © 华为云计算技术有限公司

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 12-10 工作空间页面

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

后续处理

新增节点完成后，需要进行新增连接操作，详细操作请参见**新增连接**。

12.1.6 新增连接

本章节主要介绍如何新增连接。

前提条件

已配置组件。

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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-11 工作空间页面

版权所有 © 华为云计算技术有限公司

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 12-12 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

后续处理

新增连接完成后，可以根据需要确认是否需要配置解析器，详细操作请参见**配置解析器**。

如果无需配置，请直接新增采集通道，详细操作请参见**新增采集通道**。

12.1.7 配置解析器

安全云脑支持将数据通过自定义解析方式进行采集。

本章节主要介绍如何配置解析器。

前提条件

已新增连接，详细操作请参见**新增连接**。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

 版权所有 © 华为云计算技术有限公司

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 12-13 工作空间页面

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 12-14 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 12-4 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。

 版权所有 © 华为云计算技术有限公司

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 12-5 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

后续处理

解析器配置完成后，需要新增采集通道，详细操作请参见**新增采集通道**。

12.1.8 新增采集通道

本章节主要介绍如何新增采集通道。

前提条件

新增采集通道前，需先新增连接。

操作步骤

步骤1 登录管理控制台。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-15 工作空间页面

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 12-16 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 12-6 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。

版权所有 © 华为云计算技术有限公司

参数名称		参数说明
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**管理解析器**。

图 12-17 解析器配置

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

12.1.9 采集管理

版权所有 © 华为云计算技术有限公司

12.1.9.1 管理连接

本章节主要介绍如何执行**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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-18 工作空间页面

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 12-19 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 12-7 连接管理参数说明

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。

版权所有 © 华为云计算技术有限公司

参数名称	参数说明
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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-20 工作空间页面

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 12-21 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。

 版权所有 © 华为云计算技术有限公司

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-22 工作空间页面

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 12-23 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

12.1.9.2 管理解析器

本章节主要介绍如何执行**查看解析器管理信息**、**编辑解析器**、**删除解析器**操作。

查看解析器管理信息

步骤1 登录管理控制台。

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 12-24 工作空间页面

步骤3 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。

 版权所有 © 华为云计算技术有限公司

图 12-25 进入解析器管理页面

步骤4 在解析器管理页面中，查看解析器的详细信息。

表 12-8 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5 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6 在模板列表页面中，查看解析器模板信息。

表 12-9 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

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

版权所有 © 华为云计算技术有限公司

图 12-26 工作空间页面

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 12-27 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 12-10 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

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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。

 版权所有 © 华为云计算技术有限公司

图 12-28 工作空间页面

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 12-29 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

12.1.9.3 管理采集通道

本章节主要介绍如何执行**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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-30 工作空间页面

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。

版权所有 © 华为云计算技术有限公司

图 12-31 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 12-11 采集通道参数说明

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-32 工作空间页面

版权所有 © 华为云计算技术有限公司

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 12-33 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。

图 12-34 基础配置

表 12-12 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**管理解析器**。

 版权所有 © 华为云计算技术有限公司

图 12-35 解析器配置

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-36 工作空间页面

版权所有 © 华为云计算技术有限公司

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 12-37 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 > 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-38 工作空间页面

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 12-39 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”列的启用/停止/重启。

步骤6 在弹出的确认框中单击“确认”。

----结束

版权所有 © 华为云计算技术有限公司

12.1.9.4 管理采集节点

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。

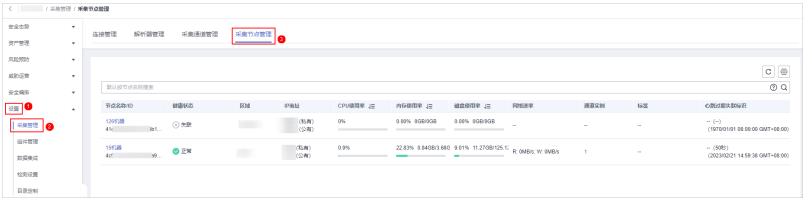
步骤2 单击页面左上方的，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-40 工作空间页面

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 12-41 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 12-13 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。

版权所有 © 华为云计算技术有限公司

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

12.1.10 组件管理

12.1.10.1 管理节点

本章节将介绍如何执行**查看节点管理信息**、**编辑节点**、**注销节点**操作。

查看节点管理信息

步骤1 登录管理控制台。

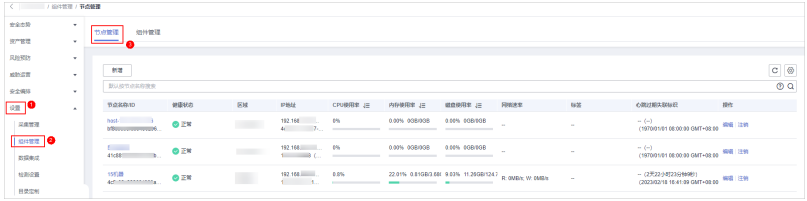
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-42 工作空间页面

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 12-43 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。

版权所有 © 华为云计算技术有限公司

表 12-14 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。
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。

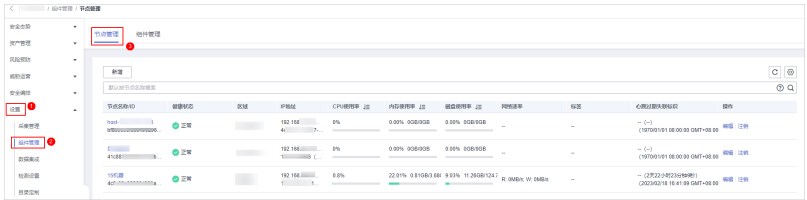
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-44 工作空间页面

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 12-45 进入节点管理页面



版权所有 © 华为云计算技术有限公司

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 12-15 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。

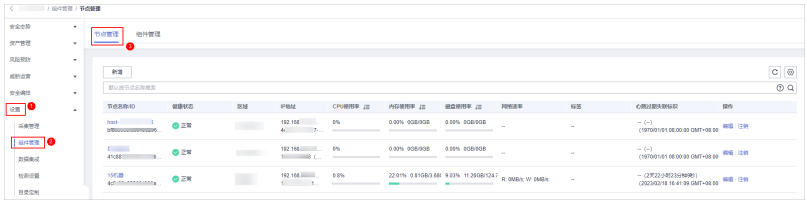
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-46 工作空间页面

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 12-47 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”。

版权所有 © 华为云计算技术有限公司

说明

仅注销节点，不会删除ECS和endpointinterface资源。

----结束

12.1.10.2 管理组件

本章节将介绍如何查看组件相关信息。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-48 工作空间页面

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”。

版权所有 © 华为云计算技术有限公司

- 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

12.2 数据集成

12.2.1 接入数据

安全云脑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。

接入服务日志

步骤1 登录管理控制台。

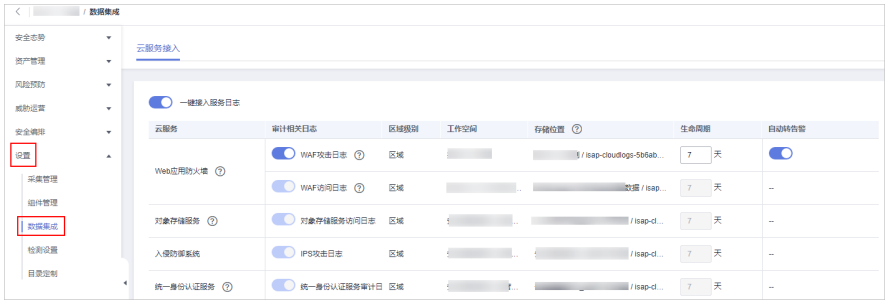
步骤2 单击页面左上方的 ☰，选择“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-49 工作空间页面

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。

图 12-50 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。

 版权所有 © 华为云计算技术有限公司

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。
- 在安全云脑的“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”。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-51 工作空间页面

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

版权所有 © 华为云计算技术有限公司

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”。

12.3 检测设置

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-52 工作空间页面

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。

图 12-53 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12-16所示。

版权所有 © 华为云计算技术有限公司

表 12-16 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，SecMaster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

12.4 目录定制

安全云脑支持自定义目录，您可以根据需要对云脑目录进行定制。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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-54 工作空间页面

版权所有 © 华为云计算技术有限公司

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 12-55 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 12-17 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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 12-56 工作空间页面

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。

 版权所有 © 华为云计算技术有限公司

图 12-57 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

版权所有 © 华为云计算技术有限公司

13 权限管理

13.1 创建用户并授权使用 SecMaster

如果您需要对您所拥有的SecMaster进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用SecMaster资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将SecMaster资源委托给更专业、高效的其他帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图13-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的SecMaster权限，并结合实际需求进行选择。

如**表13-1**所示，包括了SecMaster的所有系统权限。

表 13-1 SecMaster 系统权限

系统角色/策略名称	描述	类别	依赖关系
SecMaster FullAccess	安全云脑的所有权限。	系统策略	无
SecMaster ReadOnlyAccess	安全云脑只读权限，拥有该权限的用户仅能查看安全云脑数据，不具备安全云脑配置权限。	系统策略	无

版权所有 © 华为云计算技术有限公司

示例流程

图 13-1 给用户授予 SecMaster 权限流程

1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予安全云脑的权限“SecMaster FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入1中创建的用户组。
3. 新创建的用户登录控制台，切换至授权区域，验证权限：
   在服务列表中选择除安全云脑外（假设当前策略仅包含“SecMaster FullAccess”）的任一服务，若提示权限不足，表示“SecMaster FullAccess”已生效。

13.2 SecMaster 自定义策略

如果系统预置的SecMaster权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**SecMaster权限及授权项**。

目前云服务平台支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的SecMaster自定义策略样例。

SecMaster 自定义策略样例

- 示例1：授权用户搜索告警列表、权限执行分析

版权所有 © 华为云计算技术有限公司

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "secmaster:alert:list",
            "secmaster:search:createAnalysis"
         ]
      }
   ]
}
```

- 示例2：拒绝用户修改告警配置信息

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予“SecMaster FullAccess”的系统策略，但不希望用户拥有“SecMaster FullAccess”中定义的修改告警配置的权限，您可以创建一条拒绝修改告警类型的自定义策略，然后同时将“SecMaster FullAccess”和拒绝策略授予用户，根据Deny优先原则，则用户可以对SecMaster执行除了修改告警类型外的所有操作。拒绝策略示例如下：

  ```
  {
        "Version": "1.1",
     "Statement": [
        {
           "Effect": "Deny",
           "Action": [
              "secmaster:alert:updateType"
           ]
        }
     ]
  }
  ```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

  ```
  {
     "Version": "1.1",
     "Statement": [
        {
           "Effect": "Allow",
           "Action": [
              "secmaster:alert:get",
              "secmaster:alert:update"
           ]
        },
        {
           "Effect": "Allow",
           "Action": [
              "hss:vuls:set",
              "hss:vuls:list"
           ]
        }
     ]
  }
  ```

13.3 SecMaster 权限及授权项

如果您需要对您所拥有的安全云脑（SecMaster）进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果帐号已经能满足

 版权所有 © 华为云计算技术有限公司

您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用SecMaster服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

 版权所有 © 华为云计算技术有限公司

14 常见问题

14.1 产品咨询

14.1.1 什么是安全云脑?

安全云脑（SecMaster）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。

14.1.2 为什么没有看到攻击数据或者看到的攻击数据很少?

安全云脑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，所以安全云脑可能会显示您的系统当前遭受的攻击程度较低。

14.1.3 安全云脑的数据来源是什么?

安全云脑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。

安全云脑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。

14.1.4 安全云脑与其他安全服务之间的关系与区别?

SecMaster与其他安全防护服务（WAF、HSS、Anti-DDoS、DBSS）的关系与区别如下：

 版权所有 © 华为云计算技术有限公司

- 关联：

  SecMaster：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SecMaster中，呈现全局安全威胁攻击态势。

- 区别：

  SecMaster：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。

SecMaster与其他安全防护服务区别，详细内容如**表14-1**。

表 14-1 SecMaster 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
安全云脑（SecMaster）	安全管理	SecMaster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SecMaster。	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SecMaster。	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SecMaster，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SecMaster。	保障云上数据库安全和资产安全。

14.1.5 SecMaster 与 HSS 服务的区别?

服务含义区别

- 安全云脑（SecMaster）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。

版权所有 © 华为云计算技术有限公司

简而言之，SecMaster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

- SecMaster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 SecMaster 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。	• SecMaster：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帐号、端口、进程、Web目录、软件信息和自启动任务。
	网站资产	-	• SecMaster：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。	• SecMaster：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。
	网站漏洞	-	• SecMaster：支持同步HSS网站漏洞扫描结果，管理网站漏洞。 • HSS：不支持该功能。
基线检查	云服务基线	-	• SecMaster：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	-	• SecMaster：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。

版权所有 © 华为云计算技术有限公司

14.1.6 如何更新安全评分?

安全云脑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。

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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 14-1 工作空间页面

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

14.1.7 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。

安全云脑联动主机安全服务（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。

版权所有 © 华为云计算技术有限公司

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帐户口令。
  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“安全与合规 > 安全云脑•SecMaster”，进入安全云脑管理页面。

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 14-2 工作空间页面

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

 版权所有 © 华为云计算技术有限公司

14.1.8 为什么 WAF、HSS 中的数据和 SecMaster 中的数据不一致?

由于SecMaster中汇聚WAF和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SecMaster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。

14.1.9 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 14-3 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 14-4 磁盘空间不足

 版权所有 © 华为云计算技术有限公司

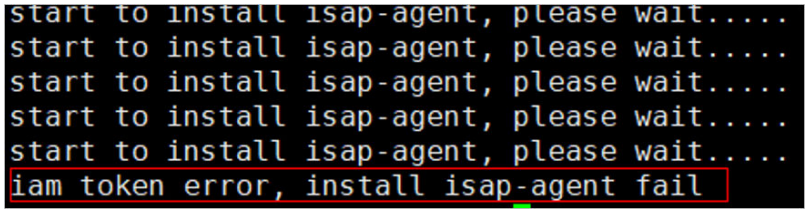
解决方法：

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 14-5 获取 iamtoken 失败

  - **排查步骤和解决方法**

    i. 确认执行命令中的IAM帐号或用户名是否有误。

    图 14-6 IAM 用户名和密码

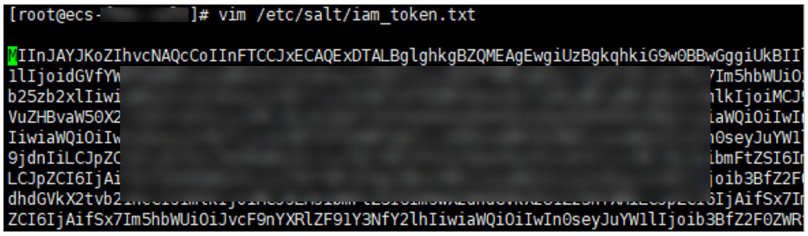
    

    - 有误，修改命令中的IAM帐号或用户名后再次执行安装命令。
    - 无误，继续执行**ii**。

    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 14-7 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 14-8 检查网络

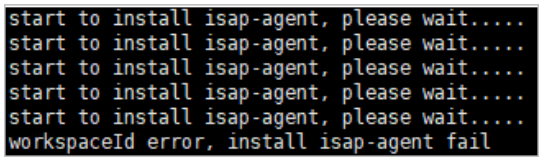
    

- **workspaceId校验失败**
  - **问题现象**

    当日志出现如下图所示信息时，则表示Workspace ID校验失败。

 版权所有 © 华为云计算技术有限公司

图 14-9 workspaceId 校验失败



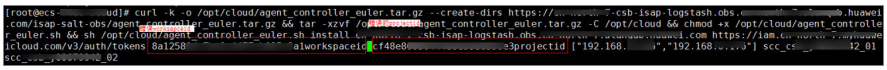
- **解决方法**
  i. 登录安全云脑管理控制台。
  ii. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。
  iii. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点名称。
  iv. 查看执行命令中的workspaceId和projectId。

  图 14-10 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。

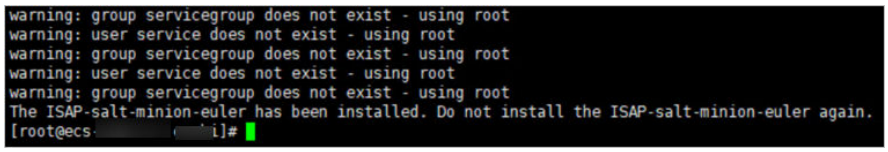
  图 14-11 命令中的参数信息

  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 14-12 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) 登录安全云脑管理控制台。
      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。

版权所有 © 华为云计算技术有限公司

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 14-13 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 14-14 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。

14.1.10 如何给 IAM 子帐号授权?

当您需要授予使用子帐号操作安全云脑服务时，需要使用主帐号对子帐号进行授权操作。

操作步骤

步骤1 使用管理员帐号登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“管理与监管 > 统一身份认证服务”，进入统一身份认证服务管理控制台。

步骤3 创建用户组。

1. 在左侧导航栏选择“用户组”，进入用户组页面后，单击右上角“创建用户组”。
2. 在创建用户组页面，设置用户组名称和描述信息。

版权所有 © 华为云计算技术有限公司

- 用户组名称：请设置为“SecMaster_ops”。
- 描述：自定义描述信息即可。

3. 单击“确定”。

步骤4 新增自定义策略。

1. 在左侧导航栏选择“权限管理 > 权限”，并在权限页面右上角单击“创建自定义策略”。
2. 配置策略。
   a. 策略名称：请设置为“SecMaster_FullAccess”。
   b. 策略配置方式：选择“JSON视图”。
   c. 策略内容：请直接复制粘贴以下内容。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "secmaster:*:*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

   a. 单击“确定”。
   b. 并在弹出的对话框中，选择作用范围为“全局级范围”。
   c. 单击“确定”。

步骤5 给用户组授权。

1. 在左侧导航栏选择“用户组”，进入用户组页面后，单击“SecMaster_ops”，进入用户组详情页面。
2. 在“授权记录”页签中，单击“授权”。
3. 在选择策略页面，搜索并选中“SecMaster_FullAccess”策略后，单击“下一步”。
4. 设置最小授权范围，请选择“所有资源”，设置完成后，单击“确定”。

步骤6 添加成功后显示如下：

----结束

14.2 购买咨询

14.2.1 安全云脑如何变更版本规格?

购买安全云脑后，如果需要增加资产配额或追加增值包功能，即需要扩充“主机配额”或新增“增值包”。

- 购买增值包：详细操作请参见**购买增值包**。
- 增加配额：详细操作请参见**增加配额**。

 版权所有 © 华为云计算技术有限公司

14.2.2 安全云脑如何收费?

安全云脑的计费模式为按需计费。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。

14.2.3 安全云脑支持退订吗?

若用户不再使用安全云脑防护功能或增值包，可执行退订或一键取消操作。

- 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。

约束与限制

- **按需计费**的专业版中，退订/取消专业版资产配额时，增值包功能将一并退订/取消。

取消按需计费

步骤1 在“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤2 针对按需购买的版本或增值包，单击“取消”，一键释放按需计费的资产配额。

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

退订增值包

步骤1 在“总览”页面，单击右上角“专业版”，显示版本管理窗口。

步骤2 单击“取消”，一键释放按需计费的资产配额。返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

 版权所有 © 华为云计算技术有限公司

A 修订记录

发布日期	修改记录
2023-09-20	第二次正式发布。 ● 更新“综合态势感知大屏”、“资产大屏”、“威胁态势大屏”、“查看资产信息”章节内容，优化界面词描述。 ● 更新“修复漏洞”、“管理漏洞”、“新增情报指标”、“管理模型”、“新增数据投递”、“组件管理”章节，优化操作步骤描述，更新参数描述信息。 ● 更新“查看告警信息”、“关闭/删除告警”章节，优化操作步骤描述。 ● 更新“新建/编辑模型”章节，刷新可用模型页面图片。
2023-07-31	第一次正式发布。

版权所有 © 华为云计算技术有限公司