安全云脑

用户指南

文档版本 11

发布日期 2024-03-28

华为云计算技术有限公司

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

1 服务委托授权

操作场景

云服务委托可将相关云服务的操作权限委托给安全云脑，让安全云脑以您的身份使用这些云服务，代替您进行一些任务调度、资源运维等工作。

当您**首次**使用安全云脑时，需要先进行委托授权，才能正常访问。具体待委托权限如下所示：

表 1-1 委托权限

权限	权限描述	授权主体	权限用途
ECS FullAccess	弹性云服务器所有权限	SecMaster_Agency	用于安全组阻断、更新安全组的剧本的执行、查询ECS资产等信息
WAF FullAccess	Web应用防火墙管理员	SecMaster_Agency	用于WAF阻断、WAF地址组关联策略配置和在基线检查功能中检查WAF网站防护信息
SecMaster FullAccess	安全云脑管理员	SecMaster_Agency	用于执行告警处置等操作
HSS FullAccess	主机安全服务的所有权限	SecMaster_Agency	用于漏洞管理、主机隔离等相关剧本的执行和在基线检查功能中获取企业主机安全服务状态
EPS ReadOnlyAccess	企业项目管理服务只读权限	SecMaster_Agency	用于WAF相关剧本流程的执行
ECS ReadOnlyAccess	弹性云服务器的只读访问权限	SecMaster_Agency	用于订购时查询ECS数量和在基线检查功能中获取ECS安全配置信息
Anti-DDoS ReadOnlyAccess	Anti-DDoS流量清洗服务只读权限	SecMaster_Agency	用于在基线功能中获取用户DDoS资产信息

权限	权限描述	授权主体	权限用途
IAM ReadOnlyAccess	统一身份认证服务的只读权限	SecMaster_Agency	用于剧本流程执行中获取凭证信息
WAF Administrator	Web应用防火墙服务（WAF）管理员，拥有该服务下的所有权限	SecMaster_Agency	用于WAF相关剧本流程的执行
SMN FullAccess	拥有消息通知服务的所有权限	SecMaster_Agency	用于通知类剧本的执行
RDS ReadOnlyAccess	关系型数据库服务资源只读权限	SecMaster_Agency	用于资产连接相关剧本的执行
EIP ReadOnlyAccess	EIP服务只读权限	SecMaster_Agency	用于资产连接类剧本的执行和在基线检查功能中获取EIP配置信息
Tenant Guest	全部云服务只读权限(除IAM权限)	SecMaster_Agency	用于剧本中HTTP插件的执行
NAT ReadOnlyAccess	NAT网关服务只读权限	SecMaster_Agency	用于资产管理获取NAT信息
VPC FullAccess	虚拟私有云所有权限	SecMaster_Agency	用于资产连接类剧本以及隔离类流程的执行，和在基线检查功能中获取租户VPC资产信息
OBS OperateAccess	具有对象存储服务（OBS）查看桶列表、获取桶元数据、列举桶内对象、查询桶位置、上传对象、获取对象、删除对象、获取对象ACL等对象基本操作权限	SecMaster_Agency	用于告警剧本的执行和在基线检查功能中获取租户OBS资产信息
ELB ReadOnlyAccess	弹性负载均衡服务只读权限	SecMaster_Agency	用于在基线检查功能中获取租户ELB资产信息
CFW FullAccess	云防火墙所有权限	SecMaster_Agency	用于止血类剧本的执行
RMS ReadOnlyAccess	资源管理服务只读权限	SecMaster_Agency	用于关键运维操作通知剧本使用

前提条件

- 已完成IAM账号授权操作，详细操作请参见**IAM账号授权**。
- 已购买安全云脑。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入工作空间管理页面。

图 1-1 工作空间管理页面

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

图 1-2 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

2 购买安全云脑

2.1 购买标准版

操作场景

安全云脑标准版支持包周期方式进行购买，本章节将介绍如何购买标准版。

说明

购买过程中，如果提示权限不足，请参照**添加权限**进行处理。

版本信息说明

安全云脑提供有基础版、标准版、专业版供您选择，各版本的功能差异请参见**服务版本差异**。

表 2-1 版本说明

版本	计费模式	版本说明
基础版	包周期（免费）	了解安全态势。
标准版	包周期	• 满足安全态势及等保合规运营要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。
专业版	• 按需 • 包周期	• 满足企业日常运营、合规检查等要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 在总览页面中，单击右上角“购买安全云脑”，进入购买安全云脑页面。

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

步骤5 在购买安全云脑页面，配置购买参数。

图 2-1 购买标准版

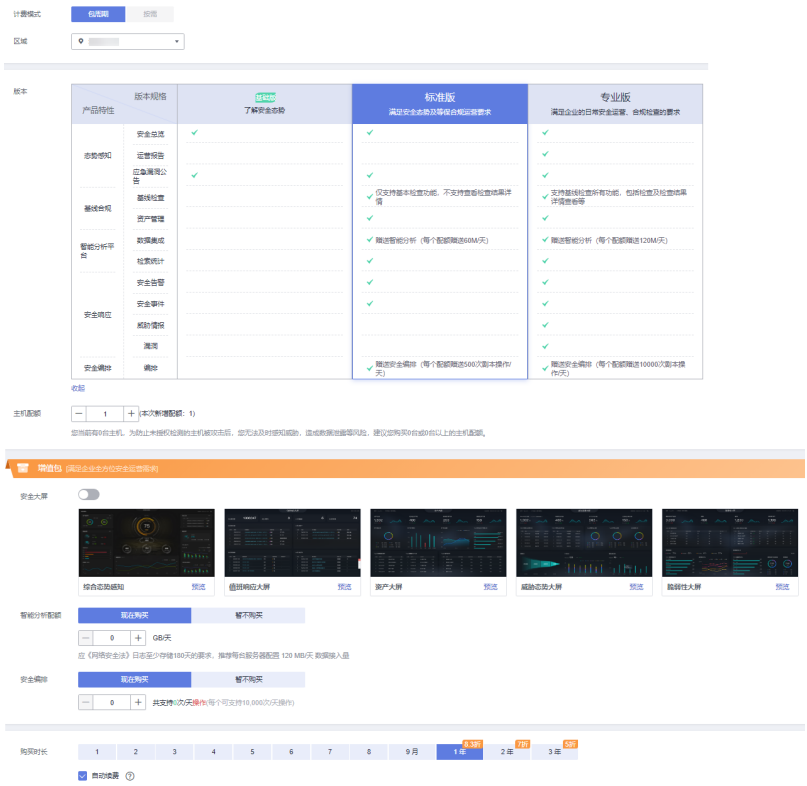


表 2-2 购买标准版参数说明

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

参数名称	说明
增值包	确认是否开通/购买“安全大屏”、“智能分析配额”或“安全编排”功能。如需购买，请根据您的需要设置对应的购买量。 增值包可以在购买标准版时一起购买，也可以后续补充购买，详细操作请参见**购买增值包**。
标签	如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在此处创建标签。
购买时长	选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月～3年的时长。 **说明** 勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤7 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

生效条件

付款成功后，您可以在管理控制台“已购资源”页面右上方查看当前购买的SecMaster版本。

相关操作

- 如果需变更资产配额，可以在“已购资源”页面，选择目标区域，并单击“增加配额”，添加资产配额购买，详细说明请参见**增加配额**。
- 如果购买的包周期版本即将到期或已经到期，可以在“已购资源”页面，选择目标区域，并单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 如果不再使用安全云脑，可以在“总览”页面右上角的版本信息中，单击“退订”或“取消”，退订相应安全云脑服务，详细说明请参见**退订**。

2.2 购买专业版

操作场景

安全云脑专业版支持包周期和按需方式进行购买，本章节介绍如何购买专业版。

说明

购买过程中，如果提示权限不足，请参照**添加权限**进行处理。

版本信息说明

安全云脑提供有基础版、标准版、专业版供您选择，各版本的功能差异请参见**服务版本差异**。

表 2-3 版本说明

版本	计费模式	版本说明
基础版	包周期（免费）	了解安全态势。
标准版	包周期	• 满足安全态势及等保合规运营要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。
专业版	• 按需 • 包周期	• 满足企业日常运营、合规检查等要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。

包周期方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 在总览页面中，单击右上角“购买安全云脑”，进入购买安全云脑页面。

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

步骤5 在购买安全云脑页面，配置购买参数。

图 2-2 包周期购买专业版

表 2-4 包周期购买专业版参数说明

参数名称	说明
计费模式	此处选择“包周期”，按配置周期计费。
区域	选择您所在的区域。
版本	选择“专业版”。
主机配额	主机配额是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 **说明** • 主机配额最大限制为10000台。 • 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。
增值包	确认是否开通/购买“安全大屏”、“智能分析配额”或“安全编排”功能。如需购买，请根据您的需要设置对应的购买量。 增值包可以在购买标准版时一起购买，也可以后续补充购买，详细操作请参见**购买增值包**。
标签	如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在此处创建标签。

参数名称	说明
购买时长	选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月～3年的时长。 **说明** 勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤7 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

按需方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 在总览页面中，单击右上角“购买安全云脑”，进入购买安全云脑页面。

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

步骤5 在购买安全云脑页面，配置购买参数。

图 2-3 包周期购买专业版

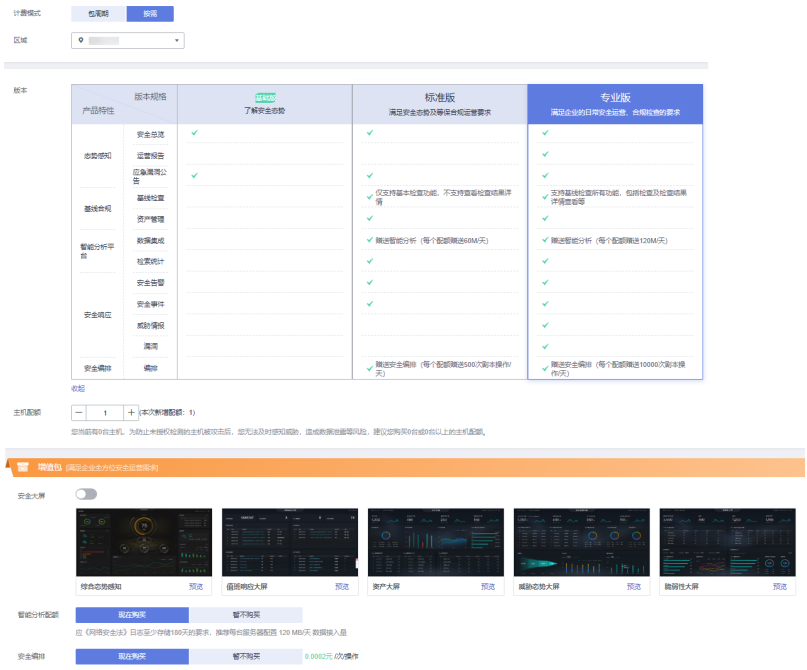


表 2-5 按需购买专业版参数说明

参数名称	说明
计费模式	此处选择“按需”，按小时计费。从开通开始到取消结束，按实际防护时长（小时）计费。
区域	选择您所在的区域。
版本	选择“专业版”。
主机配额	主机配额是指主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 **说明** • 主机配额最大限制为10000台。 • 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。
增值包	确认是否开通/购买“安全大屏”、“智能分析配额”或“安全编排”功能。 增值包可以在购买标准版时一起购买，也可以后续补充购买，详细操作请参见**购买增值包**。
标签	如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在此处创建标签。

步骤6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤7 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

生效条件

付款成功后，您可以在管理控制台“已购资源”页面查看当前购买的SecMaster版本。

相关操作

- 如果需变更资产配额，可以在“已购资源”页面，选择目标区域，并单击“增加配额”，添加资产配额购买，详细说明请参见**增加配额**。
- 如果未同时开通增值包功能，可以在“已购资源”页面，单击页面右上角的“购买增值包”，开通增值包功能，详细说明请参见**购买增值包**。
- 如果购买的包周期版本即将到期或已经到期，可以在“已购资源”页面，选择目标区域，并单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 如果不再使用资产配额或增值包功能，可以在“总览”页面右上角的版本信息中，单击“退订”或“取消”，退订相应安全云脑服务，详细说明请参见**退订**。

2.3 升级版本

升级版本分为版本的升级和配额的增加，请根据您的需要进行选择：

表 2-6 升级版本

操作场景	说明
版本升级	• **基础版升级为标准版或专业版**：已开通基础版，支持升级到标准版或专业版。 • **标准版升级为专业版**：已购买标准版，支持升级到专业版。
配额增加	同一版本，选择升级版本，支持仅增加配额，详细操作请参见**增加配额**。
升级版本并增加配额	**标准版升级为专业版**：目前仅当标准版升级为专业版时，支持同时升级版本并增加资产配额。
注意 升级后不可降级。	

说明

购买过程中，如果提示权限不足，请参照**添加权限**进行处理。

版本信息说明

安全云脑提供有基础版、标准版、专业版供您选择，各版本的功能差异请参见**服务版本差异**。

表 2-7 版本说明

版本	计费模式	版本说明
基础版	包周期（免费）	了解安全态势。
标准版	包周期	• 满足安全态势及等保合规运营要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。
专业版	• 按需 • 包周期	• 满足企业日常运营、合规检查等要求。 • 提供有**安全大屏**、**智能分析**、**安全编排**增值功能。

基础版升级为标准版或专业版

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入已购资源页面后，在待升级为标准版所在region栏中，单击“升级”。

图 2-4 基础版升级

步骤4 在购买安全云脑页面，配置购买参数。

1. “当前配置”：显示已选择region安全云脑版本信息，无需配置。
2. “升级方式”：默认选择“版本升级”。
3. “可选版本”：此处选择“标准版”或“专业版”，升级版本功能。

图 2-5 选择版本

4. 标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在购买安全云脑时创建标签。

步骤5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤6 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤7 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

标准版升级为专业版

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入已购资源页面后，在待购买安全云脑专业版所在region栏中，单击“升级”。

步骤4 在购买安全云脑页面，配置购买参数。

1. “当前配置”：显示已选择region安全云脑版本信息，无需配置。
2. “升级方式”：选择“版本升级”，还可以同时勾选增加配额。
3. “可选版本”：此处选择“专业版”，升级为专业版功能。

图 2-6 选择专业版

4. （可选）“主机配额”：配置主机配额。

表 2-8 主机配额参数说明

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

5. 标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在购买安全云脑时创建标签。

步骤5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤6 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤7 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

生效条件

付款成功后，您可以在管理控制台“总览”页面右上方查看当前购买的SecMaster版本。

相关操作

- 如果需变更资产配额，可以在“已购资源”页面，选择目标区域，并单击“增加配额”，添加资产配额购买，详细说明请参见**增加配额**。
- 如果未同时开通增值包功能，可以在“已购资源”页面中，单击右上角“购买增值包”，开通增值包功能，详细说明请参见**购买增值包**。
- 如果购买的包周期版本即将到期或已经到期，可以在“已购资源”页面，选择目标区域，并单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 如果不再使用资产配额或增值包功能，可以在“总览”页面右上角的版本信息中，单击“退订”或“取消”，退订相应安全云脑服务，详细说明请参见**退订**。

2.4 购买增值包

操作场景

安全云脑在标准版/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。

说明

购买过程中，如果提示权限不足，请参照**添加权限**进行处理。

约束与限制

- 增值包为标准版/专业版额外选购付费项目，如需使用增值包，**须**先购买标准版/专业版。
- 增值包支持包周期和按需方式进行购买。

前提条件

已购买安全云脑标准版或专业版。

包周期方式购买增值包

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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4 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“包周期”，按配置周期计费。
   - “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 2-7 购买增值包

表 2-9 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	1. 选择智能分析配额后的“现在购买”。 2. 设置每日的日志存储容量。	请选择“暂不购买”。
安全编排	1. 选择安全编排后的“现在购买”。 2. 设置每日操作次数。	请选择“暂不购买”。

4. 标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在购买安全云脑时创建标签。

步骤5 选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月～3年的时长。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤6 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤7 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤8 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

按需方式购买增值包

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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4 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 2-8 按需购买增值包

表 2-10 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”

4. 标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在此处创建标签。

步骤5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤6 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤7 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

后续管理

- 如果购买的包周期安全大屏即将到期或已经到期，可在“总览”页面右上角版本管理中，单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 如果不再使用增值包功能，可在“总览”页面右上角版本管理中，单击“退订”或“取消”，退订相应安全云脑服务，详细说明请参见**退订**。

2.5 增加配额

操作场景

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。

说明

购买过程中，如果提示权限不足，请参照**添加权限**进行处理。

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。如果购买的最大配额小于主机数量，可能会造成未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入已购资源页面后，在待购买安全云脑专业版所在region栏中，单击“增加配额”。

步骤4 在购买安全云脑页面，配置购买参数。

1. “当前配置”：显示已选择region安全云脑版本信息，无需配置。
2. “升级方式”：选择“增加配额”。
3. “主机配额”：配置主机配额。

图 2-9 增加配额

表 2-11 主机配额参数说明

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

4. 标签：如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在此处创建标签。

步骤5 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤6 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。

步骤7 在支付页面，选择付款方式完成付款，完成购买操作。

----结束

2.6 退订

操作场景

如果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。

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

更多费用和订单说明信息，请参见**费用中心**。

说明

购买过程中，如果提示权限不足，请参照**添加权限**进行处理。

约束与限制

- **包周期**计费的标准版和专业版中，资产配额与增值包功能**需分别**退订/取消。
  当资产配额（专业版或标准版）被全部退订/取消后，当前为基础版时，您**再**执行退订/取消增值包功能操作。
- **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。
- 增值包功能**不支持**单独使用。
  如果您在购买了标准版或专业版的基础上，开通了增值包功能，当专业版或标准版的退订/取消后，未退订/取消增值包功能，对应功能将无数据支撑，无法使用。因此，如果您退订/取消了专业版或标准版，须再执行退订/取消增值包功能操作。

退订包周期计费

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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“总览”页面中，单击右上角“标准版”或“专业版”，显示版本管理窗口。

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

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

步骤6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

取消按需计费

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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“总览”页面中，单击右上角“专业版”，显示版本管理窗口。

步骤4 针对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 登录管理控制台。

步骤2 在页面左上角单击 ，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“总览”页面，单击右上角“标准版”或“专业版”，显示版本管理窗口。

步骤4 退订增值包。

- 针对按需购买的增值包

  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。

- 针对包周期购买的增值包

  a. 针对包周期购买的增值包，单击“退订”，进入“退订管理”列表页面。

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

c. 确认待退订资源信息，选择退订原因，并勾选退订确认。
d. 单击“退订”，在退订管理页面确认退订。
退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

3 安全总览

3.1 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，帮助您全量了解资产的安全情况，包括资产的安全评估结果、安全监控和安全趋势等信息。

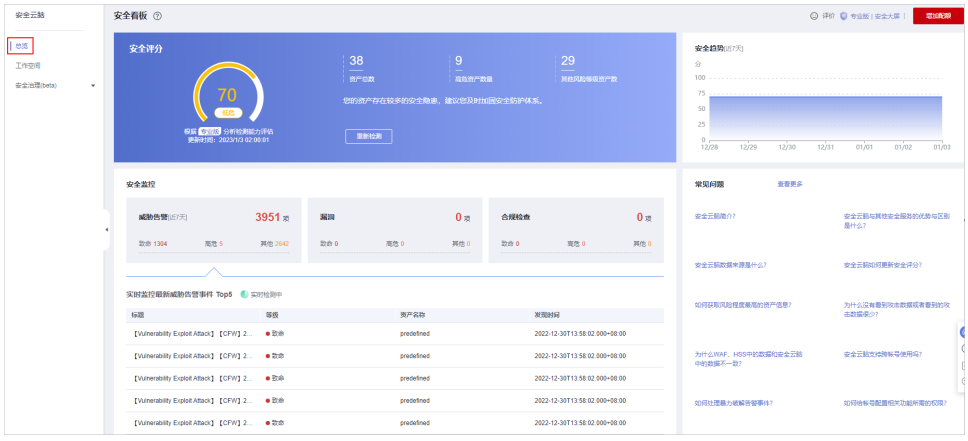
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入安全总览页面。

图 3-1 总览页面



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

- **安全评分**
- **安全监控**

- **安全趋势**

各个板块数据统计周期及更新频率如下表所示：

表 3-1 总览

参数名称	统计周期	更新频率	说明
安全评分	实时	• 每天2:00自动更新 • 随手动单击“重新检测”更新而更新	根据是否开启各安全服务防护、未处理的配置问题等级及个数、未处理的漏洞等级及个数、未处理的威胁事件等级及个数等计算而来，具体评分详细信息请参见**安全评分**。
威胁告警	近7天	每5分钟	本账号安全云脑下全部工作空间告警管理中的告警总和。
漏洞	近7天	每5分钟	本账号安全云脑下全部工作空间漏洞管理中的漏洞总和。
合规检查	实时	每5分钟	本账号安全云脑下全部工作空间基线检查中的问题总和。
安全趋势	近7天	每5分钟	近7天的安全评分数据。

----结束

安全评分

“安全评分”板块根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况，如**图3-2**。

图 3-2 安全评分

- 安全评分每天凌晨2:00自动更新，也支持通过单击“重新检测”来进行实时更新。
- 分值范围为0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见**安全评分**。
- 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

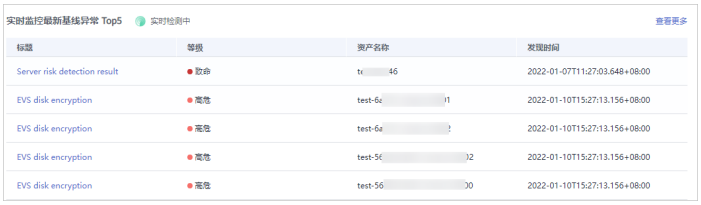
“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

图 3-3 安全监控

表 3-2 安全监控参数说明

参数名称	参数说明
威胁告警	呈现**近7天内**本账号所有工作空间内未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。统计信息更新频率为每5分钟更新一次。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 ● 单击威胁告警模块，系统将列表实时呈现**近7天内**TOP5的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 列表呈现近7天TOP5的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 如果列表显示内容为空，表示近7天无威胁告警事件。 **图 3-4** 查看实时威胁告警 

参数名称	参数说明
漏洞	展示您本账号所有工作空间内资产中TOP5漏洞类型，以及**近7天内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。统计信息更新频率为每5分钟更新一次。 • 此处严重等级含义如下： – 高危：即高危风险，表示资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 中危：即中危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“漏洞类型Top5”栏，系统将列表呈现TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的TOP等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 仅当主机中Agent版本为2.0时，才会在“漏洞类型Top5”中显示对应数据。如未显示数据或需要查看TOP5漏洞类型，请将主机将Agent1.0升级至Agent2.0。 **图 3-5** 漏洞类型  • 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。 – 如果列表显示内容为空，表示当日无漏洞事件。

参数名称	参数说明
	图 3-6 查看实时漏洞 
合规检查	展示您本账号所有工作空间内资产中存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。统计信息更新频率为每5分钟更新一次。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了不合规配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常配置，建议您立即查看合规检查事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常配置，建议您及时查看该合规检查项目的详情。 ● 单击合规检查异常模块，系统将列表实时呈现TOP5的合规检查异常事件，可快速查看合规检查详情。 – 列表呈现最近一次合规检查中TOP的合规异常事件详情，包括合规检查项目名称、等级、受影响资产数量、发现时间。 – 如果列表显示内容为空，表示近30天无合规异常事件。 **图 3-7** 查看合规异常事件 

安全趋势

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

图 3-8 安全趋势

3.2 安全评分

操作场景

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

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

本章节将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

安全分值

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

  说明

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

表 3-3 安全分值表

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

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

安全评分扣分项

安全评分扣分项及其分值情况如表3-4所示。

表 3-4 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		
	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		

分类	扣分项	单项扣分项	处理建议	最高扣分上限
	存在未处理的中危告警事件	2		
	存在未处理的低危告警事件	0.1		

4 工作空间

4.1 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。

- 空间管理：

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

什么是数据空间?

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

什么是数据管道?

数据传输消息主题和存储索引组合为数据管道。

工作空间通用规则

- 付费版本安全云脑：单账号单Region内最多创建5个工作空间。
- 免费版本安全云脑：单账号单Region内最多创建1个工作空间。
- 工作空间永久删除：永久删除的workspace立即删除，不能进行恢复。
- 空间托管：
  - 单账号单Region内最多创建1个空间托管视图。

  - 单/跨账号单Region空间托管视图（包含的纳管工作空间数）中的工作空间数 ≤ 100个。
  - 跨账号跨Region空间托管视图（包含的纳管工作空间数）中的工作空间数 ≤ 10个。
  - 单账号创建账号委托 ≤ 10个。
- 暂不支持在同一个浏览器的多个窗口进入不同的工作空间进行操作。

4.2 新增工作空间

操作场景

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。

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。

约束与限制

- 付费版本安全云脑：单账号单Region内最多创建5个工作空间。
- 免费版本安全云脑：单账号单Region内最多创建1个工作空间。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入工作空间管理页面。

图 4-1 工作空间管理页面

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

步骤5 配置新建工作空间参数，参数说明如下表所示：

表 4-1 新增工作空间

参数名称	参数说明
区域	选择待新增工作空间所在区域。

参数名称	参数说明
项目类型	选择待新增工作空间所属的项目类型。 当选择为“企业项目”时，需要在下拉列表中选择您所在的企业项目。 企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。 如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。
工作空间名称	自定义工作空间的名称。命名规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 • 长度不能超过64个字符。
标签	可选参数，添加该工作空间的标签，用于标识工作空间，方便您对工作空间进行分类和跟踪。
描述	可选参数，设置该工作空间的备注信息。

步骤6 单击“确定”，完成工作空间的新增。

----结束

4.3 空间管理

4.3.1 查看工作空间详情

操作场景

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

说明

安全云脑支持在空间管理页面中可以查看全局工作空间的信息。如果无法查看且界面提示未购买安全云脑，请先开通安全云脑任意版本。

例如，您在“华北-北京四”region已购买安全云脑、创建并使用工作空间。目前，切换至“华东-上海一”region的空间管理页面中可以查看“华北-北京四”工作空间信息。如果界面提示未购买安全云脑，且无法查看工作空间信息，请先开通安全云脑任意版本，开通后即可查看。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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”，进入工作空间管理页面。

图 4-2 工作空间管理页面

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 4-3 工作空间详情

表 4-2 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。分为“自有”、“托管视图”、“已托管”类型。
ID	工作空间的ID。
区域	工作空间所属区域。
项目	工作空间所属的项目。
更多	单击“更多”可查看工作空间详细信息。
托管状态	工作空间是否托管。
事件	该工作空间中的事件数量。
漏洞	该工作空间中的漏洞数量。
告警	该工作空间中的告警数量。
情报	该工作空间中的情报数量。
资产	该工作空间中已有资产的数量。
安全分析	该工作空间中已有数据空间数量。
实例	该工作空间中已有实例的数量。

参数名称	参数说明
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。

在工作空间的“基本信息”页签中，可以查看工作空间的名称、所属项目、ID等信息；在“标签管理”页签中，可以管理标签，管理标签详细操作请参见**管理工作空间标签**。

----结束

4.3.2 编辑工作空间

操作场景

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

该任务指导您如何编辑工作空间。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击，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”，进入工作空间管理页面。

图 4-4 工作空间管理页面

步骤4 单击目标工作空间所在栏右上角的（设置按钮），进入工作空间详情页面。

图 4-5 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

4.3.3 管理工作空间标签

操作场景

工作空间新增成功后，您可以对工作空间的标签进行添加、编辑和删除操作。标签以键值对的形式表示，用于标识工作空间，便于对工作空间进行分类。此处的标签仅用于工作空间的管理。

如您的组织已经设定安全云脑服务的相关标签策略，则需按照标签策略规则为工作空间添加标签。标签如果不符合标签策略的规则，则可能会导致工作空间创建失败，请联系组织管理员了解标签策略详情。

该章节指导您如何管理标签。

约束与限制

一个工作空间最多添加10个标签。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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”，进入工作空间管理页面。

图 4-6 工作空间管理页面

步骤4 单击目标工作空间所在栏右上角的（设置按钮），进入工作空间详情页面。

图 4-7 工作空间详情页面入口

步骤5 在工作空间的详情页面中选择“标签管理”页签中，进入标签管理页面。

图 4-8 标签管理

步骤6 在标签管理页面中，对标签进行管理。

表 4-3 管理标签

参数名称	参数说明
添加标签	1. 在标签管理页面中，单击“添加标签”。 2. 在弹出的添加标签页面中，配置标签键和值。 3. 配置完成后，单击“确定”。
编辑标签	1. 在标签管理页面中，单击标签所在行“操作”列的“编辑”。 2. 在弹出的编辑页面中，修改标签值。 3. 修改完成后，单击“确定”。
删除标签	在标签管理页面中，单击标签所在行“操作”列的“删除”，并在弹出的确认框中单击“是”。

----结束

4.3.4 删除工作空间

操作场景

如果不再需要某个工作空间，可以参照本章节进行删除。

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

约束与限制

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

删除工作空间

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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”，进入工作空间管理页面。

图 4-9 工作空间管理页面

步骤4 单击目标工作空间所在栏右上角的（设置按钮），进入工作空间详情页面。

图 4-10 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框中，确认无误后，勾选“永久删除工作空间”，并在“确认删除”中输入工作空间名称，并单击“删除”。

注意

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

----结束

4.4 空间托管

4.4.1 概述

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

表 4-4 空间托管流程

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

约束与限制

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

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

4.4.2 创建托管视图

操作场景

创建托管前，需先创建托管视图。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 > 空间托管”，进入空间托管管理页面。

图 4-11 空间托管页面

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

步骤5 配置托管视图参数。

表 4-5 创建托管视图参数说明

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

步骤6 单击“确定”。

创建成功后，可以在“空间管理”或“空间托管”页面中查看已创建的托管视图。

----结束

相关操作

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

4.4.3 创建托管

操作场景

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

约束与限制

创建托管时，当选择组织进行托管时，需注意以下信息：

- 如果选择的是所有组织下的所有账号进行托管，那么，后续某个组织下新增账号也可以实现全量托管；
- 如果选择的是某个组织下的所有账号进行托管，那么，后续该组织下新增账号，该账号下的信息无法进行立即托管，将会有一定的延迟。

前提条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 > 空间托管”，进入空间托管管理页面。

图 4-12 空间托管页面

步骤4 单击页面右上角“创建托管”，右侧弹出创建托管页面。

步骤5 配置托管参数。

表 4-6 创建托管参数说明

参数名称		参数说明
发起方式		选择空间托管的发起方式。 如果您使用的是组织管理员账号或者委托管理员账号登录的安全云脑，此处可以选择组织下的账号进行托管。 华为云Organizations云服务是一项账号管理服务，使您能够将多个华为云账号整合到您创建并集中管理的组织中。有关组织的详细说明请参见《组织用户指南》。
托管方	托管空间	选择托管工作空间。
受托管方	租户	输入受托管方用户的账号名称。获取方式如下： 1. 已登录管理控制台，并将鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，默认进入API凭证页面。 2. 在API凭证页面中，获取“账号名”。 **图 4-13** 账号名 
	托管视图	选择已有的托管视图。
托管信息	托管名称	设置托管名称。
	托管时长	选择托管时长。
	托管策略	选择托管策略。 策略具体含义可以在IAM中进行查询，查看方法如下： 1. 已登录管理控制台，并将鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”，进入IAM页面。 2. 在左侧导航栏选择“权限管理 > 权限”，并在权限页面搜索框中输入策略名称。 查看策略具体含义及策略范围。
	描述	自定义托管描述信息。

步骤6 单击“确认”。

----结束

后续处理

托管创建后，需进行托管授权，详细操作请参见**托管授权**。

4.4.4 托管授权

操作场景

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

前提条件

已创建托管，详细操作请参见**创建托管**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 > 空间托管”，进入空间托管管理页面。

图 4-14 空间托管页面

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

步骤5 在弹出的确认框中，单击“确认”。

----结束

后续处理

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

4.4.5 管理托管

操作场景

空间托管页面中，可以管理托管视图、我纳管的和纳管我的。

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

- 纳管我的：列表呈现我的工作空间被哪些托管视图纳管着。

托管视图

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 > 空间托管”，进入空间托管管理页面。

图 4-15 空间托管页面

步骤4 在托管页面中，选择“托管视图”页签，进入托管视图页面。

步骤5 在托管视图页面中，可以查看和管理托管视图。

- 查看托管视图

表 4-7 查看托管视图

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

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

a. 在待删除视图所在行“操作”列，单击“删除”。

如果需要删除多个视图，可以在列表中勾选需要删除的视图，并单击列表上方“批量删除”。

b. 在弹出确认框中，单击“确认”。

----结束

我纳管的

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 > 空间托管”，进入空间托管管理页面。

图 4-16 空间托管页面

步骤4 在托管页面中，选择“我纳管的”页签，进入我纳管的页面。

步骤5 在我纳管的页面中，可以查看和管理我纳管的任务。

- 查看我纳管的

表 4-8 查看我纳管的

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

- 管理我纳管的

表 4-9 管理我纳管的

操作	说明
接收托管	1. 在待接收拖管所在行“操作”列，单击“接收”。 如果需要接收多个拖管关系，可以在列表中勾选需要接收的拖管关系，并单击列表上方“批量接收”。 2. 在弹出确认框中，单击“确认”。
拒绝托管关系	1. 在待拒绝拖管所在行“操作”列，单击“拒绝”。 如果需要拒绝多个拖管关系，可以在列表中勾选需要拒绝的拖管关系，并单击列表上方“批量拒绝”。 2. 在弹出确认框中，单击“确认”。
解除托管关系	1. 在待解除拖管所在行“操作”列，单击“更多 > 解除”。 如果需要解除多个托管关系，可以在列表中勾选需要解除的拖管关系，并单击列表上方“批量解除”。 2. 在弹出确认框中，单击“确认”。
删除托管任务	1. 在待删除拖管所在行“操作”列，单击“更多 > 删除”。 如果需要删除多个拖管，可以在列表中勾选需要删除的拖管，并单击列表上方“批量删除”。 2. 在弹出确认框中，单击“确认”。

----结束

纳管我的

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 > 空间托管”，进入空间托管管理页面。

图 4-17 空间托管页面

步骤4 在托管页面中，选择“纳管我的”页签，进入纳管我的页面。

步骤5 在纳管我的页面中，可以查看和管理纳管我的。

- 查看纳管我的

表 4-10 查看纳管我的

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

- 管理纳管我的

表 4-11 查看纳管我的

操作	说明
修改已接收的托管任务	1. 在待修改拖管所在行“操作”列，单击“修改”。 2. 在弹出编辑页面中修改托管信息。 3. 单击“确认”。
撤回已接收的托管任务	1. 在待撤回拖管所在行“操作”列，单击“撤回”。 如果需要撤回多个解除关系，可以在列表中勾选需要撤回的拖管关系，并单击列表上方“批量撤回”。 2. 在弹出确认框中，单击“确认”。
重申托管关系	如果受纳管方拒绝了托管，可发起再次申请操作。 1. 在待重申拖管所在行“操作”列，单击“更多 > 重申”。 2. 在弹出确认框中，单击“确认”。

操作	说明
解除托管关系	1. 在待解除拖管所在行“操作”列，单击“更多 > 解除”。 如果需要解除多个托管关系，可以在列表中勾选需要解除的拖管关系，并单击列表上方“批量解除”。 2. 在弹出确认框中，单击“确认”。
删除托管任务	1. 在待删除拖管所在行“操作”列，单击“更多 > 删除”。 如果需要删除多个拖管，可以在列表中勾选需要删除的拖管，并单击列表上方“批量删除”。 2. 在弹出确认框中，单击“确认”。

----结束

5 查看已购资源

操作场景

在安全云脑的已购资源中可统一呈现当前账号已经购买的资源，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 在页面左上角单击 ☰，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。

图 5-1 已购资源管理页面

步骤4 在已购资源页面查看详细信息。

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

----结束

6 安全治理

6.1 概述

什么是安全治理?

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

说明

使用安全治理功能前，需先**提交工单**申请开通使用权限。

功能特性

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

- 提供安全遵从包

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

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

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

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

功能优势

- 全球合规治理经验服务化

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

- 提升获得法规及行业标准认证的效率

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

- 高效实施安全治理动作

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

6.2 安全遵从包规格说明

安全治理提供两大类的安全遵从包，您可以根据不同遵从包的判定指引来选择所需的安全遵从包。

- **安全标准遵从包**
- **隐私保护遵从包**

安全标准遵从包

当前可选择的安全标准遵从包如**表6-1**所示，用户依据**判定指引**选择并订阅安全遵从包。

表 6-1 安全标准遵从包一览

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

遵从包名称	描述	适用区域	分类	领域	判定指引
ISO 27701安全遵从包	该遵从包依据国际上公认的ISO 27701隐私信息管理要求和指南（2019版），提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评隐私信息管理情况，并给出了隐私保护方面的改进建议，帮助企业贯彻隐私保护的责任，提升隐私保护及信息安全水平。	全球	国际标准	隐私保护	1. 您是否涉及处理（包括收集、使用、传输、存储、删除等）个人可识别信息（简称“PII”，如姓名、电话号码、电子邮箱、身份证件信息等，在本遵从包中也称作“个人数据”）？ 2. 您是否作为PII控制者（决定PII处理目的和方法的隐私利益相关方，在本遵从包中也称作“数据控制者”）和/或PII处理者（代表PII控制者，并按照PII控制者的指示对PII进行处理的隐私利益相关方，在本遵从包中也称作“数据处理者”）的角色? 3. 您是否期望对您在隐私保护方面的风险进行识别，并获知如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。
等保2.0标准四级安全遵从包	该遵从包依据国家标准GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》中四级的安全要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）自评网络安全管理情况，并给出了网络安全等级保护的改进建议，帮助企业建设网络安全体系，提升网络安全水平。	中国	国家标准	网络安全	1. 您是否涉及网络安全等级保护工作的作用对象，主要包括基础信息网络（为信息流通、信息系统运行等起基础支撑作用的信息网络，包括电信网、广播电视传输网、互联网、业务专网等网络设备设施）、信息系统（例如工业控制系统、云计算平台、物联网、使用移动互联技术的信息系统以及其他信息系统）和大数据等? 2. 您是否期望对网络实施分级保护措施，在网络安全保护方面的风险进行识别，并获知如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。

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

隐私保护遵从包

当前可选择的隐私保护遵从包如**表6-2**所示，用户依据**判定指引**选择并订阅安全遵从包。

表 6-2 隐私保护遵从包

遵从包名称	描述	适用区域	分类	领域	判定指引
中国-澳门隐私保护遵从包	该遵从包依据《澳门个人资料保护法》2005年（Personal Data Protection Act，2005，简称“PDPA”），提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）进行自评估，并为您的企业处理个人数据的有关活动提供指引。	中国-澳门	法律法规	隐私保护	1. 您或者您的企业是否涉及如下场景之一： ● 以全部或部分自动化方式进行个人资料（在本遵从包中也称作“个人数据”）处理活动； ● 以非自动化方式进行的，构成或拟构成人工存档系统的一部分的个人资料的处理活动； ● 使用监控录像或其它设备来捕捉、处理和传播可用以识别某一特定个人的声音和图像。 **说明** 澳门个人资料保护法没有对适用的“地域范围”进行规定。是否适用澳门PDPA或者是否受澳门法律的管辖，在上述3个场景涉及的情况，建议考虑以下两点： ● 资料处理活动是否在澳门特区领土范围有关联，例如在澳门特区内进行的个人资料搜集、储存的行为； ● 资料处理活动是否与澳门居民（包括法人、自然人）有关联。 2. 您是否期望对您在澳门的个人资料处理方面的风险进行识别，并获知如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。

遵从包名称	描述	适用区域	分类	领域	判定指引
中国-大陆隐私保护遵从包	该遵从包依据《中国个人信息安全规范》2020年的法规要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）进行自评估，为企业提供开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的安全要求，并给出了隐私保护方面的改进建议，帮助您的企业提升个人信息保护水平。	中国大陆	法律法规	隐私保护	1. 您是否涉及在中国大陆境内进行个人数据的收集、使用或披露等个人信息处理活动? 2. 您是否期望对您在中国个人信息安全规范下的个人信息安全风险进行识别，并获取如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。
中国-香港隐私保护遵从包	该遵从包依据《香港个人资料（私隐）条例》1995年（Personal Data（Privacy）Ordinance，1995，简称PDPO）的法规要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）进行自评估，指导您的企业如何收集、存储、传输、处理和使用收集到的个人数据，并给出了隐私保护方面的改进建议，帮助您的企业提升隐私保护及信息安全水平。	中国香港	法律法规	隐私保护	1. 您是否涉及对一名在世人士有关及可确定个人身份的资料，以可供查阅及处理的方式记录下来? **说明** 中国香港PDPO没有对适用的“地域范围”进行规定，是否适用中国香港PDPO，建议结合以下条件考虑：您是否涉及作为中国香港境内的资料使用者（在本遵从包中也称作“数据控制者”）收集、使用、或处理个人资料（在本遵从包中也称作“个人数据”）? 2. 您是否期望对您在中国香港PDPO下的个人资料处理相关风险进行识别，并获取如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。

遵从包名称	描述	适用区域	分类	领域	判定指引
新加坡隐私保护遵从包	该遵从包依据《新加坡个人数据保护法》2012年（Personal Data Protection Act，2012，简称PDPA）的法规要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）进行自评估，并给出了隐私保护方面的改进建议，帮助您的企业规范个人数据的收集、使用或披露，以及提升个人保护其个人信息数据各项权利的意识。	新加坡	法律法规	隐私保护	1. 您是否涉及在新加坡境内进行个人数据的收集、使用或披露等个人信息处理活动? 2. 您是否期望对您在新加坡个人数据保护法下的个人数据保护相关风险进行识别，并获取如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。
泰国隐私保护遵从包	该遵从包依据《泰国个人数据保护法B.E.2562》2019年（Personal Data Protection Act B.E.2562 2019, 简称PDPA）的法规要求，提供检查项和评测指引供云计算客户（在本遵从包中也称作“您”或者“您的企业”）进行自评估，并给出了隐私保护方面的改进建议，帮助企业全面管理数据保护以及个人数据的收集、保护、使用、存储、披露、传输。	泰国	法律法规	隐私保护	1. 您是否涉及在泰国境内收集、保护、使用、披露、传输和其他处理个人数据的情形? 2. 您是否涉及对位于泰国境内的个人数据主体从事以下活动： ● 您向泰国境内的数据主体提供服务，无论是否由该数据主体支付费用 ● 监控数据主体的行为，且该监控发生在泰国境内 3. 您是否期望对您在泰国个人数据保护法下的个人数据保护风险进行识别，并获取如何采取措施降低风险? 如果以上任一回答为是，建议您订阅该遵从包。

6.3 使用流程

安全治理功能的使用流程如表6-3所示。

图 6-1 使用流程

表 6-3 使用流程

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

6.4 服务授权

操作场景

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

本章节将介绍如何授权访问用户云上资产。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-2 进入订阅列表页面

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

步骤5 在弹出服务授权确认框中，单击“同意授权”，完成授权。

----结束

6.5 订阅安全遵从包

操作场景

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

本章节将介绍如何订阅安全遵从包。

前提条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-3 进入订阅列表页面

步骤4 在订阅列表页面中单击“订阅安全遵从包”，进入订阅安全遵从包页面。

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

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

安全遵从包详细介绍请参见**安全遵从包规格说明**。

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

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

----结束

6.6 用户自评估

操作场景

订阅安全遵从包后，用户可以依据国际标准进行自评估。

前提条件

已订阅安全遵从包，详细操作请参见**订阅安全遵从包**。

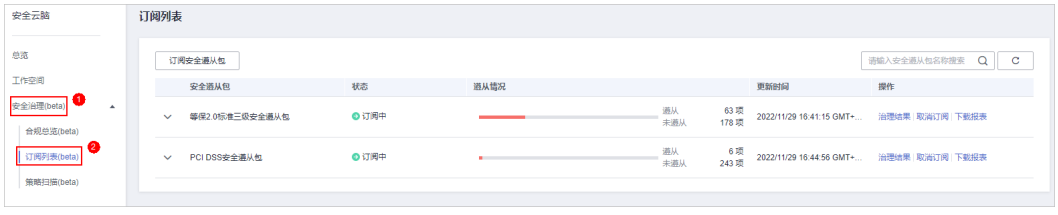
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-4 进入订阅列表页面



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

图 6-5 自评估

步骤5 在租户自评估页面，对每个检查项进行自评。

图 6-6 自评估界面

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

步骤6 评估完成后，单击右下角的“提交”。

----结束

6.7 安全合规总览

操作场景

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

前提条件

已订阅安全遵从包，详细操作请参见**订阅安全遵从包**。

查看法规、标准条款遵从概况

步骤1 登录管理控制台。

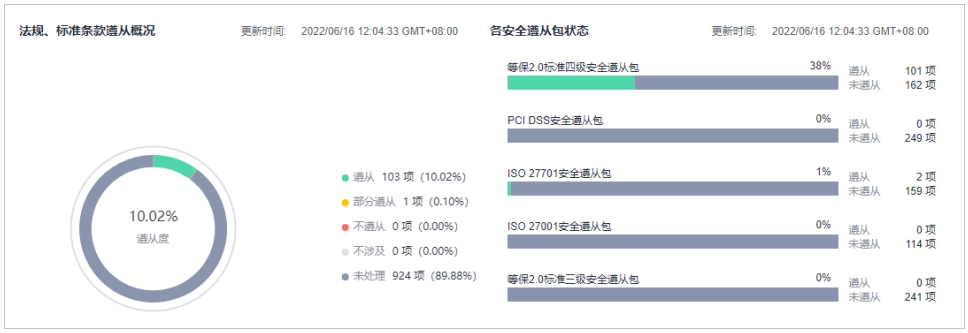
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“安全治理 > 合规总览”，进入合规总览页面。

图 6-7 进入合规总览页面

步骤4 在合规总览页面中，查看“法规、标准条款遵从概况”。

图 6-8 法规、标准条款遵从概况



----结束

查看策略扫描概况

步骤1 登录管理控制台。

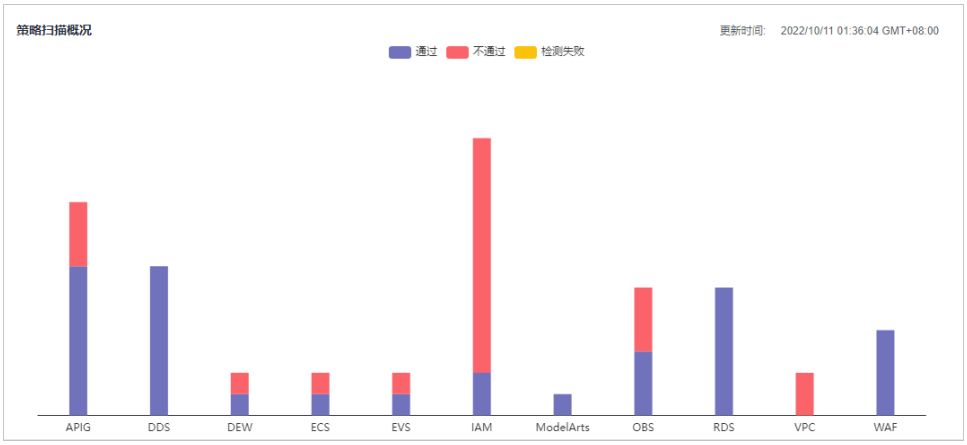
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 在左侧导航栏选择“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-9 进入订阅列表页面

步骤4 在合规总览页面中，查看“策略扫描概况”。

图 6-10 策略扫描概况



----结束

6.8 查看治理结果

操作场景

订阅安全遵从包后，安全云脑将自动依据安全遵从包进行扫描。扫描后，可查看整体遵从情况，并查看改进建议。

前提条件

已订阅安全遵从包，详细操作请参见**订阅安全遵从包**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-11 进入订阅列表页面

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

图 6-12 治理结果

步骤5 查看治理结果。

图 6-13 治理结果界面

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

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

  a. 在左边目录树选择需要自评估的条款。

  图 6-14 选择条款

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

如果有相关的凭据，可单击“附件上传”。

图 6-15 自评估

c. 完成自评估后单击右上角的“提交”，完成该条款下单个检查项的评估。

----结束

6.9 查看策略扫描结果

操作场景

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

说明

策略扫描将在每日凌晨1:30自动扫描一次并生成扫描结果。

前提条件

已订阅安全遵从包，详细操作请参见**订阅安全遵从包**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 策略扫描”，进入策略扫描页面。

图 6-16 进入策略扫描页面

步骤4 查看策略扫描结果。

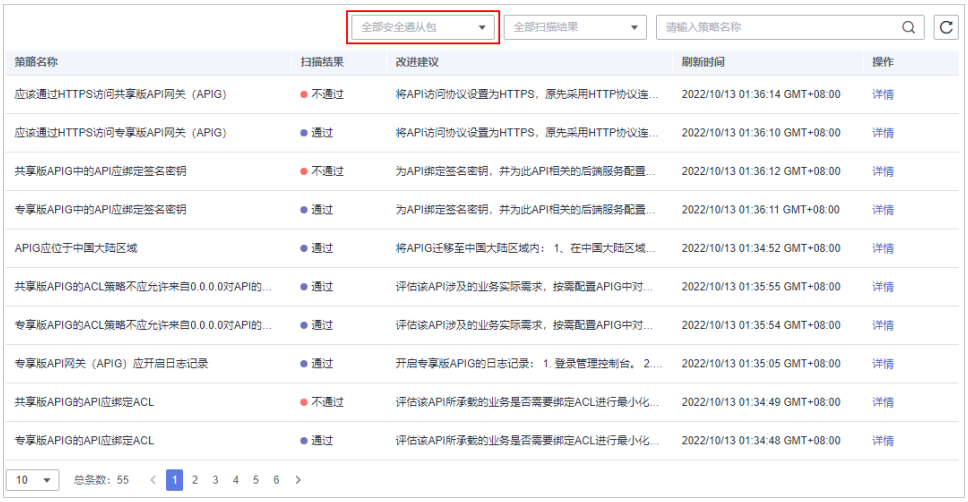
图 6-17 策略扫描

- 默认展示所有资源的所有策略扫描情况。
  - 策略扫描情况：所有资源的所有策略扫描情况率、通过、不通过以及检测失败情况。
  - 风险点TOP5：策略扫描时，不通过的策略TOP5。
- 如需查看某个资源的所有策略扫描情况，可在上方筛选框中，选择对应资源。

图 6-18 选择资源

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

图 6-19 选择遵从包

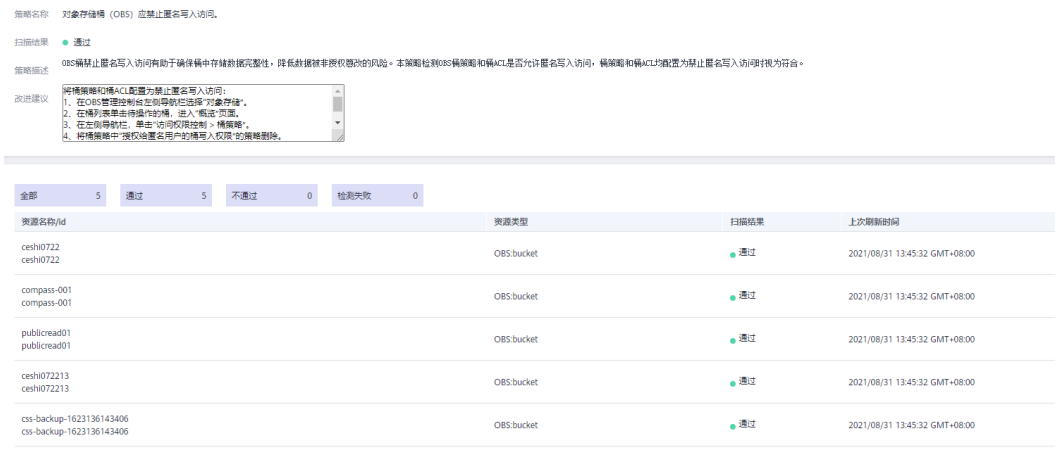


- 如需查看某个资源的某个策略扫描情况，可先在上方筛选框中，选择对应资源，再在表格上方，选择对应遵从包。

图 6-20 具体筛选

步骤5 在下方策略表格中，单击具体策略“操作”列的“详情”，可进入到相应策略扫描结果界面，查看具体改进建议，如图6-21所示。

图 6-21 策略扫描详情



说明

每天凌晨1:30自动扫描一次并生成扫描结果。

----结束

6.10 下载安全合规报表

操作场景

安全治理提供安全合规报表的功能，支持下载当前资源的合规情况。

前提条件

已订阅安全遵从包，详细操作请参见**订阅安全遵从包**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-22 进入订阅列表页面

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

系统将下载指定合规的报表到本地路径。

----结束

6.11 取消订阅安全遵从包

操作场景

当您需要更换或取消当前订阅的安全遵从包时，可在订阅列表删除该安全遵从包。

前提条件

已订阅安全遵从包，详细操作请参见**订阅安全遵从包**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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“安全治理 > 订阅列表”，进入订阅列表页面。

图 6-23 进入订阅列表页面

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

步骤5 在弹出的确认框中，单击“确认”。

说明

删除后，对该安全遵从包的处理结果将清空，且不可恢复，请谨慎操作。

----结束

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的整体安全评估状况，帮助您全量了解资产的安全情况，包括资产的安全评估结果、安全监控和安全趋势等信息。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 态势总览”，进入态势总览页面。

图 7-2 态势总览

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

- **安全评分**
- **安全监控**
- **安全趋势**

各个板块数据统计周期及更新频率如下表所示：

表 7-1 态势总览

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

----结束

安全评分

“安全评分”板块根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况，如**图7-3**。

图 7-3 安全评分

- 安全评分每天凌晨2:00自动更新，也支持通过单击“重新检测”来进行实时更新。
- 分值范围为0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见**安全分值和扣分项说明**。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 单击“立即处理”，系统右侧弹出“安全风险处理”页面，您可根据该页面的提示，参考对应的帮助文档或直接对风险进行处理。
  - 安全风险处理页面中包含所有需要您尽快处理的安全风险和威胁，分为“威胁告警”、“漏洞”、“合规检查”三大类别。
  - “安全风险处理”页面中显示的数据为最近/最新检测后的数据结果，“告警管理”、“漏洞管理”、“基线检查”页面（单击“前往处理”，进入该页面）显示的是所有检测时间的各类数据详情，因此，安全风险处理页面的数据总数≤告警管理或漏洞管理页面的数据总数。
  - **处理安全风险**：
    i. 在“安全评分”栏中，单击“立即处理”，系统右侧弹出“安全风险处理”页面。
    ii. 在“安全风险处理”页面中，单击“前往处理”，进入“告警管理”、“漏洞管理”或“基线检查”页面。
    iii. 对风险告警、漏洞或基线检查项目进行处理。
- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。资产安全风险修复后，也可以直接单击“重新检测”，重新检测资产并进行评分。

  说明

  资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。
- 安全评分显示为历史扫描结果，**非实时**数据，如需获取最新数据及评分，可单击“重新检测”，获取最近的数据。

安全分值和扣分项说明

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

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

  SecMaster根据不同版本的威胁检测能力，评估整体资产安全健康得分。
  - 风险等级包括“无风险”、“提示”、“低危”、“中危”、“高危”和“致命”。

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

  说明

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

表 7-2 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7-3所示。

表 7-3 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		

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

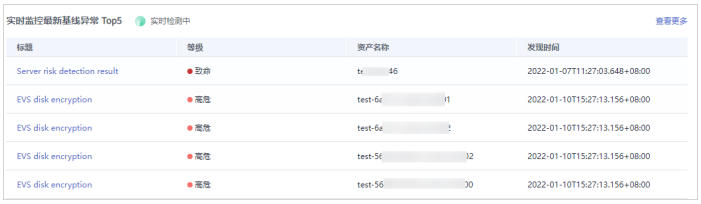
“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

图 7-4 安全监控

表 7-4 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**当前工作空间中未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。统计信息更新频率为每5分钟更新一次。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 ● 单击威胁告警模块，系统将列表实时呈现**近7天内**TOP5的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 列表呈现近7天TOP5的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 如果列表显示内容为空，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，查看威胁告警详细操作请参见**查看告警信息**。 **图 7-5** 查看实时威胁告警 

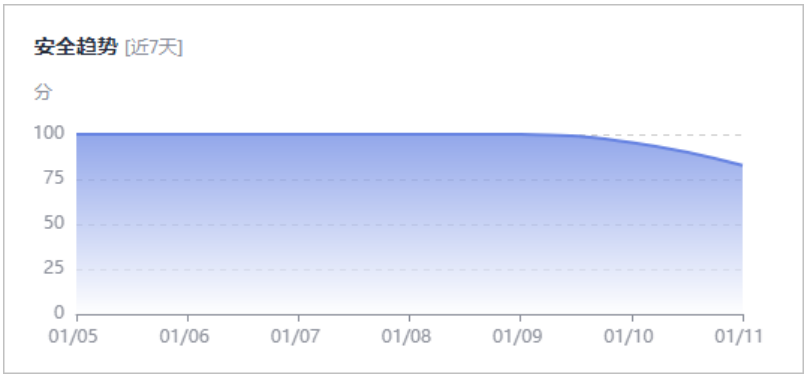
参数名称	参数说明
漏洞	展示当前工作空间中您资产中TOP5漏洞类型，以及**近7天内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。统计信息更新频率为每5分钟更新一次。 • 此处严重等级含义如下： – 高危：即高危风险，表示资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 中危：即中危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 • 单击漏洞模块中的“漏洞类型Top5”栏，系统将列表呈现TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的TOP等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 仅当主机中Agent版本为2.0时，才会在“漏洞类型Top5”中显示对应数据。如未显示数据或需要查看TOP5漏洞类型，请将主机将Agent1.0升级至Agent2.0。 **图 7-6** 漏洞类型  • 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。 – 如果列表显示内容为空，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，查看漏洞详细操作请参见**查看漏洞详情**。

参数名称	参数说明
	图 7-7 查看实时漏洞 
合规检查	展示当前工作空间中您资产中存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。统计信息更新频率为每5分钟更新一次。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看合规检查事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该合规检查项目的详情。 ● 单击合规检查异常模块，系统将列表实时呈现**近30天内**TOP5的合规检查异常事件，可快速查看合规检查详情。 – 列表呈现最近一次合规检查中TOP的合规异常事件详情，包括合规检查项目名称、等级、受影响资产数量、发现时间。 – 如果列表显示内容为空，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，查看合规检查详细操作请参见**查看基线检查结果**。 **图 7-8** 查看合规异常事件 

安全趋势

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

图 7-9 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。

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。

前提条件

已开通**安全大屏**增值项，详细操作请参见**购买增值包**。

操作步骤

步骤1 登录管理控制台。

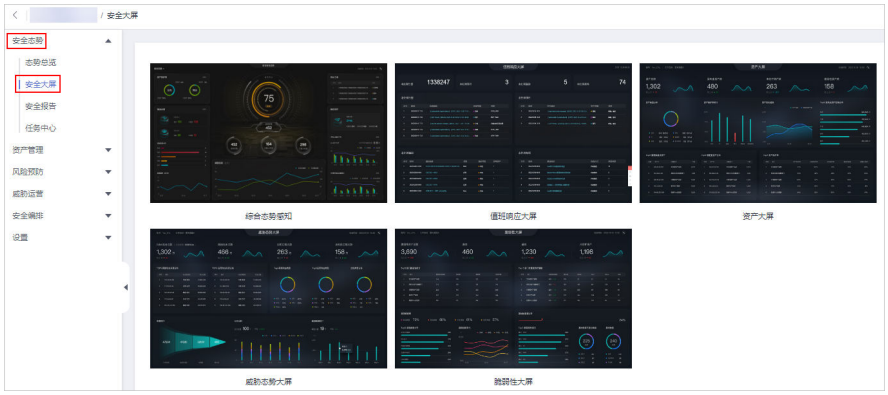
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-10 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

图 7-11 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，如图7-12。

页面中各个模块的功能介绍和使用方法详见下述内容。

图 7-12 综合态势感知大屏

----结束

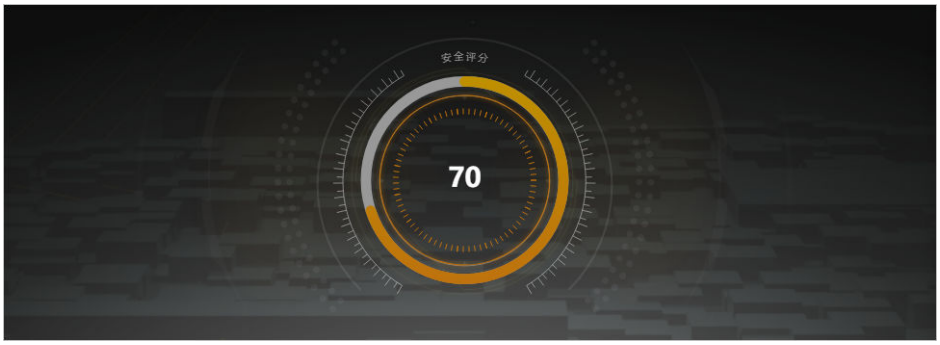
安全评分

如图7-13所示，展示当前资产安全健康得分。

表 7-5 安全评分

参数名称	统计周期	更新频率	说明
安全评分	实时	• 每天2:00自动更新 • 随当前工作空间“态势总览”中的“安全评分”手动更新而更新，约有5分钟延迟	根据是否开启各安全服务防护、未处理的配置问题等级及个数、未处理的漏洞等级及个数、未处理的威胁事件等级及个数等，加权计算得来。 • 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”。

图 7-13 安全评分



告警统计情况

如图7-14所示，展示已接入服务的告警统计情况。

告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。

表 7-6 告警统计情况

参数名称	统计周期	更新频率	说明
新增告警	今天	5分钟	当天新增的告警数量。
威胁告警	近7天	5分钟	近7天新增的告警数量。
待解决告警	近7天	5分钟	近7天“状态”不是“关闭”的告警数量。

参数名称	统计周期	更新频率	说明
已解决告警	近7天	5分钟	近7天“状态”为“关闭”的告警数量。

图 7-14 告警统计情况

资产防护率

如图7-15所示，展示近7天内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。

表 7-7 资产防护率

参数名称	统计周期	更新频率	说明
资产防护率	近7天	5分钟	近7天内主机和网站的防护情况，包含已防护和未防护资产的比例。 • 主机防护情况：已开启和未开启主机安全服务 HSS的ECS数量统计。 • 网站防护情况：已开启和未开启Web应用防火墙 WAF防护网站数据统计。

图 7-15 资产防护率

基线合规

如图7-16所示，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。

- 基线数据统计情况来源于当前工作空间的“风险预防 > 基线检查”，如需查看对应详细信息，可以前往该页面进行查看。
- 漏洞数据统计情况来源于当前工作空间的“风险预防 > 漏洞管理”，如需查看对应详细信息，可以前往该页面进行查看。

表 7-8 基线合规

参数名称	统计周期	更新频率	说明
配置基线	实时	5分钟	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	近7天	5分钟	近7天的漏洞处理情况，包括已修复、未修复漏洞的数量。
风险资源分布	实时	5分钟	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	近7天	5分钟	近7天的每日新增的漏洞数据及其分布趋势。

图 7-16 基线合规

威胁态势

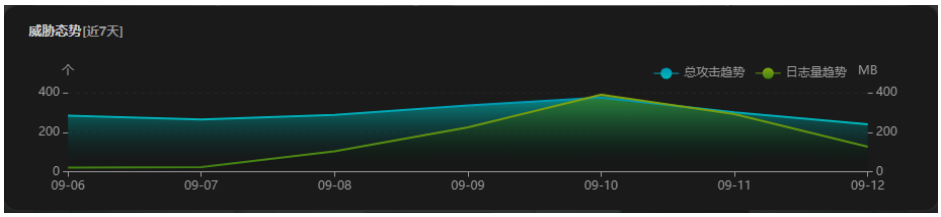
如图7-17所示，展示**近7天内**每日受到威胁的资产的数量和**近7天内**每日上报的安全日志日志量大小。

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。

表 7-9 威胁态势

参数名称	统计周期	更新频率	说明
总攻击趋势	近7天	5分钟	近7天每日告警数量。 告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。
日志量趋势	近7天	5分钟	近7天每日上报的安全日志日志量大小。

图 7-17 威胁态势



待办工单

如图7-18所示，实时展示当前工作空间内的待办事项。

表 7-10 待办工单

参数名称	统计周期	更新频率	说明
待办工单	实时	5分钟	当前工作空间内的“安全态势 > 任务中心”中待办的任务。

图 7-18 待办工单

响应闭环

如图7-19所示，展示告警处置情况、近7天内SLA（计划关闭时间）和MTTR（平均恢复时间）达成率和近7天内事件自动处置统计情况。

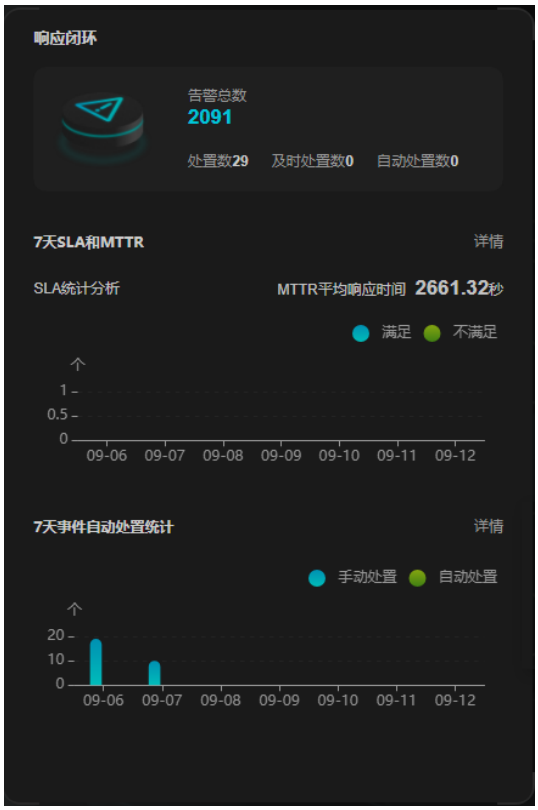
告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。

表 7-11 响应闭环

参数名称		统计周期	更新频率	说明
告警统计	告警总数	近7天	5分钟	近7天新增的告警数量。
	处置数			近7天“状态”为“关闭”的告警数量。
	及时处置数			近7天“状态”为“关闭”且满足计划关闭时间的告警数量。 满足计划关闭时间是指关闭时间早于或等于计划关闭时间。
	自动处置数			近7天“状态”为“关闭”且为安全云脑剧本等自动关闭的告警数量。 告警关闭方式查看方法：在告警详情中查看“close_comment”字段中的数值是否为“ClosedByCSB”或“ClosedBySecMaster”，如果是，则为自动关闭，如果不是则为手动关闭。

参数名称		统计周期	更新频率	说明
7天SLA和MTTR	SLA统计分析	近7天	5分钟	近7天告警处理的时效满足情况。计算方法如下： 已设置了SLA（计划关闭时间）字段的告警，当告警关闭时间-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。 ● 满足：告警关闭时间早于或等于告警计划关闭时间； ● 不满足：告警关闭时间晚于告警计划关闭时间。
	MTTR平均响应时间			近7天平均告警关闭时间。计算方法如下： MTTR（平均恢复时间）=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		近7天	5分钟	近7天告警被手动处理和自动处理了的统计总数。 ● 手动处置：告警管理中手动关闭的告警数量； ● 自动处置：由安全云脑剧本等方式自动关闭的告警数量。 告警关闭方式查看方法：在告警详情中查看“close_comment”字段中的数值是否为“ClosedByCSB”或“ClosedBySecMaster”，如果是，则为自动关闭，如果不是则为手动关闭。

图 7-19 响应闭环



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。

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。

前提条件

已开通**安全大屏**增值项，详细操作请参见**购买增值包**。

操作步骤

步骤1 登录管理控制台。

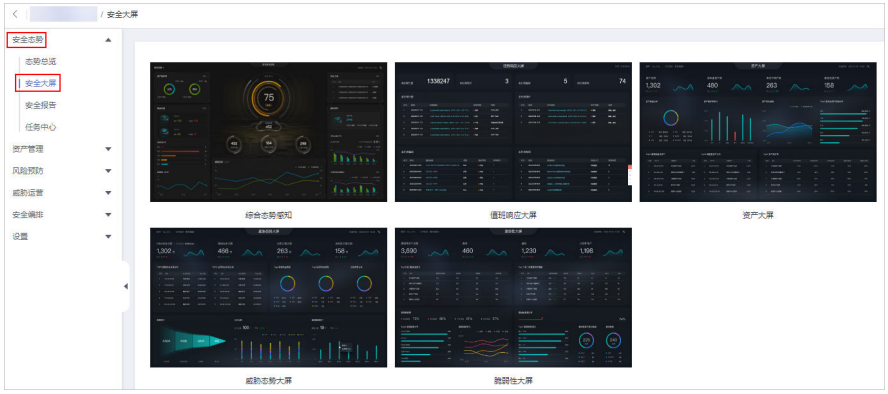
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-20 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

图 7-21 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，如图7-22。

页面中各个模块的功能介绍和使用方法详见下述内容。

图 7-22 值班响应大屏

----结束

值班响应大屏总览

如图7-23所示，展示未处理告警、事件、漏洞、基线的总数。

表 7-12 值班响应大屏总览

参数名称	统计周期	更新频率	说明
未处理告警	近7天	5分钟	近7天“状态”为“打开”的告警数量。 告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。
未处理事件	近7天	5分钟	近7天“状态”为“打开”或“阻塞”的事件数量。 事件数据统计情况来源于当前工作空间的“威胁运营 > 事件管理”，如需查看对应详细信息，可以前往该页面进行查看。
未处理漏洞	实时	5分钟	未处理漏洞统计数据。 漏洞数据统计情况来源于当前工作空间的“风险预防 > 漏洞管理”，如需查看对应详细信息，可以前往该页面进行查看。
未处理基线	实时	5分钟	基线检查中检查不通过的统计数据。 基线数据统计情况来源于当前工作空间的“风险预防 > 基线检查”，如需查看对应详细信息，可以前往该页面进行查看。

图 7-23 值班响应大屏总览

未处理告警

如图7-24所示，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。

表 7-13 未处理告警

参数名称	统计周期	更新频率	说明
未处理告警	近7天	5分钟	近7天“状态”为“打开”的告警数量。 告警数据统计情况来源于当前工作空间的“威胁运营 > 告警管理”，如需查看对应详细信息，可以前往该页面进行查看。

图 7-24 未处理告警

未处理事件

如图7-25所示，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。

表 7-14 未处理事件

参数名称	统计周期	更新频率	说明
未处理事件	近7天	5分钟	近7天“状态”为“打开”或“阻塞”的事件数量。 事件数据统计情况来源于当前工作空间的“威胁运营 > 事件管理”，如需查看对应详细信息，可以前往该页面进行查看。

图 7-25 未处理事件

未处理漏洞

如图7-26所示，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。

表 7-15 未处理漏洞

参数名称	统计周期	更新频率	说明
未处理漏洞	近7天	5分钟	未处理漏洞统计数据。 漏洞数据统计情况来源于当前工作空间的“风险预防 > 漏洞管理”，如需查看对应详细信息，可以前往该页面进行查看。

图 7-26 未处理漏洞

未处理基线

如图7-27所示，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。

表 7-16 未处理基线

参数名称	统计周期	更新频率	说明
未处理基线	近7天	5分钟	基线检查中检查不通过的统计数据。 基线数据统计情况来源于当前工作空间的“风险预防 > 基线检查”，如需查看对应详细信息，可以前往该页面进行查看。

图 7-27 未处理基线

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。

前提条件

已开通**安全大屏**增值项，详细操作请参见**购买增值包**。

操作步骤

步骤1 登录管理控制台。

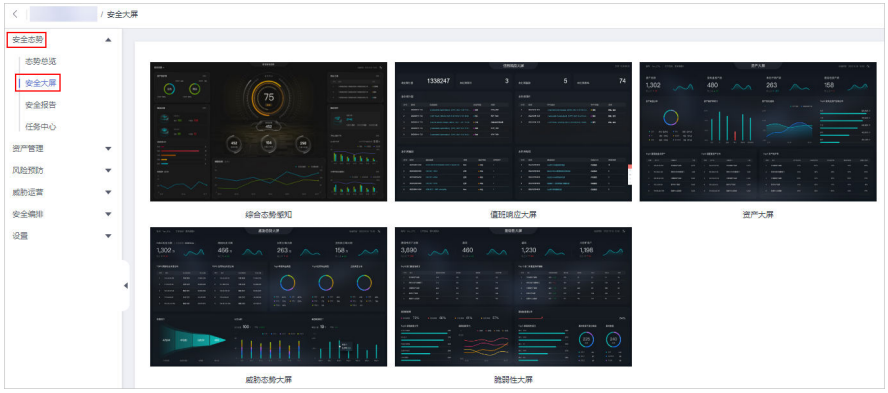
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-28 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

图 7-29 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，如**图7-30**。

页面中各个模块的功能介绍和使用方法详见下述内容。

图 7-30 资产大屏

----结束

资产大屏总览

如图7-31所示，展示当前工作空间内资产、受攻击资产、未防护资产、漏洞和弱配置资产的总数。

表 7-17 资产大屏总览

参数名称	统计周期	更新频率	说明
资产总数	实时	每小时	“资产管理”中的全部资产数量。
受攻击资产数	近7天	每小时	“威胁运营 > 告警管理”中，受告警影响的资产去重后的数量。
未防护资产数	实时	每小时	未开启安全防护的资产数量，例如，没有开启主机安全的ECS，没有开启DDoS的弹性公网IP等。 “资产管理”中“防护状态”不是“已防护”的资产。
漏洞和弱配置资产数	实时	每小时	受漏洞影响资产和基线检查中检查资源存在风险项的资产去重后的数据。 漏洞数据来源于“风险预防 > 漏洞管理”，基线检查数据来源于“风险预防 > 基线检查”中“检查资源”页签，如需查看对应详细信息，可以前往该页面进行查看。

图 7-31 资产大屏总览

资产分布情况

如图7-32所示，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。

表 7-18 资产分布情况

参数名称	统计周期	更新频率	说明
资产类型分布	实时	每小时	“资产管理”中的全部资产的不同类型资产的数量。
资产防护率统计	实时	每小时	不同类型资产开启安全防护的比例。 某一类型资产的开启安全防护的比例 = “防护状态”为“已防护”的资产 / 该类型资产总数。
资产变化趋势	近7天	每小时	近7天资产总数和存在漏洞、弱配置的资产数统计。
TOP5 受攻击资产	近7天	每小时	近7天受到攻击的前五名资产及其被攻击次数。 该数据来源于“威胁运营 > 告警管理”页面中，近7天告警数据中受影响资产统计情况，如需查看对应详细信息，可以前往该页面进行查看。

图 7-32 资产分布情况

TOP5 漏洞数最多资产和 TOP5 资产防护率

如图7-33所示，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。

表 7-19 TOP5 漏洞数最多资产和 TOP5 资产防护率

参数名称	统计周期	更新频率	说明
Top5 漏洞数最多资产	实时	每小时	不同部门存在漏洞最多的资产前五名。 资产统计信息为“风险预防 > 漏洞管理”页面中受漏洞影响资产（该资产须在“资产管理”页面中的部门信息不为空的资产），按照部门进行统计后取前五名的资产。

参数名称	统计周期	更新频率	说明
Top5 资产防护率	实时	每小时	不同部门资产开启防护的比例，由高到低前五名。 “资产管理”中部门信息不为空的资产，按照部门进行统计后取前五名的信息。

图 7-33 漏洞最多资产和资产防护率

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。

前提条件

已开通**安全大屏**增值项，详细操作请参见**购买增值包**。

操作步骤

步骤1 登录管理控制台。

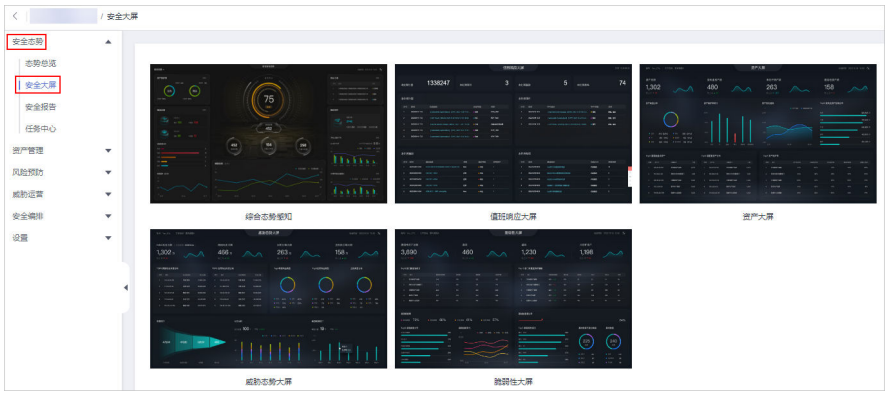
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-34 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

图 7-35 进入安全大屏页面



步骤5 单击“威胁态势大屏”图片，进入威胁态势大屏信息页面，如图7-36。

页面中各个模块的功能介绍和使用方法详见下述内容。

图 7-36 威胁态势大屏

----结束

威胁态势大屏总览

如图7-37所示，展示当前账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。

表 7-20 威胁态势大屏总览

参数名称		统计周期	更新频率	说明
网络日志攻击	次数	近7天	每小时	近7天弹性公网IP被攻击的次数。
	较上周			近7天弹性公网IP被攻击次数，与近7-14天弹性公网IP被攻击次数的差值。
应用日志攻击	次数	近7天	每小时	近7天网站被攻击次数。

参数名称		统计周期	更新频率	说明
	较上周			近7天网站被攻击次数，与近7-14天网站被攻击次数的差值。
主机日志攻击	次数	近7天	每小时	近7天ECS被攻击次数。
	较上周			近7天ECS被攻击次数，与近7-14天ECS被攻击次数的差值。

图 7-37 威胁态势大屏总览

攻击来源分布情况

如图7-38所示，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。

表 7-21 攻击来源分布情况

参数名称	统计周期	更新频率	说明
Top5 网络日志攻击来源分布	近7天	每小时	近7天弹性公网IP被攻击的情况，按照攻击的源IP进行聚合统计，按照聚合后的统计次数由多到少取前五名。
Top5 应用告警攻击来源分布	近7天	每小时	近7天网站被攻击的情况，按照攻击的源IP进行聚合统计，按照聚合后的统计次数由多到少取前五名。

图 7-38 攻击来源分布

攻击类型分布

如图7-39所示，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。

表 7-22 攻击类型分布

参数名称	统计周期	更新频率	说明
Top5 网络告警攻击类型	近7天	每小时	近7天弹性公网IP被攻击的类型统计，按照不同类型的攻击从多到少取前5名。 如果不存在网络攻击或没有对应数据表，则会展示五项全为0的默认类型。
Top5 应用告警攻击类型	近7天	每小时	近7天网站被攻击的类型统计，按照不同类型的攻击从多到少取前5名。 如果不存在应用攻击或没有对应数据表，则会展示五项全为0的默认类型。
Top5 主机告警攻击类型	近7天	每小时	近7天ECS被攻击的类型统计，按照不同类型的攻击从多到少取前5名。 如果不存在ECS攻击或没有对应数据表，则会展示五项全为0的默认类型。 资产统计信息来源于安全云脑的“威胁运营 > 告警管理”页面。

图 7-39 攻击类型分布

威胁态势统计

如图7-40所示，当前账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。

表 7-23 威胁态势统计

参数名称		统计周期	更新频率	说明
告警统计	日志条数	近7天	每小时	近7天网络、应用、主机被访问产生的日志条数总和。
	威胁攻击数			近7天网络、应用、主机识别为被攻击产生的日志条数总和。

参数名称		统计周期	更新频率	说明
	告警数			近7天“威胁运营 > 告警管理”中依据攻击日志产生的告警数量。
	事件数			近7天“威胁运营 > 事件管理”依据告警，转为的事件数量。
日志分析	总日志量	近7天	每小时	近7天网络、应用、主机被访问产生的日志大小总和，单位为MB。
	环比			近7天网络、应用、主机被访问产生的日志大小总和，与近7-14天用户网络、应用、主机被访问产生的日志大小总和的对比。 计算方法：（本期数 - 上期数）/ 上期数 × 100%。
	统计趋势图			近7天每天网络、应用、主机被访问产生的日志大小总和，单位为MB。
模型监测统计	模型总数	实时	每小时	“威胁运营 > 智能建模”中已有模型的数量。
	统计表格	近7天	每小时	每种类型的威胁检测模型，检测出的威胁次数。 如果没有威胁检测模型，则会默认展示四种类型，其值全部为0。

图 7-40 威胁态势统计

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。

前提条件

已开通**安全大屏**增值项，详细操作请参见**购买增值包**。

操作步骤

步骤1 登录管理控制台。

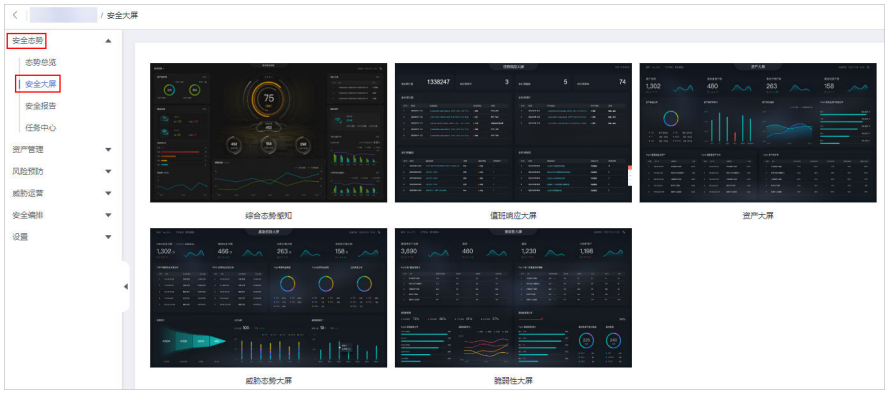
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-41 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

图 7-42 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，如图7-43。

页面中各个模块的功能介绍和使用方法详见下述内容。

图 7-43 脆弱性大屏

----结束

脆弱性大屏总览

如图7-44所示，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。

表 7-24 脆弱性大屏总览

参数名称	统计周期	更新频率	说明
脆弱性资产总数	实时	每小时	存在漏洞、基线检查问题的资产数量统计
漏洞	实时	每小时	漏洞管理中的漏洞统计数据
不合格基线数	实时	每小时	安全云脑基线检查中的数据
未防护资产	实时	每小时	用户没有开启安全防护的资产数量，例如没有开启主机安全的ECS，没有开启DDoS的弹性公网IP等。

图 7-44 脆弱性大屏总览

TOP5 部门脆弱性统计

如图7-45所示，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。

表 7-25 部门脆弱性统计

参数名称	统计周期	更新频率	说明
Top5 部门脆弱性统计	实时	每小时	不同部门存在脆弱性资产、受漏洞影响资产、未防护的资产总和，从多到少排列的前五名资产。 脆弱性资产包括“风险预防 > 漏洞管理”中受漏洞影响的资产、“风险预防 > 基线检查”中包含检查不通过项的资产、“资产管理”中未开启防护的资产相加的总数，按照部门进行统计后取的前五名。其中，资产须在“资产管理”页面中的部门信息不为空的资产。

图 7-45 TOP5 部门脆弱性统计

TOP5 部门未防护统计

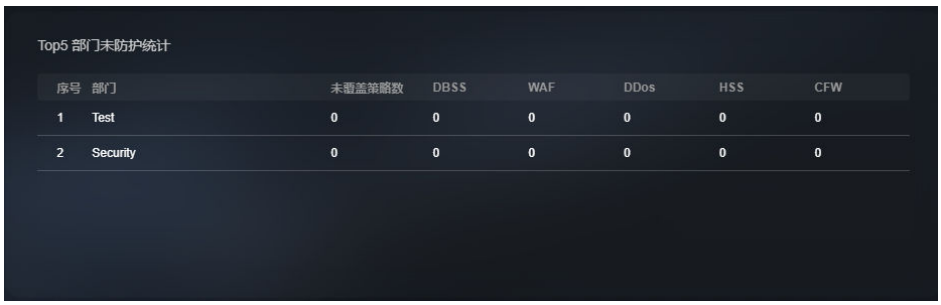
如图7-46所示，列表呈现TOP5的部门未覆盖防护策略情况，包括部门的名称、未覆盖策略数、DBSS、WAF、DDoS、HSS、CFW。

TOP5是从部门索引取值，按未防护资产数降序排序。

表 7-26 部门未防护统计

参数名称	统计周期	更新频率	说明
Top5 部门未防护统计	实时	每小时	不同部门未开启安全防护的资产，将其未开启的安全服务进行统计计数。将总数按从多到少排列，取前5名。

图 7-46 TOP5 部门未防护统计



漏洞修复率

如图7-47所示，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。

表 7-27 漏洞修复率

参数名称	统计周期	更新频率	说明
漏洞修复率	实时	每小时	漏洞修复率 =（已修复漏洞数 / 漏洞总数）* 100%。 如果不存在漏洞，则全部显示为100%。
漏洞类型分布	实时	每小时	漏洞按照漏洞的类型进行统计。
漏洞趋势变化	近7天	每小时	近7天的漏洞按照严重程度进行分类计数。

图 7-47 漏洞修复率

基线检查通过率

如图7-48所示，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。

表 7-28 基线检查通过率

参数名称	统计周期	更新频率	说明
基线检查通过率	实时	每小时	基线检查通过率 =（基线检查合格项 / 总检查项）* 100%。
基线自动检查不通过资源统计	实时	每小时	基线检查不合格项，按照严重程度统计其影响的资源数。
基线检查	实时	每小时	基线检查合格、不合格、失败数量统计。

图 7-48 基线检查通过率

7.3 安全报告

7.3.1 创建/复制安全报告

操作场景

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。

约束与限制

单账号单workspace内，最多可创建10个安全报告（包含日报、周报和月报）。

前提条件

已购买安全云脑专业版，且在有效使用期内。

创建安全报告

步骤1 登录管理控制台。

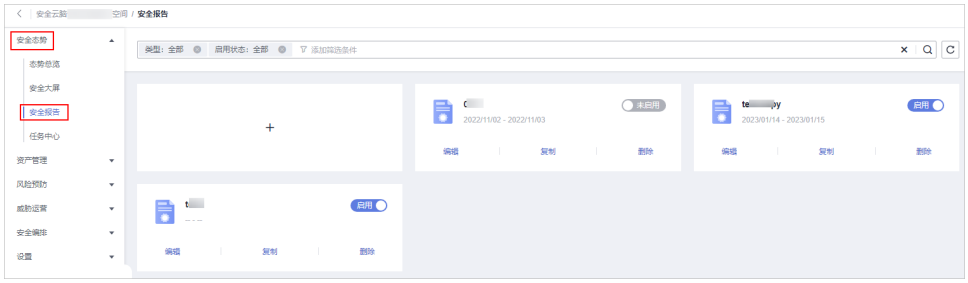
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-49 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 7-50 进入安全报告页面



步骤5 在安全报告页面中单击 + 按钮，进入配置报告基本信息页面。

步骤6 配置报告基本信息。

表 7-29 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00:00~24:00的安全信息。 • 周报：默认统计上一周安全信息，上周一00:00到上周日24:00。 • 月报：默认统计上一月安全信息，上月第一天00:00到上月最后一天24:00。 • 自定义：自定义选择时间范围。
统计周期	根据您选择的“报告类型”显示安全报告统计周期。 当“报告类型”选择“日报”、“周报”或“月报”时，系统会根据您选择的“报告类型”显示安全报告统计周期。
报告发送时间	当“报告类型”选择为“日报”、“周报”或“月报”时，需要设置报告发送时间。 • 日报：设置为每天报告的发送时间点，默认发送前一天00:00:00~23:59:59的安全信息报告。 • 周报：设置为每周报告的发送时间点，默认发送上周一00:00到上周日24:00的安全信息报告。 • 月报：设置为每月报告的发送时间点，默认发送前一个月整月的安全信息报告。
报告发送频次	当“报告类型”选择“自定义”时，需要选择安全报告的发送频次。
发送规则	当“报告类型”选择“自定义”时，需要设置报告的发送时间以及统计范围。 最多可添加5个发送规则。
邮件标题	设置报告发送邮件的标题信息。

参数名称	参数说明
报告接收人邮箱	添加接收人邮箱地址。 • 最多可添加100个邮箱地址。 • 有多个邮箱地址，请使用英文逗号隔开。例如：test01@example.com,test02@example.com
（可选）抄送	添加抄送人邮箱地址。 • 最多可添加100个邮箱地址。 • 有多个邮箱地址，请使用英文逗号隔开。例如：test03@example.com,test04@example.com
（可选）备注	自定义安全报告的备注信息。

步骤7 单击右上角“下一步：报告选择”，进入报告选择页面。

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

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

- 下载报告
  a. 单击右侧预览页面左上角的  。
  b. 在弹出的下载对话框中，选择报告格式，并单击“确定”。
  系统将自动下载对应格式的报告到本地。
- 全屏查看报告：单击右侧预览页面左上角的  ，可以全屏查看安全报告。

步骤9 单击右下角“完成”，返回安全报告管理页面，即可查看创建的安全报告。

----结束

复制安全报告

步骤1 登录管理控制台。

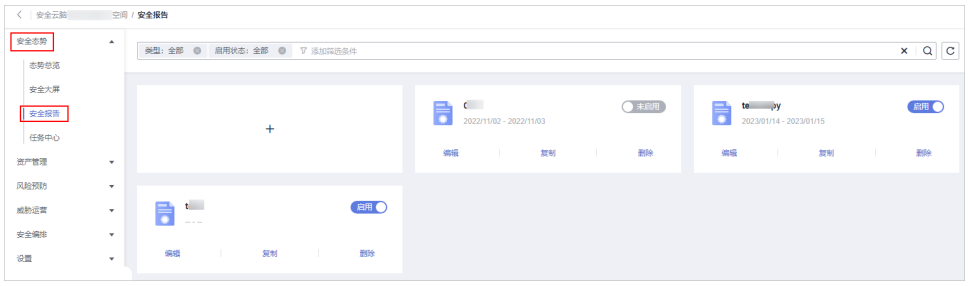
步骤2 在页面左上角单击  ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-51 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 7-52 进入安全报告页面



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

步骤6 修改报告基本信息。

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

- 下载报告
  a. 单击右侧预览页面左上角的  。
  b. 在弹出的下载对话框中，选择报告格式，并单击“确定”。
  系统将自动下载对应格式的报告到本地。
- 全屏查看报告：单击右侧预览页面左上角的  ，可以全屏查看安全报告。

步骤8 单击右上角“完成”，返回安全报告管理页面，即可查看复制的安全报告。

----结束

7.3.2 查看安全报告

操作场景

本章节介绍如何查看已创建的安全报告及其展示的信息。

操作步骤

步骤1 登录管理控制台。

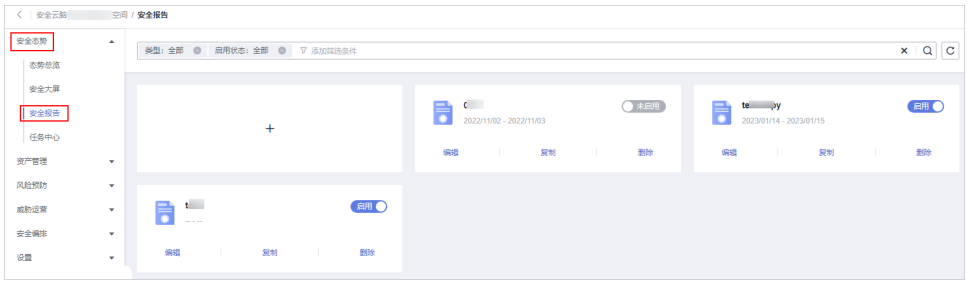
步骤2 在页面左上角单击  ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-53 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 7-54 进入安全报告页面



步骤5 选择目标报告，单击报告图标，跳转到报告详情页面。

在报告详情页面，可以预览当前安全报告的详细信息。

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

----结束

模板日报展示内容

表 7-30 模板日报展示内容

参数模块	参数说明
统计周期	日报默认统计周期为前一天00:00:00~23:59:59。
安全评分	根据您的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
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

参数模块	参数说明
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（总览）	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

参数模块	参数说明
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（详细信息）	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。

模板周报展示内容

表 7-31 模板周报展示内容

参数模块	参数说明
统计周期	周报默认统计周期为上周一00:00到上周日24:00。
安全评分	根据您的安全云脑的威胁检测能力，评估上周最后一天最新的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	展示上周最后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 ● 最后一次基线检查不合规检查项数量
安全漏洞	展示接入云服务上周日最新的漏洞统计情况，包含以下信息： ● 漏洞总数量 ● 未修复漏洞数量

参数模块	参数说明
策略覆盖	展示上周最后一天最新的安全产品覆盖情况，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	展示上周最后一天最新的资产安全情况，包含以下信息： ● 资产总数量 ● 存在风险的资产数量
安全分析	展示安全分析统计情况，包含以下信息： ● 上周一整周安全日志总流量 ● 上周最后一天的安全日志模型数量
安全响应（总览）	展示上周一整周安全响应情况，包含以下信息： ● 上周一整周已处置的安全告警数量 ● 上周一整周确认的入侵事件数量 ● 运行的自动化响应剧本数量 ● 自动化剧本闭环率 ● MTTR平均时间 ● 确认高风险入侵事件数量
资产风险	展示上周最后一天最新的资产安全状况，包含以下信息： ● 受攻击资产数量以及较月报统计月的上周的变化 ● 未防护资产数以及较月报统计月的上周的变化 ● 脆弱性资产数以及较月报统计月的上周的变化 ● 上周的资产变化趋势 ● 资产防护率

参数模块	参数说明
威胁态势	展示上周最后一天最新的资产的威胁态势情况，包含以下信息： ● DDoS攻击次数 ● 网络攻击次数 ● 应用攻击次数 ● 主机攻击次数 ● DDoS巡检情况 ● 网络攻击变化趋势 ● WAF巡检情况 ● TOP5网络攻击类型统计情况 ● TOP5应用攻击类型统计情况 ● TOP5主机攻击类型统计情况 ● TOP5应用攻击源分布情况 ● TOP5应用攻击目的分布情况 ● TOP主机告警分布情况 ● TOP5网络攻击源分布情况 ● 主机安全巡检情况
日志分析	展示上周一整周日志分析的情况，包含以下信息： ● 日志源数量 ● 日志索引数量 ● 日志接收总数 ● 日志存储总量 ● 日志存储量变化趋势 ● TOP5日志源接入量统计情况 ● TOP10模型检测告警统计数量
安全响应（详细信息）	展示上周一整周安全响应的情况，包含以下信息： ● 已处理告警数量 ● 已处理事件数量 ● 已处理漏洞数量 ● 已处理基线数量 ● 威胁告警分布情况及数量 ● TOP5入侵事件分布情况及数量 ● TOP5应急响应统计情况 ● TOP20威胁告警处理情况
外部安全热点	展示外部安全热点的情况。

模板月报展示内容

表 7-32 模板月报展示内容

参数模块	参数说明
统计周期	月报默认统计周期为上一个月整月。
安全评分	根据您的安全云脑的威胁检测能力，评估上一个月最后一天最新的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	展示上一个月最后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 ● 最后一次基线检查不合规检查项数量
安全漏洞	展示接入云服务上一个月最后一天最新的漏洞统计情况，包含以下信息： ● 漏洞总数量 ● 未修复漏洞数量
策略覆盖	展示上一个月最后一天最新的安全产品覆盖情况，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	展示上一个月最后一天最新的资产安全情况，包含以下信息： ● 资产总数量 ● 存在风险的资产数量
安全分析	展示安全分析统计情况，包含以下信息： ● 上一个月整月安全日志总流量 ● 上一个月最后一天的安全日志模型数量
安全响应（总览）	展示上一个月整月安全响应情况，包含以下信息： ● 上一个月整月已处置的安全告警数量 ● 上一个月整月确认的入侵事件数量 ● 运行的自动化响应剧本数量 ● 自动化剧本闭环率 ● MTTR平均时间 ● 确认高风险入侵事件数量

参数模块	参数说明
资产风险	展示上一个月最后一天最新的资产安全状况，包含以下信息： ● 受攻击资产数量以及较月报统计月的上一月的变化 ● 未防护资产数以及较月报统计月的上一月的变化 ● 脆弱性资产数以及较月报统计月的上一月的变化 ● 上一个月的资产变化趋势 ● 资产防护率
威胁态势	展示上一个月最后一天最新的资产的威胁态势情况，包含以下信息： ● DDoS攻击次数 ● 网络攻击次数 ● 应用攻击次数 ● 主机攻击次数 ● DDoS巡检情况 ● 网络攻击变化趋势 ● WAF巡检情况 ● TOP5网络攻击类型统计情况 ● TOP5应用攻击类型统计情况 ● TOP5主机攻击类型统计情况 ● TOP5应用攻击源分布情况 ● TOP5应用攻击目的分布情况 ● TOP主机告警分布情况 ● TOP5网络攻击源分布情况 ● 主机安全巡检情况
日志分析	展示上一个月整月日志分析的情况，包含以下信息： ● 日志源数量 ● 日志索引数量 ● 日志接收总数 ● 日志存储总量 ● 日志存储量变化趋势 ● TOP5日志源接入量统计情况 ● TOP10模型检测告警统计数量

参数模块	参数说明
安全响应（详细信息）	展示上一个月整月安全响应的情况，包含以下信息： • 已处理告警数量 • 已处理事件数量 • 已处理漏洞数量 • 已处理基线数量 • 威胁告警分布情况及数量 • TOP5入侵事件分布情况及数量 • TOP5应急响应统计情况 • TOP20威胁告警处理情况
外部安全热点	展示外部安全热点的情况。

安全报告样例

此处将以安全日报为例，展示安全报告样图，安全报告样例具体信息如下所示：

图 7-55 日报样例 1-信息总览

图 7-56 日报样例 2-资产风险

图 7-57 日报样例 3-威胁态势

图 7-58 日报样例 4-日志分析

图 7-59 日报样例 5-安全响应

图 7-60 日报样例 6-外部安全热点

7.3.3 下载安全报告

操作场景

使用自定义布局创建的安全报告支持下载报告至本地。

本章节将介绍如何下载报告至本地。

操作步骤

步骤1 登录管理控制台。

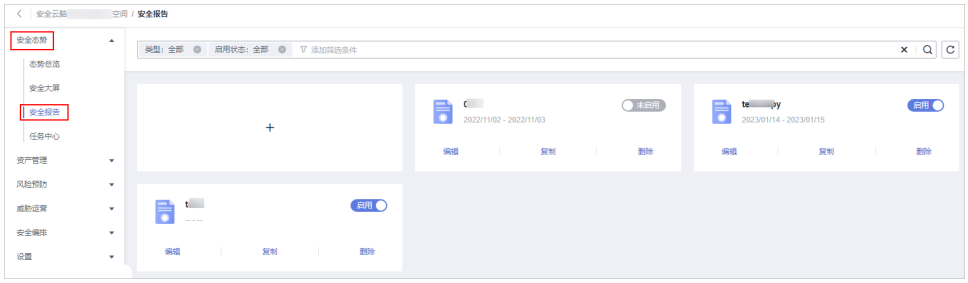
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-61 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 7-62 进入安全报告页面



步骤5 在已创建的目标安全报告模块，单击“编辑”，进入报告基本信息配置页面。

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

步骤6 单击右上角“下一步：报告选择”，进入报告选择配置页面。

步骤7 在报告选择页面，单击右侧预览页面左上角的  。

如需修改报告数据周期，可以在右侧预览页面右上角进行编辑。

步骤8 在弹出的下载对话框中，选择报告格式，并单击“确定”。

系统将自动下载对应格式的报告到本地。

----结束

7.3.4 管理安全报告

操作场景

本章节介绍如何管理安全报告，包括启用、停用、编辑、删除操作。

操作步骤

步骤1 登录管理控制台。

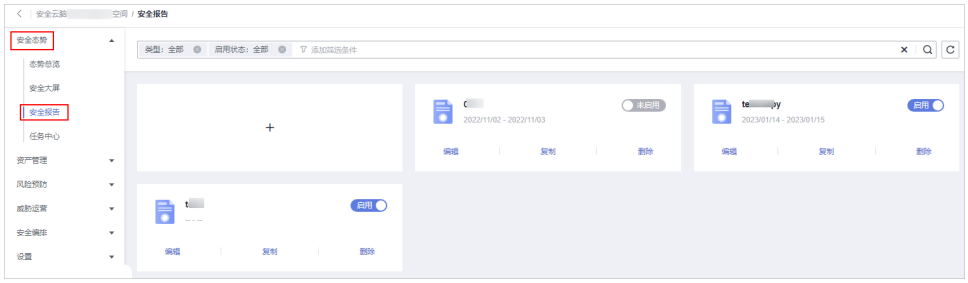
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-63 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

图 7-64 进入安全报告页面



步骤5 管理安全报告。

表 7-33 管理安全报告

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

----结束

7.4 任务中心

7.4.1 查看待办任务

操作场景

待办列表呈现当前需要您进行处理的任务，本章节主要介绍如何查看待办任务列表。

操作步骤

步骤1 登录管理控制台。

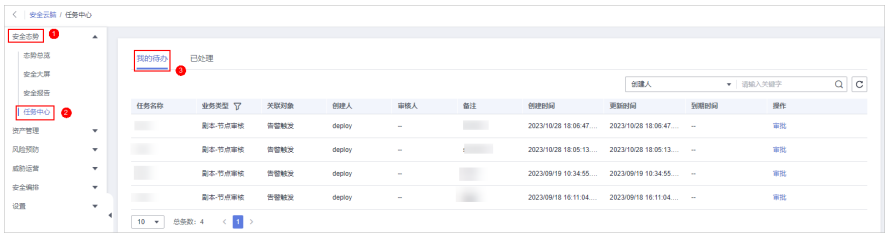
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-65 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 任务中心”，默认进入我的待办页面。

图 7-66 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”、“任务名称”或“备注”，并在搜索框中输入关键词，单击 🔍，即可快速查询指定待办任务。

表 7-34 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。

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

----结束

7.4.2 处理待办任务

操作场景

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

本章节主要介绍如何处理待办任务。

前提条件

已触发剧本/流程任务，且任务流程需人工处理。

操作步骤

步骤1 登录管理控制台。

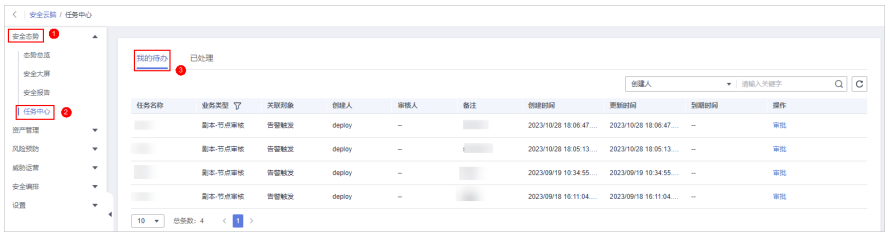
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 7-67 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全态势 > 任务中心”，默认进入我的待办页面。

图 7-68 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

7.4.3 查看已处理任务

操作场景

已处理列表呈现当前您已处理的任务，本章节主要介绍如何已处理的任务列表。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 7-69 进入目标工作空间管理页面

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

图 7-70 已处理

步骤5 在已处理任务列表中查看已处理任务详情。

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

表 7-35 已处理任务参数说明

参数名称	参数说明
任务名称	该条任务的名称。
业务类型	任务属于的类型。 ● 流程发布 ● 剧本发布 ● 剧本-节点审核
关联对象	对应的剧本/流程名称。
创建人	创建任务的用户。
备注	该条任务的备注信息。
审核人	该剧本/流程的审核人员。
审核意见	该条任务的审核意见。
描述	该条任务的描述信息。
创建时间	该剧本/流程的创建时间。
更新时间	该剧本/流程的最近一次更新时间。
到期时间	该条任务的到期时间。

----结束

8 资产管理

8.1 资产管理概述

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。		

8.2 设置资产订阅

操作场景

安全云脑只有在开启资产订阅设置的工作空间才能同步资产相关信息。订阅后，资产信息将在一分钟内同步展示。

本章节介绍如何订阅资产。

说明

仅支持订阅和同步云上资产。同时，不建议同一个区域的资产订阅至多个工作空间。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

图 8-2 资产管理

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

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

步骤7 单击页面右下角的“确认”。

订阅后，资产信息将在一分钟内同步展示。

----结束

8.3 查看资产信息

操作场景

在资产管理页面，可以查看资产的名称、类型、防护状态等信息。

前提条件

已购买安全云脑**标准版**或**专业版**，且在有效使用期内。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 8-3 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

图 8-4 资产管理

步骤5 在资产管理页面查看资产的详细信息。

- 如需查看指定类型资产信息，如主机资产，请选择“主机资产”页签进行查看。
- 当资产较多时，可以通过搜索功能，选择搜索类型并按“Enter”，即可快速查询指定资产。
- 在资产列表中下方可以查看资产总条数。其中，使用翻页查看时最多可查看10000条资产信息，如果需要查看超过10000条以外数据，请优化过滤条件筛选数据。
- 如果需要查看某个资产的更多详细信息，可以单击资产名称，进入资产详情页面进行查看。

- 在资产详情页面，可以查看资产的基本信息、环境信息和管理的资产等信息。
- 在资产详情页面，可以对资产的责任人、业务系统和部门信息进行编辑，还可以绑定或解绑资产。

表 8-2 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。		

----结束

相关操作

在资产管理页面可以对资产的部门、业务系统、责任人进行编辑。操作步骤如下：

1. 勾选需要编辑的资产，并单击资产列表左上角“批量编辑”。
2. 在弹出的资产编辑框中，编辑资产信息。
3. 单击“确认”。

8.4 导入/导出资产

操作场景

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。

前提条件

已购买安全云脑**标准版**或**专业版**，且在有效使用期内。

约束与限制

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

导入资产

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 8-5 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

图 8-6 资产管理

步骤5 在资产管理页面中，选择对应资产页签。例如，需要导入主机资产，则选择“主机资产”页签。

步骤6 在资产列表左上方，单击“导入”，弹出导入资产对话框。

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

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

步骤9 选择完成后，单击“确定”，完成导入。

----结束

导出资产

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 8-7 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

图 8-8 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。例如，需要导出主机资产，则选择“主机资产”页签。

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 8-3 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

8.5 编辑/删除资产

操作场景

在资产管理页面可以对资产的部门、业务系统、责任人进行编辑。另外，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。

本章节介绍如何编辑/删除资产。

前提条件

已购买安全云脑**标准版**或**专业版**，且在有效使用期内。

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 在页面左上角单击 ☰，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 8-9 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面。

图 8-10 资产管理

步骤5 编辑或删除资产。

表 8-4 编辑或删除资产

操作	执行步骤
编辑资产	1. 在资产管理页面中，勾选需要编辑的资产，并单击资产列表左上角“批量编辑”。 如果需要编辑某个类型的资产，可以选择对应资产页签，进入对应资产页面。例如，需要编辑主机资产，则选择“主机资产”页签。 2. 在弹出的资产编辑框中，对资产的部门、业务系统、责任人进行编辑。 3. 编辑完成后，单击“确认”。

操作	执行步骤
删除资产	1. 在资产管理页面中，选择对应资产页签，进入对应资产页面。例如，需要删除主机资产，则选择“主机资产”页签。 2. 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

9 风险预防

9.1 基线检查

9.1.1 基线检查概述

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

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

约束与限制

SecMaster**基础版**暂不支持使用基线检查功能。**标准版**暂不支持云服务基线查看详情功能。为及时了解云服务配置状态，以及确保云服务的配置的合理性，建议您**购买专业版**。

基线检查方式

- 自动执行基线检查

  SecMaster默认每隔3天检查一次，每次在00:00~06:00对您账号下当前region所有资产进行检查。

  同时，您还可以自定义自动检测周期及时间，详细操作请参见**新增自定义基线检查计划**。

- 手动执行基线检查

  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。另外，自动检查的检查项目也可以进行手动检查。

  手动检查详细操作请参见**执行手动检查**。

使用流程

表 9-1 使用流程

序号	操作项	说明
1	（可选）新增自定义基线检查计划	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：默认每隔3天检查一次，每次在00:00~06:00对您账号下当前区域的所有资产进行检查。 • 自定义基线检查计划：根据您的需求自定义检查规范和检查时间。
2	（可选）立即执行基线检查	基线检查功能支持定期自动检查和立即检查。 • 定期自动检查：根据系统默认基线检查计划或您自定义的基线检查计划，定时自动执行基线检查。 • 立即检查：如果您新增或修改了自定义的基线检查计划，您可以在基线检查页面选择该基线检查计划，立即执行基线检查，实时查看服务器中是否存在对应的基线风险。
3	查看基线检查结果	基线检查完后后，可以查看基线检查结果，解基线检查项影响的资产、基线项目详情等信息。
4	处理基线检查结果	基线检查完后后，可以根据修复建议对风险项目进行处理。

9.1.2 基线检查项目

安全云脑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。

如需查看每个检查项目的详情，如检查状态、风险等级、检查内容等信息，请在检查项目详情页面进行查看，具体操作请参见查看基线检查结果。

本章节将介绍SecMaster云服务基线检查支持的检查项目。

表 9-2 基线检查项目

检查规范	检查类别	包含的检查项数量
安全上云合规检查1.0	身份与访问管理	12
	检测	7
	基础设施防护	24
	数据防护	22
	事件响应	13

检查规范	检查类别		包含的检查项数量
护网检查	**安全套件覆盖**		8
	账号加固		5
	主机加固		4
	Sudo漏洞		1
	访问控制		1
	敏感信息排查		5
等保2.0三级要求	安全通用要求	**安全物理环境**	22
		安全通信网络	8
		安全区域边界	20
		安全计算环境	34
		安全管理中心	12
		安全管理制度	7
		安全管理机构	14
		安全管理人员	12
		安全建设管理	34
		安全运维管理	48
	云计算安全扩展要求	**安全物理环境**	1
		安全通信网络	5
		安全区域边界	8
		安全计算环境	19
		安全管理中心	4
		安全建设管理	8
		安全运维管理	1
	安全运维管理		1
	安全运维管理		1

安全上云合规检查—身份与访问管理

表 9-3 身份与访问管理风险项检查项目

检查项目	检查内容
IAM用户启用检查	启用统一身份认证（Identity and Access Management，IAM）服务后，系统默认用户组admin中的IAM用户，可以使用华为云所有服务。 检查所有IAM用户列表，是否已启用至少两个IAM用户，以及IAM用户所属的用户组是否都为admin用户组。
IAM用户开启登录保护检查	在IAM的安全设置中启用登录保护后，登录时还需要通过虚拟MFA或短信或邮件验证，再次确认登录者身份，进一步提高账号安全性，有效避免钓鱼式攻击或者用户密码意外泄漏，保护您安全使用云产品。 检查在IAM的安全设置中是否开启登录保护。
IAM用户开启操作保护检查	在IAM的安全设置中开启操作保护后，主账户及子用户在控制台进行敏感操作（如：删除弹性云服务器、解绑弹性IP等）时，将通过虚拟MFA、手机短信或邮件再次确认操作者身份，进一步提高账号安全性，有效保护您安全使用云产品。 检查IAM用户是否开启操作保护。
管理员账号AK/SK启用检查	访问密钥（AK/SK，Access Key ID/Secret Access Key）是账号的长期身份凭证。 由于管理员具有IAM用户管理权限，且具有大范围的操作权限。为了避免因AK/SK泄露带来的安全隐患，建议管理员账号不启用AK/SK身份凭证。 检查管理员账户是否启用访问密钥。
IAM用户密码配置检查	IAM用户的密码策略建议设置强密码策略。建议满足以下要求：包含以下字符中的3种：大写字母、小写字母、数字和特殊字符；密码最小长度为8；新密码不能与最近的历史密码相同（重复次数设置为3） 检查IAM用户的密码策略是否符合要求。
IAM登录验证策略（账号锁定策略）检查	拥有安全管理员权限（Security Administrator权限）的用户可以设置登录验证策略来提高用户信息和系统的安全性。 IAM允许用户设置账号锁定策略，即如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间，锁定时间结束后，才能重新登录。 建议设置为在60分钟内登录失败5次，用户被锁定。 检查账号锁定策略是否设置为在60分钟内登录失败5次，用户被锁定。

检查项目	检查内容
IAM登录验证策略（账号锁定时限）检查	拥有安全管理员权限（Security Administrator权限）的用户可以设置登录验证策略来提高用户信息和系统的安全性。 用户可设置账号锁定策略，即如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间，锁定时间结束后，才能重新登录。 IAM应允许用户设置账号锁定时间，且在此期间用户将无法输入密码。账号锁定时限建议设置为15分钟。 检查账号锁定时限是否设置为15分钟。
IAM密码策略（防止密码重复使用）检查	IAM允许用户设置密码策略。 启用防止密码重复使用规则后，新密码不能与最近使用的密码相同。 检查IAM密码策略是否启用密码重复使用规则，且重复次数小于五次。
会话超时策略检查	IAM允许用户设置会话到期时间。如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。 检查会话时限是否设置为15分钟。
账号停用策略检查	IAM用户可以通过使用用户名和密码登录华为云控制台。如果用户在90天或更长时间内未登录控制台，建议禁用该用户的控制台访问权限。 检查账号停用策略是否启用，且有效期设置为90天。
IAM用户密码强度检查	IAM用户的登录密码建议设置为安全程度强的密码。 IAM用户设置的登录密码分为弱、中、强三个级别。安全性高的密码可以使账号更安全，建议您定期更换密码以保护账号安全。 检查IAM用户的密码强度是否为最高级别。
CBH实例登录开启多因子认证检查	通过Web浏览器或SSH客户端登录CBH实例时应开启用户的多因子认证，进一步提高堡垒机账号安全性。多因子认证方式有：手机短信、手机令牌、USBKey、动态令牌。 检查CBH实例是否已开启多因子认证。

安全上云合规检查—检测

表 9-4 检测风险项检查项目

检查项目	检查内容
ELB健康状态检查	弹性负载均衡（Elastic Load Balance，ELB）定期向后端服务器发送请求健康检查，通过健康检查来判断后端服务器是否可用。 如果判断出后端服务器健康检查异常，ELB会将异常后端服务器的流量分发到正常后端服务器。 当异常后端服务器恢复正常运行后，ELB会自动恢复其承载业务流量能力。 检查所有ELB实例是否开启健康检查功能，以及检查后端服务器状态是否正常。
CTS启用检查	云审计服务（Cloud Trace Service，CTS）可以将当前账户下所有的操作记录在追踪器中，通过查询和审计操作记录，实现安全分析、资源变更、合规审计、问题定位等。 检查是否已经开通CTS，以及检查是否有一个追踪器的状态为正常。
OBS桶日志记录启用检查	对象存储服务（Object Storage Service，OBS）的桶日志记录，指用户开启一个桶的日志记录功能后，OBS会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶（即目标桶）中。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。 检查所有OBS桶，是否开启日志记录功能。
数据库安全审计启用检查（云上RDS场景）	数据库安全审计提供旁路模式审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警，对数据库的内部违规和不正当操作进行定位追责。 检查是否已启用数据库安全审计。
云监控服务启用检查	云监控（Cloud Eye）服务为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。 检查是否已启用云监控服务。
云监控服务中的主机监控检查	主机监控针对主机提供多层次指标监控，包括基础监控、操作系统监控和进程监控。 基础监控为用户提供免安装的基础指标监控服务；操作系监控和进程监控通过在主机中安装开源插件，为用户主机提供系统级、主动式、细颗粒度的监控服务。 检查主机监控中的弹性云服务器是否已安装监控插件。

检查项目	检查内容
云监控服务中站点监控检查	站点监控用于模拟真实用户对远端服务器的访问，从而探测远端服务器的可用性、连通性等问题。 检查是否配置站点监控。

安全上云合规检查—基础设施防护

表 9-5 基础设施防护风险项检查项目

检查项目	检查内容
安全组入方向规则控制检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。
高危端口、远程管理端口暴露检查	安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器提供访问策略。安全组创建后，可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云服务器出入方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。 安全组入方向规则中不应对外开放或未最小化开放高危端口、远程管理端口。 高危端口如下：20，21，135，137，138，139，445，389，593，1025 未最小化开放指的是：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 检查安全组入方向规则中是否存在对外开放或未最小化开放高危端口、远程管理端口。
绑定EIP的ECS配置密钥对登录检查	当存在ECS对外暴露EIP的情况下，为安全起见，弹性云服务器登录时应使用密钥方式进行身份验证。
日志指标过滤和告警事件（VPC更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 检查CTS中是否存在因VPC更改而产生的日志和告警事件。

检查项目	检查内容
日志指标过滤和告警事件（网络网关更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 检查CTS中是否存在因网络网关更改而产生的日志和告警事件。
日志指标过滤和告警事件（安全组更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 检查CTS中是否存在因安全组更改而产生的日志和告警事件。
日志指标过滤和告警事件（子网更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 检查CTS中是否存在因子网更改而产生的日志和告警事件。
日志指标过滤和告警事件（VPN更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 检查CTS中是否存在因VPN更改而产生的日志和告警事件。
ELB实例（共享型）启用访问控制检查	共享型负载均衡器用户可以通过添加白名单和黑名单的方式控制访问负载均衡监听器的IP。通过白名单能够设置允许特定IP访问，而其它IP不许访问。通过黑名单能够设置允许特定的IP不能访问，而其它IP允许访问。 检查弹性负载均衡（Elastic Load Balance，ELB）实例，是否开启访问控制策略。
网络ACL规则配置检查	网络ACL是对子网的访问控制策略系统，根据与子网关联的入站/出站规则，判断数据包是否被允许流入/流出关联子网。同一个VPC内的子网间设置网络ACL，可以增加额外的安全防护层，实现更精细、更复杂的安全访问控制。 检查是否配置网络ACL规则。

检查项目	检查内容
用于VPC对等连接路由表检查	对等连接是指两个VPC之间的网络连接，因此用于对等连接的路由表应满足最小访问权限。 本端路由的目的地址尽量限定在最小子网网段内，对端路由的目的地址尽量限定在最小子网网段内。 检查用于对等连接的路由表是否满足最小访问权限。
VPC规划检查	如果在当前区域下有多套业务部署，且希望不同业务之间进行网络隔离时，则可为每个业务在当前区域建立相应的VPC。 两个VPC之间可以采用对等连接进行互连。 VPC具有区域属性，默认情况下，不同区域的VPC之间内网不互通，同区域的不同VPC内网不互通，同一个VPC下的不同可用区之间内网互通。 检查VPC规范是否合理。
WAF启用（云模式/独享模式/ELB模式）检查	启用Web应用防火墙（Web Application Firewall，WAF）服务后，网站所有的公网流量都会先经过Web应用防火墙，恶意攻击流量在Web应用防火墙上被检测过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。 检查是否已启用WAF。
WAF回源配置检查（未配置ELB）	使用Web应用防火墙（Web Application Firewall，WAF）服务后，需配置源站服务器只允许来自WAF的访问请求访问源站，既可保障访问不受影响，又能防止源站IP暴露。 未使用弹性负载均衡（Elastic Load Balance，ELB）情况下，检查在ECS关联的安全组源地址中，是否添加WAF回源IP。
WAF防护策略配置（地理位置访问控制）检查	WAF的防护策略应配置地理位置访问控制，可针对指定国家、地区的来源IP自定义访问控制。配置后，可以进一步减小业务网站的攻击面（检测版和专业版暂不支持该功能）。
Web基础防护配置检查	Web基础防护支持“拦截”（发现攻击行为后立即阻断并记录）和“仅记录”（发现攻击行为后只记录不阻断攻击）模式，检测版仅支持“仅记录”模式。 WAF中所有待防护的域名应开启Web基础防护并设置为拦截模式，开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查是否已开启Web基础防护并设置为拦截模式。

检查项目	检查内容
VSS启用检查	漏洞扫描服务（Vulnerability Scan Service）是针对网站进行漏洞扫描的一种安全检测服务，可以帮助快速检测出网站存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。 检查是否已启用VSS服务。
Anti-DDoS流量清洗启用检查	DDoS原生基础防护（Anti-DDoS流量清洗）服务为华为云内公网IP资源，提供网络层和应用层的DDoS攻击防护，并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠。 检查是否已启用Anti-DDoS流量清洗服务。
DDoS高防启用检查	DDoS高防（Advanced Anti-DDoS，AAD）是企业重要业务连续性的有力保障。DDoS高防通过高防IP代理源站IP对外提供服务，将恶意攻击流量引流到高防IP清洗，确保重要业务不被攻击中断。 检查是否已启用DDoS高防。
云堡垒机启用检查	云堡垒机（Cloud Bastion Host，CBH）是华为云的一款4A统一安全管控平台，为企业提供集中的账号、授权、认证和审计管理服务。启用后，可实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计，不仅能保障系统运行安全，且满足相关合规性规范。 检查是否已启用云堡垒机服务。
主机安全防护启用检查	企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务。可以全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。 主机实例应安装HSS且开启防护，版本要求至少为企业版（旗舰版、网页防篡改版更优）。 检查主机是否开启主机安全防护。
HSS网页防篡改启用与防护目录配置检查	网页防篡改可实时监控网站目录，并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。 有网站或者关键系统防篡改需求，以及有应用安全防护需求的主机，应开启HSS中的网络防篡改防护并配置好防护目录。 检查主机是否开启网络防篡改防护且已配置好防护目录。
主机紧急修复漏洞检查	企业主机安全服务（Host Security Service，HSS）提供漏洞管理功能，检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞。 检查HSS中是否存在紧急修复漏洞。

检查项目	检查内容
CDN访问控制配置检查	当客户CDN需要对访问者身份进行识别和过滤，限制部分用户访问，提高CDN的安全性，应配置防盗链与IP黑名单。 检查CDN是否配置访问控制规则。

安全上云合规检查—数据防护

表 9-6 数据防护风险项检查项目

检查项目	检查内容
ELB证书有效性检查	弹性负载均衡（Elastic Load Balance，ELB）支持两种类型的证书，服务器证书和CA证书。配置HTTPS监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定CA证书。 检查所有ELB中的证书是否有效可用。如果SSL证书过期且未及时更新，用户访问网站时会显示“网站的安全证书已过期”的告警信息。
CDN证书有效性检查	通过配置加速域名的HTTPS证书，并将其部署在全网CDN节点，实现HTTPS安全加速。 检查CDN中证书是否均在有效期内，如果SSL证书过期且未及时更新，用户访问网站时会显示“网站的安全证书已过期”的告警信息。
SSL证书有效性检查	SSL证书管理（SSL Certificate Manager，SCM）是一个SSL（Secure Socket Layer）证书管理平台。SSL证书部署到服务器后，服务器端的访问将启用HTTPS协议。SSL证书超出有效期，将无法正常使用SSL证书。 检查所有SSL证书（检查已签发状态SSL证书，如果SSL证书未签发则默认为检查合格）状态是否在有效期内。
RDS数据库绑定EIP时的安全设置检查	当云数据库RDS（Relational Database Service，简称RDS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当RDS数据库配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。
DDS数据库绑定EIP时安全设置检查	当文档数据库服务（Document Database Service）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当DDS数据库配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。

检查项目	检查内容
DCS数据库绑定EIP时的安全设置检查	当分布式缓存服务（Distributed Cache Service，简称DCS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当DCS数据库配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。
云数据库GaussDB绑定EIP时的安全设置检查	当云数据库GaussDB配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当云数据库GaussDB配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。
RDS数据库绑定EIP检查	当云数据库RDS（Relational Database Service，简称RDS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当RDS数据库配置，是否开通公网连接方式。
DDS数据库绑定EIP检查	当文档数据库服务（Document Database Service）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当DDS数据库配置，是否开通公网连接方式。
DCS数据库绑定EIP检查	当分布式缓存服务（Distributed Cache Service，简称DCS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当DCS数据库配置，是否开通公网连接方式。
云数据库GaussDB绑定EIP检查	当云数据库GaussDB配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当云数据库GaussDB配置，是否开通公网连接方式。
RDS数据库实例安全组规则检查	检查关系型数据库（Relational Database Service，RDS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。当源地址为0.0.0.0/0或空时，代表未设置IP访问的限制，数据库将会有高安全风险。不安全规则示例：方向为入方向，协议为任一类别协议，源地址为0.0.0.0/0（所有地址），端口为1~65535或者数据库业务端口，如3306。
GaussDB数据库实例安全组规则检查	安全组入方向规则应满足最小化访问控制原则。 一般地，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0

检查项目	检查内容
OBS桶服务端加密检查	OBS服务端加密是在上传对象到桶时，将数据在服务端加密成密文后存储。再次下载加密对象时，存储的密文会先在服务端解密为明文，再反馈给用户。将数据加密后存储到OBS桶中，提高数据的安全性。 检查所有OBS桶是否开启服务端加密。
OBS桶的ACL权限检查	OBS桶ACL是基于账号或用户组的桶级访问控制，桶的拥有者可以通过桶ACL授予指定账号或用户组特定的访问权限。 匿名用户指未注册华为云的普通访客。如果OBS桶的ACL赋予了匿名用户桶的访问权限或ACL访问权限，表示所有人无需经过任何身份验证即可访问OBS桶。 检查所有OBS桶，是否给匿名用户赋予桶访问权限或者ACL访问权限。
MySQL数据库实例root用户远程登录控制检查	MySQL数据库实例的root应做好远程登录的控制，限制仅应用端、DAS管理网段等业务需要方可登录，防止root账号被暴力破解。
RDS数据库实例安全组入方向规则检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0 检查云数据库（Relational Database Service，RDS）实例所关联的安全组入方向规则是否按最小化访问控制。
DCS数据库实例安全组入方向规则检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0 检查分布式缓存服务（Distributed Cache Service，DCS）实例所关联的安全组入方向规则是否按最小化访问控制。
DDS数据库实例安全组入方向规则检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0 检查文档数据库服务（Document Database Service，DDS）实例所关联的安全组入方向规则是否按最小化访问控制。

检查项目	检查内容
RDS数据库实例安全组端口开放检查	检查云数据库（Relational Database Service，RDS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。 不安全规则示例：方向为入方向，端口为1~65535或者非数据库业务端口，如3306。 检查RDS实例是否开放非必要的端口。
DCS数据库实例安全组端口开放检查	检查分布式缓存服务（Distributed Cache Service，DCS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。 不安全规则示例：方向为入方向，端口为1~65535或者非数据库业务端口，如6379。 检查DCS实例是否开放非必要的端口。
DDS数据库实例安全组端口开放检查	检查文档数据库服务（Document Database Service，DDS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。 不安全规则示例：方向为入方向，端口为1~65535或者非数据库业务端口，如8635。 检查DDS实例是否开放非必要的端口。

安全上云合规检查—事件响应

表 9-7 事件响应风险项检查项目

检查项目	检查内容
云硬盘备份开启检查	云备份（Cloud Backup and Recovery）可以为云硬盘（Elastic Volume Service，EVS）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。 检查所有是否开启云硬盘备份。
OBS桶跨区域复制检查	OBS跨区域复制能够提供跨区域数据容灾的能力，通过创建跨区域复制规则，在同一个账号下，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中，满足用户数据复制到异地进行备份的需求。 检查所有OBS桶是否开启跨区域复制。
云审计服务关键操作通知启用检查	云审计服务在记录某些特定关键操作时，支持对这些关键操作通过消息通知服务实时向相关订阅者发送通知，该功能由云审计服务触发，消息通知服务（SMN）完成通知发送。

检查项目	检查内容
云日志服务LTS的日志转储（OBS/DIS）检查	主机和云服务的日志数据上报至云日志服务后，默认存储时间为7天。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至其他云服务中进行长期保存。 检查LTS是否已配置日志转储（OBS/DIS）。
ECS/BMS实例的云服务器备份检查	云备份（Cloud Backup and Recovery, CBR）为云内的弹性云服务器（Elastic Cloud Server, ECS）、云耀云服务器（Hyper Elastic Cloud Server，HECS）、裸金属服务器（Bare Metal Server, BMS）（下文统称为服务器）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。 检查ECS/BMS实例是否已开启云服务器备份。
RDS数据库实例备份检查	RDS数据库实例应开启自动备份功能，以保证数据可靠性。 检查RDS数据库实例是否已开启自动备份功能。
GaussDB数据库实例备份检查	GaussDB数据库实例应开启自动备份功能，以保证数据可靠性。 检查GaussDB数据库实例是否已开启自动备份功能。
WAF全量日志功能开启检查	启用WAF全量日志功能后，可以将攻击日志、访问日志记录到华为云的云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的WAF日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。 检查WAF是否已启用全量日志功能。
WAF防护事件告警通知开启检查	通过对攻击日志进行通知设置，WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户，以便在发生攻击时运维人员进行及时响应，告警频率、事件类型可以根据业务场景进行调整。 检查WAF防护事件是否已开启告警通知。
数据库安全审计日志备份检查	数据库安全审计支持将数据库的审计日志备份到OBS桶，实现高可用容灾，以便可以根据需要备份或恢复数据库审计日志。 检查数据库安全审计是否已配置日志备份。
数据库安全审计告警通知设置检查	通过设置告警通知，当数据库发生设置的告警事件时，您可以收到DBSS发送的告警通知，及时了解数据库的安全风险。 检查数据库安全审计是否设置告警通知。
云硬盘可用备份检查	云备份（Cloud Backup and Recovery）可以为云硬盘（Elastic Volume Service, EVS）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。 检查云硬盘中是否有可用备份，以便用于恢复。

检查项目	检查内容
RDS数据库实例备份检查	云数据库（Relational Database Service，RDS）支持数据库实例的备份和恢复，以保证数据可靠性。RDS数据库实例默认开启数据自动备份策略，备份周期默认每天备份数据一次。 检查所有RDS实例，是否开启自动备份功能。
DDS数据库开启自动备份	文档数据库服务（Document Database Service，DDS）支持数据库实例的备份和恢复，以保证数据可靠性。DDS数据库实例开启数据自动备份策略后，备份周期默认每天备份数据一次。 检查所有DDS实例是否开启自动备份功能。

护网检查—安全套件覆盖

表 9-8 安全套件覆盖风险项检查项目

检查项目	检查内容
主机防护状态检查	企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。 检查主机是否已开启防护。
主机Agent状态检查	企业主机安全服务（Host Security Service，HSS）是一个用于全面保障主机整体安全的服务，能帮助您高效管理主机的安全状态，并构建服务器安全体系，降低当前服务器面临的主要安全风险。 在主机中安装Agent后，您的主机才能收到HSS的保护。 检查主机Agent是否为在线状态。
主机安全检测状态检查	企业主机安全服务（Host Security Service，HSS）将实时检测主机中的风险和异常操作，在每日凌晨将对主机执行全面扫描。执行配置检测后，您可以根据检测结果中的相关信息，修复主机中含有风险的配置项或忽略可信任的配置项。 检查主机的检测结果是否存在异常。
WAF（云模式）基础防护配置检查	Web基础防护开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在云模式下是否已开启Web基础防护。

检查项目	检查内容
WAF（云模式）防护策略配置检查	Web基础防护支持“拦截”（发现攻击行为后立即阻断并记录）和“仅记录”（发现攻击行为后只记录不阻断攻击）模式，检测版仅支持“仅记录”模式。 WAF中所有待防护的域名应开启Web基础防护并设置为拦截模式，开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在云模式下是否已开启Web基础防护并设置为拦截模式。
WAF（独享模式）基础防护配置检查	Web基础防护开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在独享模式下是否已开启Web基础防护。
WAF（独享模式）防护策略配置检查	Web基础防护支持“拦截”（发现攻击行为后立即阻断并记录）和“仅记录”（发现攻击行为后只记录不阻断攻击）模式，检测版仅支持“仅记录”模式。 WAF中所有待防护的域名应开启Web基础防护并设置为拦截模式，开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在独享模式下是否已开启Web基础防护并设置为拦截模式。
主机Agent版本检查	在主机中安装Agent后，您的主机将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。 企业主机安全服务有基础版、企业版、旗舰版和网页防篡改版四个版本。 基础版一般只用于测试、个人用户防护主机账户安全。建议您选择企业版及以上版本。 检查所有主机Agent是否为企业版及以上版本。

护网检查—账号加固

表 9-9 账号加固风险项检查项目

检查项目	检查内容
管理员账号AK/SK启用检查	访问密钥（AK/SK，Access Key ID/Secret Access Key）是账号的长期身份凭证。 由于管理员具有IAM用户管理权限，且具有大范围的操作权限。为了避免因AK/SK泄露带来的安全隐患，建议管理员账号不启用AK/SK身份凭证。 检查管理员账户是否启用访问密钥。
主机弱密码检查	HSS提供基线检查功能，主动检测主机中口令复杂度策略，给出修改建议，帮助用户提升口令安全性检测账口令是否属于常用的弱口令，针对弱口令提示用户修改，防止账户口令被轻易猜解。 检查主机是否存在弱口令。
委托账号检查	通过创建委托，可以将资源共享给其他账号，或委托更专业的人或团队来代为管理资源。被委托方使用自己的账号登录后，切换到委托方账号，即可管理委托方委托的资源，避免委托方共享自己的安全凭证（密码/密钥）给他人，确保账号安全。 在云服务环境中，如果创建委托给个人账号，可能会导致不可信，因此不建议委托给个人账号。 检查是否存在个人委托账号。
全局服务中的委托权限配置检查	检查全局服务中的委托权限是否存在Security Administrator，Tenant Administrator。
项目服务中的委托权限配置检查	检查项目服务中的委托权限是否存在Security Administrator，Tenant Administrator。

护网检查—主机加固

表 9-10 主机加固风险项检查项目

检查项目	检查内容
主机高危端口暴露检查	HSS提供资产管理功能，主动检测主机中的开放端口，及时发现主机中含有风险的各项资产。 如果检测到开放了危险端口或者开放了不必要的端口，需要排查这些端口是否是正常业务使用，如果不是正常业务端口，建议关闭端口。对于危险端口建议进一步检查程序文件，如果存在风险建议删除或者隔离源文件。 检查所有主机是否在对外开放或未最小化开放的高危端口。

检查项目	检查内容
CCE集群Kubernetes版本检查	云容器引擎（Cloud Container Engine，简称CCE）提供高度可扩展的、高性能的企业级Kubernetes集群，支持运行Docker容器。借助云容器引擎，您可以在华为云上轻松部署、管理和扩展容器化应用程序。 当CCE集群Kubernetes版本低于1.15，有安全漏洞风险，建议您进行升级。 检查CCE集群Kubernetes版本是否在1.15以下。
VPC配置（对等连接）检查	对等连接是指两个VPC之间的网络连接。您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。您可以在自己的VPC之间创建对等连接，也可以在自己的VPC与同一区域内其他的VPC之间创建对等连接。 检查VPC是否已经创建对等连接，如果已创建，则检查是否开放或未最小化高危端口。
VPC配置（VPN网关）检查	VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。 检查VPC是否已经创建了VPN网关。

护网检查—Sudo 漏洞

表 9-11 Sudo 漏洞风险项检查项目

检查项目	检查内容
检查主机是否存在Sudo漏洞	HSS提供漏洞管理功能，检测Linux软件漏洞，通过与漏洞库进行比对，检测出系统和官方软件（非绿色版、非自行编译安装版；例如：SSH、OpenSSL、Apache、MySQL等）存在的漏洞，帮助用户识别出存在的风险。 检查所有主机是否存在Sudo漏洞。

护网检查—访问控制

表 9-12 访问控制风险项检查项目

检查项目	检查内容
安全组入方向规则控制检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。 IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。 IPv6：源地址为::/0。

护网检查—敏感信息排查

表 9-13 敏感信息排查风险项检查项目

检查项目	检查内容
OBS桶的ACL权限检查	OBS桶ACL是基于账号或用户组的桶级访问控制，桶的拥有者可以通过桶ACL授予指定账号或用户组特定的访问权限。 匿名用户指未注册华为云的普通访客。如果OBS桶的ACL赋予了匿名用户桶的访问权限或ACL访问权限，表示所有人无需经过任何身份验证即可访问OBS桶。 检查所有OBS桶，是否给匿名用户赋予桶访问权限或者ACL访问权限。
OBS桶日志记录启用检查	对象存储服务（Object Storage Service，OBS）的桶日志记录，指用户开启一个桶的日志记录功能后，OBS会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶（即目标桶）中。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。 检查所有OBS桶，是否开启日志记录功能。
数据库中敏感信息检查	数据安全中心服务（Data Security Center，DSC）根据敏感数据发现策略来识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。 检查数据库中是否存在敏感信息。
OBS中敏感信息检查	数据安全中心服务（Data Security Center，DSC）根据敏感数据发现策略来识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。 检查OBS中是否存在敏感信息。

检查项目	检查内容
ES中敏感信息检查	数据安全中心服务（Data Security Center，DSC）根据敏感数据发现策略来识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。 检查ES中是否存在敏感信息。

等保 2.0 三级要求—安全物理环境

表 9-14 安全物理环境风险项检查项目

检查子项目	检查项目
物理位置选择	机房场地应选择在具有防震、防风和防雨等能力的建筑内。
	机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
防盗窃和防破坏	应将设备或主要部件进行固定，并设置明显的不易除去的标识。
	应将通信线缆铺设在隐蔽安全处。
	应设置机房防盗报警系统或设置有专人值守的视频监控系统。
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
防火	机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。
	机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
	应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
防水和防潮	应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
	应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。

检查子项目	检查项目
	应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
电力供应	应在机房供电线路上配置稳压器和过电压防护设备。
	应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
	应设置冗余或并行的电力电缆线路为计算机系统供电。
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
	应对关键设备实施电磁屏蔽。

等保 2.0 三级要求—安全通信网络

表 9-15 安全通信网络风险项检查项目

检查子项目	检查项目
网络架构	应保证网络设备的业务处理能力满足业务高峰期需要。
	应保证网络各个部分的带宽满足业务高峰期需要。
	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
	应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
	应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
通信传输	应采用密码技术保证通信过程中数据的完整性。
	应采用密码技术保证通信过程中数据的保密性。
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

等保 2.0 三级要求—安全区域边界

表 9-16 安全区域边界风险项检查项目

检查子项目	检查项目
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
	应能够对非授权设备私自联到内部网络的行为进行限制或检查。
	应能够对内部用户非授权联到外部网络的行为进行限制或检查。
	应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
	应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
	应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。
	应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
	应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
	当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
	应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

检查子项目	检查项目
	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

等保 2.0 三级要求—安全计算环境

表 9-17 安全计算环境风险项检查项目

检查子项目	检查项目
身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。
	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。
	当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。
	应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
访问控制	应对登录的用户分配账户和权限。
	应重命名或删除默认账户，修改默认账户的默认口令。
	应及时删除或停用多余的、过期的账户，避免共享账户的存在。
	应授予管理用户所需的最小权限，实现管理用户的权限分离。
	应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。
	访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
	应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。
安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

检查子项目	检查项目
	审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。
	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	应对审计进程进行保护，防止未经授权的中断。
入侵防范	应遵循最小安装的原则，仅安装需要的组件和应用程序。
	应关闭不需要的系统服务、默认共享和高危端口。
	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。
	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。
	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
恶意代码和垃圾邮件防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。
数据完整性	应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
数据保密性	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
数据备份恢复	应提供重要数据的本地数据备份与恢复功能。
	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。
	应提供重要数据处理系统的热冗余，保证系统的高可用性。

检查子项目	检查项目
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
	应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
个人信息保护	应仅采集和保存业务必需的用户个人信息。
	应禁止未授权访问和非法使用用户个人信息。

等保 2.0 三级要求—安全管理中心

表 9-18 安全管理中心风险项检查项目

检查子项目	检查项目
系统管理	应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。
	应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
审计管理	应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。
	应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理	应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。
	应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
集中管控	应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。
	应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。
	应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。
	应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。
	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

检查子项目	检查项目
	应能对网络中发生的各类安全事件进行识别、报警和分析。

等保 2.0 三级要求—安全管理制度

表 9-19 安全管理制度风险项检查项目

检查子项目	检查项目
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
管理制度	应对安全管理活动中的各类管理内容建立安全管理制度。
	应对管理人员或操作人员执行的日常管理操作建立操作规程。
	应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
制定和发布	应指定或授权专门的部门或人员负责安全管理制度的制定。
	安全管理制度应通过正式、有效的方式发布，并进行版本控制。
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

等保 2.0 三级要求—安全管理机构

表 9-20 安全管理机构风险项检查项目

检查子项目	检查项目
岗位设置	应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。
	应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
	应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
	应配备专职安全管理员，不可兼任。

检查子项目	检查项目
授权和审批	应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。
	应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。
	应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
沟通和合作	应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。
	应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
	应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
	应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
	应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

等保 2.0 三级要求—安全管理人员

表 9-21 安全管理人员风险项检查项目

检查子项目	检查项目
人员录用	应指定或授权专门的部门或人员负责人员录用。
	应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。
	应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
	应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

检查子项目	检查项目
	应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。
	应定期对不同岗位的人员进行技能考核。
外部人员访问管理	应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
	应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
	外部人员离场后应及时清除其所有的访问权限。
	获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

等保 2.0 三级要求—安全建设管理

表 9-22 安全建设管理风险项检查项目

检查子项目	检查项目
定级和备案	应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。
	应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。
	应保证定级结果经过相关部门的批准。
	应将备案材料报主管部门和相应公安机关备案。
安全方案设计	应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。
	应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。
	应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
产品采购和使用	应确保网络安全产品采购和使用符合国家的有关规定。
	应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
	应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
自行软件开发	应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制。

检查子项目	检查项目
	应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。
	应制定代码编写安全规范，要求开发人员参照规范编写代码。
	应具备软件设计的相关文档和使用指南，并对文档使用进行控制。
	应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
	应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
	应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
外包软件开发	应在软件交付前检测其中可能存在的恶意代码。
	应保证开发单位提供软件设计文档和使用指南。
	应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
工程实施	应指定或授权专门的部门或人员负责工程实施过程的管理。
	应制定安全工程实施方案控制工程实施过程。
	应通过第三方工程监理控制项目的实施过程。
测试验收	应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告。
	应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
系统交付	应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。
	应对负责运行维护的技术人员进行相应的技能培训。
	应提供建设过程文档和运行维护文档。
等级测评	应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。
	应在发生重大变更或级别发生变化时进行等级测评。
	应确保测评机构的选择符合国家有关规定。
服务供应商选择	应确保服务供应商的选择符合国家的有关规定。
	应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

检查子项目	检查项目
	应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

等保 2.0 三级要求—安全运维管理

表 9-23 安全运维管理风险项检查项目

检查子项目	检查项目
环境管理	应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。
	应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定。
	应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
	应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。
	应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
介质管理	应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。
	应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
设备维护管理	应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。
	应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
	信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。
	含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

检查子项目	检查项目
	应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
网络和系统安全管理	应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。
	应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
	应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。
	应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
	应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
	应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。
	应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。
	应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。
	应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。
	应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
恶意代码防范管理	应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。
	应定期验证防范恶意代码攻击的技术措施的有效性。
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
	应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
密码管理	应遵循密码相关国家标准和行业标准。
	应使用国家密码管理主管部门认证核准的密码技术和产品。
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

检查子项目	检查项目
	应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。
	应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
备份与恢复管理	应识别需要定期备份的重要业务信息、系统数据及软件系统等。
	应规定备份信息的备份方式、备份频度、存储介质、保存期等。
	应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
安全事件处置	应及时向安全管理部门报告所发现的安全弱点和可疑事件。
	应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等。
	应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
	对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
应急预案管理	应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。
	应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。
	应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
	应定期对原有的应急预案重新评估，修订完善。
外包运维管理	应确保外包运维服务商的选择符合国家的有关规定。
	应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。
	应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明。
	应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。

等保 2.0 三级要求—安全物理环境

表 9-24 安全物理环境风险项检查项目

检查子项目	检查项目
基础设施位置	应保证云计算基础设施位于中国境内。

等保 2.0 三级要求—安全通信网络

表 9-25 安全通信网络风险项检查项目

检查子项目	检查项目
网络架构	应保证云计算平台不承载高于其安全保护等级的业务应用系统。
	应实现不同云服务客户虚拟网络之间的隔离。
	应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
	应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。
	应提供开放接口或开放安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

等保 2.0 三级要求—安全区域边界

表 9-26 安全区域边界风险项检查项目

检查子项目	检查项目
访问控制	应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
	应在不同等级的网络区域边界部署访问控制机制，设备访问控制规则
入侵防范	应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
	应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
	应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
	应在检测到网络攻击行为、异常流量情况时进行告警。

检查子项目	检查项目
安全审计	应对云服务提供商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
	应保证云服务提供商对云服务客户系统和数据的操作可被云服务客户审计。

等保 2.0 三级要求—安全计算环境

表 9-27 安全计算环境风险项检查项目

检查子项目	检查项目
身份鉴别	当远程管理云计算平台的设备时，管理终端和云计算平台之间应建立双向身份验证机制。
访问控制	应保证当虚拟机迁移时，访问控制策略随其迁移。
	应允许云服务客户设置不同虚拟机之间的访问控制策略。
入侵防范	应能检测虚拟机之间的资源隔离失效，并进行告警。
	应能检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。
	应能检测恶意代码感染及在虚拟机间蔓延情况，并进行告警。
镜像和快照保护	应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
	应提供虚拟机镜像、快照完整性检验功能，防止虚拟机镜像被恶意篡改。
	应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
数据完整性和保密性	应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
	应确保只有在云服务客户授权下，云服务提供商或第三方才具有云服务客户数据的管理权限。
	应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
	应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。
数据备份恢复	云服务客户应在本地保存其业务数据的备份。
	应提供查询云服务客户数据及备份存储位置的能力。

检查子项目	检查项目
	云服务提供商的云存储服务应保证云服务客户数据存在多个可用的副本，各副本之间的内容应保持一致。
	应为云服务客户将业务系统及数据迁移到其体云计算平台和本地系统提供技术手段，并协助完成迁移过程。
剩余信息保护	应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
	云服务客户删除业务应用数据时，云计算平台将云存储中所有副本删除。

等保 2.0 三级要求—安全管理中心

表 9-28 安全管理中心风险项检查项目

检查子项目	检查项目
集中管控	应能对物理资源和虚拟资源按照策略做统一管理调度与分配。
	应保证云计算平台管理流量与云服务客户业务流量分离。
	应根据云服务提供商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。
	应根据云服务提供商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

等保 2.0 三级要求—安全建设管理

表 9-29 安全建设管理风险项检查项目

检查子项目	检查项目
云服务提供商选择	应选择安全合规的云服务提供商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
	应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
	应在服务水平协议规定云服务提供商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
	应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

检查子项目	检查项目
	应与选定的云服务提供商签署保密协议，要求其不得泄漏云服务客户数据。
供应链管理	应确保供应商的选择符合国家有关规定。
	应将供应链安全事件信息或安全威胁信息及时传达到云服务客户。
	应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

等保 2.0 三级要求—安全运维管理

表 9-30 安全运维管理风险项检查项目

检查子项目	检查项目
云计算环境管理	云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

等保 2.0 三级要求—安全运维管理

表 9-31 安全运维管理风险项检查项目

检查子项目	检查项目
配置管理	应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

等保 2.0 三级要求—安全运维管理

表 9-32 安全运维管理风险项检查项目

检查子项目	检查项目
感知节点管理	应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。

9.1.3 新增自定义基线检查计划

操作场景

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

本文档将介绍如何新增自定义基线检查计划。

约束与限制

- 同一个检查规范只能属于一个检查计划。
- 仅**标准版**、**专业版**支持使用该功能。

操作步骤

步骤1 登录管理控制台。

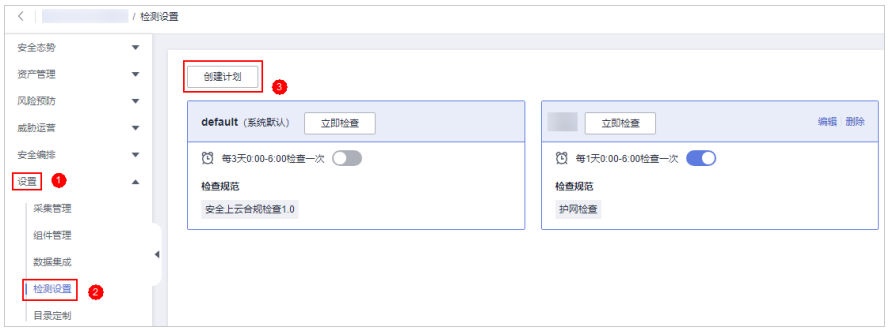
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-1 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面后，单击“创建计划”，系统右侧弹出新建检查计划页面。

图 9-2 创建检查计划



步骤5 配置检查计划。

1. 填写基本信息，具体参数配置如**表9-33**所示。

表 9-33 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。更多关于基线检查项目详细描述请参见**基线检查项目**。

步骤6 单击“确定”。

检查计划创建完成后，安全云脑会在指定的时间执行云服务基线扫描，扫描结果可以在“风险预防 > 基线检查”中查看。

----结束

相关操作

基线检查计划创建后，您可以查看检查计划、对检查计划进行编辑或删除。

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

  仅支持修改用户自定义创建的检查计划。
  a. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。
  b. 在目标计划所在框的右上角单击“编辑”，系统右侧弹出编辑检查计划页面。
  c. 编辑需要修改的计划参数后，单击“确定”。
- 删除检查计划

  仅支持删除用户自定义创建的检查计划。
  a. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。
  b. 在目标计划所在框的右上角单击“删除”。
  c. 在弹出的对话框中，单击“确认”。

9.1.4 立即执行基线检查

操作场景

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

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

本章节介绍如何**立即**执行基线检查。

约束与限制

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

立即检查所有检查规范

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

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

图 9-4 立即检查

步骤5 在弹出的确认框中，单击“确认”。

刷新页面，查看“最近检查时间”，即可确认是否为最新的扫描结果。

----结束

立即执行某个检查计划

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

步骤1 登录管理控制台。

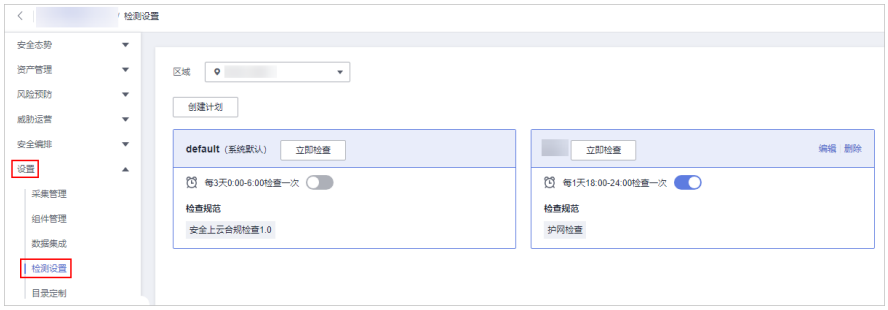
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

图 9-6 进入检测设置页面



步骤5 在待执行立即手动检查的检查计划所在栏的上方单击“立即检查”。

系统将立即执行已选择的基线检查计划。

----结束

9.1.5 执行手动检查

操作场景

基线检查的“等保2.0三级要求”中所有的检查项目、“安全上云合规检查1.0”和“护网检查”中的一些检查项目为手动检查项，需要您在线下执行检查后，再在控制台上反馈检查结果，以便计算检查项合格率。

本章节介绍手动检查项目执行检查的操作。

前提条件

- 已购买安全云脑**专业版**，且在有效使用期内。
- 已在线下完成检查。

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 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入基线检查页面。

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”。

图 9-9 反馈结果入口

步骤6 在弹出提示框中，选择反馈结果，并单击“确定”。

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

9.1.6 查看基线检查结果

操作场景

安全云脑支持在“基线检查”页签中查看所有检查结果，同时，还可以在“检查结果”页签中，查看已关联资产的自动检查项的检查结果。

- **在基线检查页签中查看检查结果**
- **在检查结果页签中查看检查结果**

本章节介绍如何查看基线检查结果。

前提条件

- 已购买安全云脑**专业版**，且在有效使用期内。
- 已进行云服务基线扫描。

在“基线检查”页签中查看检查结果

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。

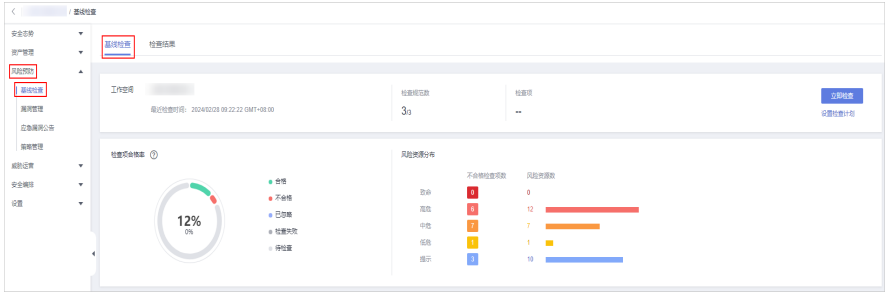
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入基线检查页面。

图 9-11 进入基线检查页面



步骤5 在“基线检查”页面中，查看基线检查结果，参数说明如**表9-34**所示。

图 9-12 查看基线检查结果

表 9-34 查看基线检查结果

参数名称	参数说明
工作空间	当前所属的工作空间名称。 工作空间名称下方显示最近一次基线检查的具体时间点。
检查规范	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、已忽略、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。
检查规范	按照检查规范维度展示基线检查结果。 • 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。 • 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。 **说明** SecMaster**基础版**暂不支持云服务基线查看详情功能。如需查看“风险资源列表”，“加固建议”等详情信息，建议您**购买专业版**。

参数名称	参数说明
检查资源	按照检查资源维度展示基线检查结果。 • 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。 • 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。 **说明** SecMaster**基础版**和**标准版**暂不支持云服务基线查看详情功能。如需查看“风险资源列表”，“修复方式”等详情信息，建议您**购买专业版**。
检查结果	按照检查结果维度展示基线检查情况。 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。 **说明** SecMaster**基础版**和**标准版**暂不支持查看检查结果功能。为及时了解云服务配置状态，以及确保云服务的配置的合理性，建议您**购买专业版**。

----结束

在“检查结果”页签中查看检查结果

安全云脑支持单独查看已关联资产的自动检查项的检查结果。

步骤1 登录管理控制台。

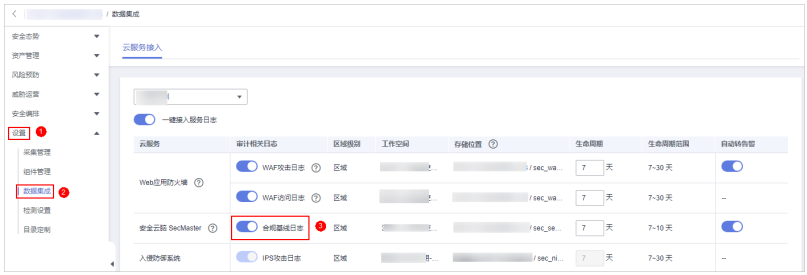
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-13 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 数据集成”，进入数据集成页面后，在**安全云脑**所在行“审计相关日志”列，开启合规基线日志设置。

图 9-14 合规基线日志



设置完成后，如果需尽快查看检查结果，可以在基线检查页面，执行立即检查。执行完成后，约10分钟后将可以在检查结果页面进行查看。立即检查相关操作请参见**立即执行基线检查**。

如果未执行立即检查，系统将按照已设置的检查计划，在指定时间内执行检查。检查完成后，将可以在检查结果页面中进行查看。

步骤5 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，选择“检查结果”页签，进入检测结果页面。

图 9-15 进入检查结果页面

步骤6 在“检查结果”页面中，查看已关联资产的自动检查项的检查结果，参数说明如**表 9-35**所示。

图 9-16 查看检查结果

表 9-35 查看检查结果

参数名称	参数说明
检查合格率	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、检查失败几种。

参数名称	参数说明
风险等级	最近一次支持基线检查的检查结果中，不同风险等级的不合格检查项目数据和对应的风险资源的数量。 风险等级分为：致命、高危、中危、低危、提示几个级别。
安全包遵从状态	最近一次执行基线检查后，各个安全遵从包中合格、不合格以及检查失败数据和不合格检查项目所占比例。
策略扫描情况	对各个云服务的资产扫描的后，合格、不合格以及检查失败数据信息。
安全遵从包及检查结果列表	展示所有遵从包以及检查结果列表。 • 如果需要查看某个检查规范的检查结果，可以在左侧选择需要查看的检查规范，右侧列表中将会展示该检查规范中的检查项目的检查结果详情。 • 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。 **说明** SecMaster**基础版**暂不支持云服务基线查看详情功能。如需查看风险资源列表、加固建议等详情信息，建议您**购买专业版**。

----结束

9.1.7 处理基线检查结果

操作场景

本章节介绍如何处理检查结果，请根据您的需要进行选择：

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

约束与限制

导入检查结果数据时，有以下限制条件：

- 支持导入.xlsx格式的文件。
- 一次仅支持导入一个文件，文件大小不超过500KB，且单次导入数据条不超过500条。
- 重复数据信息系统将进行去重处理，不会重复导入。

前提条件

- 已购买安全云脑**专业版**，且在有效使用期内。
- 已扫描云服务基线。

修复风险项

步骤1 登录管理控制台。

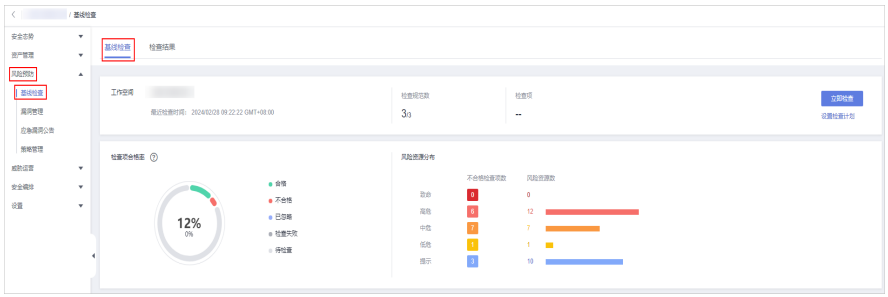
步骤2 在页面左上角单击 ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入基线检查页面。

图 9-18 进入基线检查页面



步骤5 在“检查规范”页签中，查看子检查项的风险状态。如果检查状态显示为不合格，则单击目标子检查项所在行的“操作”列的“查看详情”，进入检查项目详情页面。

在“检查状态”列可以查看子检查项风险状态。

- 检查状态图标呈绿色，则表示配置合格，不存在风险配置；
- 检查状态图标呈红色，则表示配置不合格，资产存在一定风险。

步骤6 查看风险详细信息，并根据“检查结果”和“加固建议”，修复风险点。

表 9-36 子检查项信息说明

参数名称	参数说明
检查状态	呈现当前检查项的检查状态。 ● 合格，提示当前子检查项配置合理，全部合格。 ● 不合格，提示当前子检查项配置可能不合理，并列表呈现检查结果。
最近检查	最近一次执行当前检查项的时间。
检查方式	当前检查项的检查方式。
风险等级	当前检查项出现问题所属的级别。
影响	当前检查项如果有问题将会带来的安全影响。
规范与分类	当前检查项所属的规范以及分类。
描述	当前检查项的具体检查内容。
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7 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。

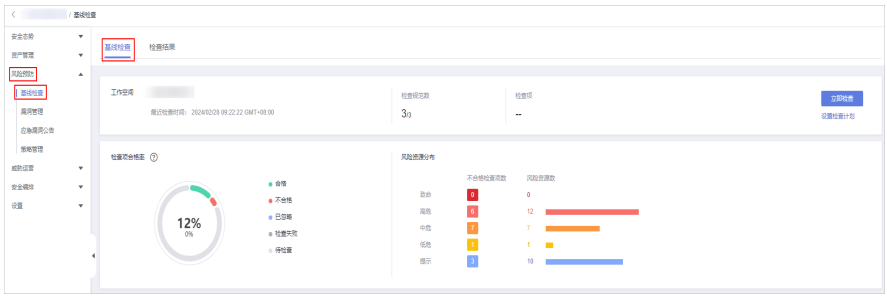
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-19 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入基线检查页面。

图 9-20 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”。

图 9-21 反馈结果入口

步骤6 在弹出提示框中，选择反馈结果，并单击“确定”。

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

忽略检查项

如果您对某个检查项有其他检查要求（例如，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。

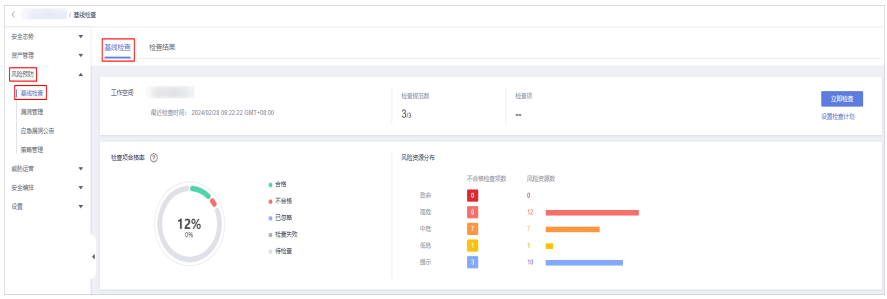
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-22 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，默认进入基线检查页面。

图 9-23 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”。

图 9-24 忽略检查项操作示例

步骤6 在弹出的确认框中，单击“确定”。

说明

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

----结束

导入/导出检查结果

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-25 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“检查结果”页签，进入检测结果页面。

图 9-26 进入检查结果页面

步骤5 导入/导出检查结果。

- 导入：

  说明

  - 支持导入.xlsx格式的文件。
  - 一次仅支持导入一个文件，文件大小不超过500KB，且单次导入数据条不超过500条。
  - 重复数据信息系统将进行去重处理，不会重复导入。

  a. 在下方检查结果列表左上角，单击的“导入”。
  b. 在弹出的对话框中单击“下载模板”，根据模板填写检查项目信息。
  c. 填写完成后，在弹出的对话框中单击“添加文件”，上传已填写的信息表格。
  d. 上传完成后，单击“导入”。

- 导出：

  a. 在下方检查结果列表中勾选需要导出的基线检查项目，并单击检查结果列表左上角的“导出”。
  b. 在弹出的对话框中，选择导出格式并自定义勾选需要导出的列。
  c. 单击“确定”。

----结束

9.2 漏洞管理

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。

HSS的漏洞扫描原理以及支持扫描的漏洞类型请参见**HSS漏洞管理概述**。

主机漏洞

安全云脑支持实时呈现主机漏洞扫描检测信息，支持查看漏洞详情，并提供相应漏洞修复建议。

主机漏洞共支持以下漏洞项的检测：

表 9-37 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。

集成后，安全云脑中漏洞的等级和HSS中修复优先级的说明如下：

- HSS：显示漏洞的修复优先级，它是由漏洞最高CVSS分值、漏洞发布时间和漏洞影响的资产重要性进行加权计算得出，反映了漏洞修复的紧急程度。

  漏洞修复优先级主要分为紧急、高、中、低四个等级，您可以参考修复优先级优先修复对您的服务器影响较大的漏洞。
- SecMaster：显示漏洞的等级，等级是根据漏洞最高CVSS分值得出的，反应漏洞的严重程度。

  漏洞等级主要分为高危、中危、低危、提示四个等级，您可以根据漏洞的严重程度（由高到低）进行修复。

9.2.2 查看漏洞详情

操作场景

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

前提条件

- 已购买安全云脑专业版，且在有效使用期内。
- 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。

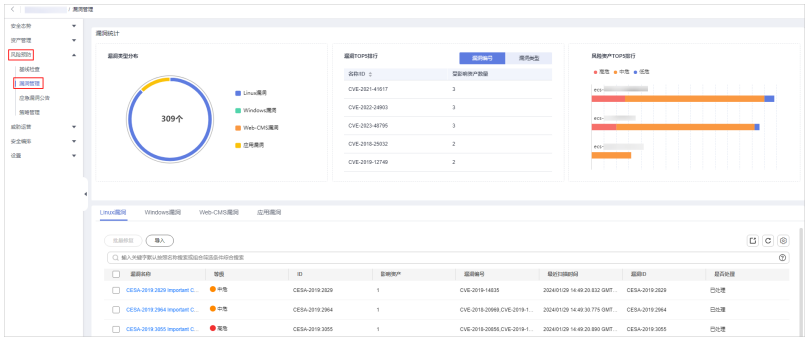
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-27 进入目标工作空间管理页面

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 9-28 进入漏洞管理页面



步骤5 在漏洞管理页面，查看漏洞信息。

表 9-38 查看漏洞信息

参数名称	参数说明
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	• TOP5是根据受漏洞影响的资产数量的多少来进行排序，影响资产越多排序越靠前。 • “漏洞编号”页签中，显示TOP5的漏洞的编号及受影响资产数量。 • “漏洞类型”页签中，显示TOP5的漏洞的名称、漏洞危险等级及受影响资产。
风险资产TOP5排行	呈现TOP5的风险资产。

参数名称	参数说明
漏洞列表	• 在下方漏洞列表中，选择“Linux漏洞”、“Windows漏洞”、“Web-CMS漏洞”、“应用漏洞”任意一个页签，进入对应漏洞列表管理页面，漏洞列表参数信息说明请参见表9-39。 • 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。 • 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。 • 在漏洞列表中下方可以查看漏洞总条数。其中，使用翻页查看时最多可查看10000条漏洞信息，如果需要查看超过10000条以外数据，请优化过滤条件筛选数据。

表 9-39 漏洞参数说明

参数名称	参数说明
漏洞名称	扫描出的漏洞名称。 单击漏洞名称，可查看该漏洞的简介、相关漏洞库信息。
等级	漏洞的危险程度。
ID	漏洞的ID信息。
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。
是否处理	该漏洞是否已处理。

----结束

9.2.3 修复漏洞

操作场景

当扫描到服务器存在漏洞时，您需要及时根据漏洞的危害程度结合实际业务情况处理漏洞，避免漏洞被入侵者利用入侵您的服务器。

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 9-40 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	

⚠ 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，建议您通过云备份（CBR）为ECS创建备份，详细操作请参见**创建云服务器备份**。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。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，可以使用华为云提供的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，确认主机中已配置华为云提供的对应操作系统的镜像源，详细的配置操作请参见**配置镜像源**。

约束与限制

- HSS各版本支持的漏洞处理操作请参见**支持扫描和修复的漏洞类型**。
- CentOS 6和CentOS 8官方已停止维护，HSS使用Redhat的补丁公告替代扫描，因此这两个操作系统的漏洞无法修复，建议您切换其他操作系统。
- Ubuntu 18.04及以下版本目前已不支持免费补丁更新，需要购买配置Ubuntu Pro后才能安装升级包，未配置Ubuntu Pro会导致漏洞修复失败。
- CCE、MRS、BMS的主机不能修复内核漏洞，贸然修复可能导致功能不可用。
- CCE主机的内核漏洞不支持自动修复，主机安全服务在执行批量自动修复漏洞任务时会自动过滤不修复这类漏洞。
- 处理漏洞时需保证目标服务器的“服务器状态”为“运行中”、“Agent状态”为“在线”、“防护状态”为“防护中”。

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。

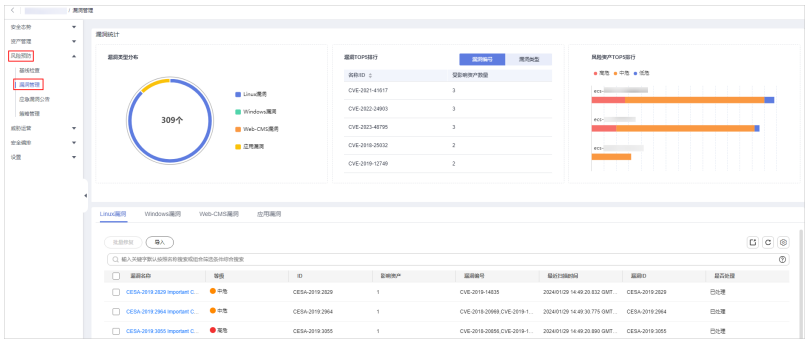
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-29 进入目标工作空间管理页面

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 9-30 进入漏洞管理页面



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

步骤6 在漏洞列表中，单击目标漏洞名称，右侧弹出漏洞信息页面。

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

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

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

对于Web-CMS漏洞、应用漏洞，不支持一键自动修复，您可以参考漏洞详情页面的修复建议，登录服务器手动修复。

- **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9-41**。

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。
- 如果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 9-41 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，详细操作请参见**通过云服务器创建整机镜像**。
    ii. 使用该镜像创建新的ECS主机，详细操作请参见**通过镜像创建云服务器**。
    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，详细操作请参见**创建云服务器备份**。
    ii. 在当前主机上直接进行漏洞修复。
    iii. 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态，详细操作请参见**使用备份恢复服务器**。

  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。新创建的ECS主机建议采用按需计费的方式创建，待业务切换完成后可以根据需要转换为包周期计费模式。如果漏洞修复不成功可以随时释放以节省开销。
  - 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 9-42 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* • 在HSS中进行**手动执行漏洞检测**，查看漏洞修复结果。
自动验证	如果您未进行手动验证，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。

相关操作

如果您评估某些漏洞对您的业务不会产生影响，并且不想在漏洞列表中看到该漏洞，您可以将该漏洞加入白名单，加入白名单后，针对漏洞列表已经展示的漏洞信息会处理为忽略，不再为您上报告警，在下一次漏洞扫描任务执行时不再扫描该漏洞和呈现该漏洞信息。详细操作请参见**处理漏洞**。

9.2.4 导入/导出漏洞

操作场景

本章节介绍如何导入、导出漏洞。

- **导入漏洞**
- **导出漏洞**

约束与限制

- 仅支持导入.xlsx格式的文件，且文件大小不超过5MB。
- 安全云脑最多支持导出9999条漏洞信息。

导入漏洞

步骤1 登录管理控制台。

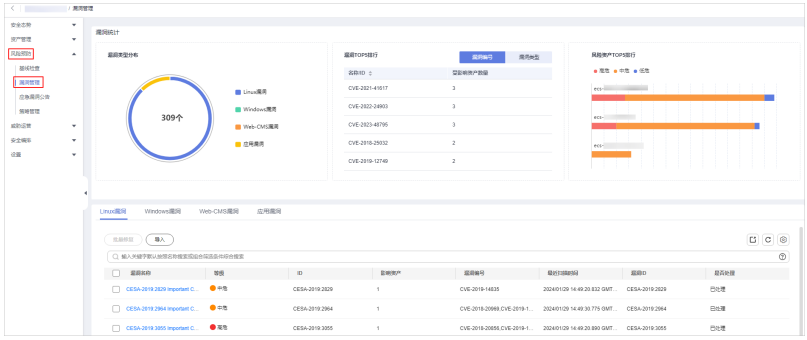
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-31 进入目标工作空间管理页面

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 9-32 进入漏洞管理页面



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

步骤6 在漏洞管理页面中，单击漏洞管理列表上方的“导入”，弹出导入对话框。

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

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

步骤9 选择完成后，单击“确认”，完成导入。

----结束

导出漏洞

最多支持导出9999条漏洞信息。

步骤1 登录管理控制台。

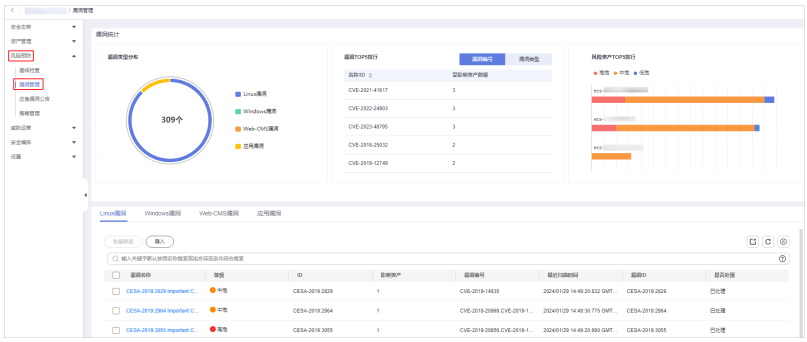
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-33 进入目标工作空间管理页面

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 9-34 进入漏洞管理页面



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

步骤6 在漏洞管理页面中，单击漏洞管理列表右上方的，弹出导出漏洞对话框。

步骤7 在导出漏洞对话框中，配置漏洞参数。

表 9-43 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

操作场景

某些漏洞只在特定条件下存在风险，比如某漏洞必须通过开放端口进行入侵，如果主机系统并未开放该端口，则该漏洞不存在危害。如果评估后确认某些漏洞无害，可以忽略该漏洞，无需修复。忽略后，下次HSS漏洞扫描后仍然会对该漏洞进行告警，安全云脑也将同步漏洞信息。同时，如果某个漏洞仍然需要关注，可以执行取消忽略操作。

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。

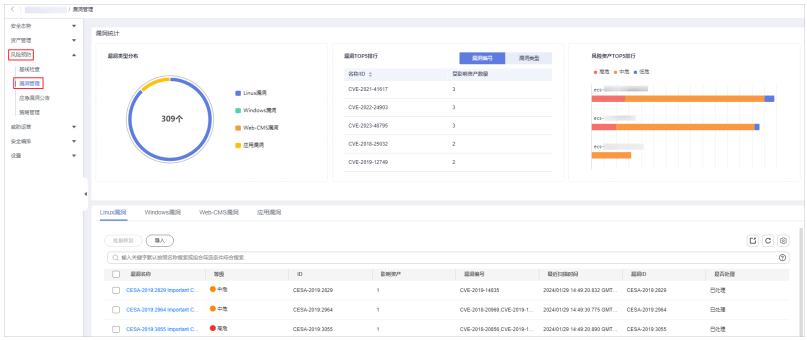
步骤2 在页面左上角单击，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 9-35 进入目标工作空间管理页面

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 9-36 进入漏洞管理页面



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

步骤6 在漏洞列表中，单击目标漏洞名称，右侧弹出漏洞信息页面。

步骤7 对目标漏洞进行忽略或取消忽略操作。

- 忽略

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

- 取消忽略

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

  b. 在确认框中，确认无误后，单击“确认”。

----结束

9.3 查看/导出应急漏洞公告

背景信息

安全云脑通过采集华为云安全公告讯息，及时呈现业界近期广泛披露的安全漏洞，并支持一键获取安全漏洞详情、影响范围和处置建议等信息，提供对资产风险的消减建议。

应急漏洞功能支持以下特性：

- 支持追溯已披露的安全漏洞至2014年4月。
- 支持每5分钟抓取一次安全公告讯息，更新应急漏洞公告。
- 支持按披露时间排序应急漏洞公告。
- 支持按关键字查找应急漏洞公告。
- 支持导出全部应急漏洞公告列表。

操作场景

本章节将介绍如何查看以及导出应急漏洞公告信息。

约束与限制

- 仅支持追溯已披露的安全漏洞公告至2014年4月。
- 仅支持导出应急漏洞公告列表，暂不支持导出公告详细信息。

查看应急漏洞公告

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-37 进入目标工作空间管理页面

步骤4 在安全云脑管理页面选择“风险预防 > 应急漏洞公告”，进入应急漏洞公告汇聚页面。

图 9-38 进入应急漏洞公告页面

步骤5 查看应急漏洞公告列表刷新时间。

查看右上角“更新时间”，即可获知列表刷新时间。

步骤6 查看应急漏洞公告详细信息。

单击应急漏洞公告名称，“一键跳转”到安全公告的漏洞详情页面，可查看安全漏洞披露历程，威胁级别、影响范围、处置办法等信息。

步骤7 按时间查看应急漏洞公告。

在下拉框筛选“全部时间”、“近7天”、“近3天”或“近24小时”条件选项，在列表栏查看显示符合过滤条件的应急漏洞公告。

步骤8 搜索历史应急漏洞公告。

通过在搜索框输入关键字，可搜索到相关应急漏洞公告，在列表栏查看显示符合过滤条件的应急漏洞公告。

----结束

导出应急漏洞公告

在“应急漏洞公告”页面，单击右上角导出标识，一键导出当前列表中安全公告，并以Excel文件形式保存在本地。导出完成后，即可离线查看应急漏洞公告列表。

导出的Excel文件中包含“公告名称”、“披露时间”、“链接”等信息。

9.4 策略管理

9.4.1 策略管理概述

安全云脑的策略管理功能可以简化您在多个账户和资源上的管理和维护任务，以实现各种保护，包括WAF、CFW、VPC安全组、IAM。

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

约束与限制

- 应急策略目前仅支持CFW/WAF/VPC安全组/IAM的黑名单策略。
- 单用户单工作空间内容最多新增300条支持阻断老化的应急策略，全量最多新增1300条应急策略。同时，单次下发应急策略最多可新增50个IP或IAM用户作为阻断对象。
- 将IP或IP地址段或IAM用户配置为黑名单后，来自该IP或IP地址段的访问，CFW/WAF/VPC/IAM将不会做任何检测，直接拦截。

9.4.2 查看防线策略

操作场景

本章节介绍如何查看防线策略。

七层防线是指：物理防线、身份防线、主机防线、运维防线、数据防线、应用防线、网络防线。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-39 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 策略管理”，默认进入防线策略管理页面。

图 9-40 进入防线策略管理页面

步骤5 查看防线策略的统计情况。

- 健康评分：展示当前资产的健康评分。

  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**。

- 资产数量：展示资产总数、高危资产数量和其他风险等级资产数量。
- 告警、漏洞、基线检查统计：展示待处理**威胁告警**、待修复**漏洞**、**基线检查**问题的安全监控统计数据。
  - 威胁告警：展示资产中最**近7天内**未处理威胁告警，可快速了解待处理威胁告警的数量。
  - 漏洞风险：展示资产中TOP5漏洞类型，以及**近7天内**还未修复的漏洞总数。
  - 基线风险：展示最近一次执行基线检查的风险资源的数量，包括致命、高危、中危、低危、提示级别的风险资源。
- 安全云脑防护总览图：展示七层防线中的防护情况及其资源信息。
  - 在“七层防线”栏中可以单击对应防线图标查看对应防线的防护产品及其防护统计信息。
  - 在“资源”栏中可以查看资源统计情况。

----结束

9.4.3 配置防线策略

操作场景

本章节介绍如何配置防线策略。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-41 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“风险预防 > 策略管理”，默认进入防线策略管理页面。

图 9-42 进入防线策略管理页面

步骤5 单击需配置防线策略产品所属的防线名称，右侧滑出对应防线对应的云服务信息。

步骤6 在对应云服务页签中，单击“防护策略”，进入对应云服务防护策略配置页面。

如果还未购买对应云服务，请在产品介绍描述信息中单击产品名称，进入对应与服务控制台页面后，购买对应云服务。

步骤7 在防护策略配置，配置对应云服务的防线策略。

- DDoS防护策略配置：
  - DDoS原生高级防护配置请参考：**配置防护策略**。
  - DDoS高防配置请参考：**配置防护策略**。
- CFW防护策略配置请参考：**配置入侵防御策略**、**管理基础防御规则**。
- WAF防护策略配置请参考：**新增防护策略**。

- HSS防护策略配置请参考：**开启主机防护**、**创建策略组**、**安全配置**。

----结束

9.4.4 新增/编辑应急策略

操作场景

安全云脑可以创建CFW/WAF/VPC安全组/IAM的黑名单策略。

应急策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断。**表9-44**中为推荐设置，除此之外，您也可以结合对多条告警的综合调查结果，对单个攻击源采用多种类型进行阻断。

表 9-44 推荐阻断策略

告警类型	对应防线	推荐阻断策略
HSS告警	主机防线	建议优先采用VPC策略阻断
WAF告警	应用防线	建议优先采用WAF策略阻断
CFW告警	网络防线	建议优先采用CFW策略阻断
IAM告警	身份防线	建议优先采用IAM策略阻断
OBS/DBSS告警	数据防线	当前可根据实际攻击场景和调查结果考虑使用VPC策略阻断/CFW策略阻断，隔绝防护资产和攻击源的网络通信等

本章节介绍如何新增/编辑应急策略。

约束与限制

- 单用户单工作空间内容最多新增300条支持阻断老化的应急策略，全量最多新增1300条应急策略。同时，单次下发应急策略最多可新增50个IP或IAM用户作为阻断对象。
- 将IP或IP地址段或IAM用户配置为黑名单后，来自该IP或IP地址段的访问，CFW/WAF/VPC/IAM将不会做任何检测，直接拦截。
- 应急策略新增成功后，**不支持**修改阻断对象类型和阻断对象（即新增时设置的IP地址或IP地址段或IAM用户名）。

前提条件

如果阻断对象为IAM用户，在新增应急策略前，需要先执行委托授权操作。具体操作步骤请参见**添加委托授权**。

新增应急策略

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-43 进入目标工作空间管理页面

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

图 9-44 进入应急策略管理页面

步骤5 在应急策略管理页面中，单击“新增”，右侧弹出新增应急策略页面。

步骤6 在新增策略页面中，配置策略信息。

表 9-45 新增应急策略

参数名称	参数说明
阻断对象类型	选择阻断对象的类型，可选择IP或IAM。
阻断对象	• 当阻断对象类型选择IP时，输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 • 当阻断对象类型为IAM时，请填写IAM用户名称。 • 单次下发应急策略最多可新增50个IP地址或地址段、或IAM用户作为阻断对象。
标签	自定义应急策略的标签。
操作连接	选择该策略的操作连接。

参数名称	参数说明
阻断老化	确认是否老化该条阻断。 • 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 • 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
原因描述	自定义该策略的描述信息。

步骤7 单击“确定”。

----结束

编辑应急策略

说明

应急策略新增成功后，**不支持**修改阻断对象类型和阻断对象（即新增时设置的IP地址或IP地址段或IAM用户名）。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-45 进入目标工作空间管理页面

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

图 9-46 进入应急策略管理页面

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

步骤6 在编辑策略页面中，修改策略信息。

表 9-46 新增应急策略

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

步骤7 单击“确定”。

----结束

添加委托授权

如果阻断对象为IAM用户，在新增应急策略前，需要执行委托授权操作。具体操作步骤如下：

步骤1 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 IAM”，进入统一身份认证服务管理控制台。

步骤3 添加自定义策略。

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。
   - 策略名称：自定义。
   - 策略配置方式：选择“JSON视图”。
   - 策略内容：请直接复制粘贴以下内容。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:users:updateUser"
```



```
        ]
      }
    ]
}
```

a. 单击“确定”。

步骤4 委托授权。

1. 在左侧导航栏选择“委托”，进入委托页面后，单击“SecMaster_Agency”，默认进入SecMaster_Agency的基本信息页面。
2. 选择“授权记录”页签，并单击“授权”。
3. 在选择策略页面，搜索并选中**步骤3**添加的策略后，单击“下一步”。
4. 设置授权范围，请选择“所有资源”，设置完成后，单击“确定”。

----结束

9.4.5 查看应急策略

操作场景

本章节介绍如何查看已有应急策略。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-47 进入目标工作空间管理页面

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

图 9-48 进入应急策略管理页面

步骤5 在应急策略管理页面上方中，查看应急策略统计情况。

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

步骤6 在策略列表中，查看应急策略的相关信息，参数说明下所示：

表 9-47 查看应急策略

参数名称	参数说明
阻断对象	阻断的单个（或多个）IP地址或IP地址段、或IAM用户名。
标签	策略的标签信息。
策略下发数量	策略在产品中下发的数量。
阻断类型	策略所属的阻断类型。
创建人	策略的创建人信息。
原因描述	策略的描述信息。
创建时间	策略的创建时间。
操作	对策略进行编辑、删除等操作。

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

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

----结束

9.4.6 删除应急策略

操作场景

本章节介绍删除/批量删除应急策略。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-49 进入目标工作空间管理页面

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

图 9-50 进入应急策略管理页面

步骤5 在应急策略管理页面中，单击待删除策略所在行“操作”列的“删除”。

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

步骤6 在弹出的删除确认框中，确认无误后单击“确定”。

----结束

9.4.7 批量阻断/批量取消阻断

操作场景

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

本章节介绍如何执行批量阻断、批量取消阻断操作。

约束与限制

将IP或IP地址段或IAM用户配置为黑名单后，来自该IP或IP地址段的访问，CFW/WAF/VPC/IAM将不会做任何检测，直接拦截。

批量阻断

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-51 进入目标工作空间管理页面

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

图 9-52 进入应急策略管理页面

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

步骤6 在弹出的批量阻断对话框中，输入阻断原因，并单击“确定”。

----结束

批量取消阻断

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 9-53 进入目标工作空间管理页面

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

图 9-54 进入应急策略管理页面

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

步骤6 在弹出的取消阻断对话框中，输入取消阻断原因，并单击“确定”。

----结束

10 威胁运营

10.1 事件管理

10.1.1 查看事件信息

操作场景

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

本章节主要介绍如何查看事件信息。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 10-2 事件管理页面

步骤5 在事件管理页面查看事件信息。

图 10-3 查看事件信息

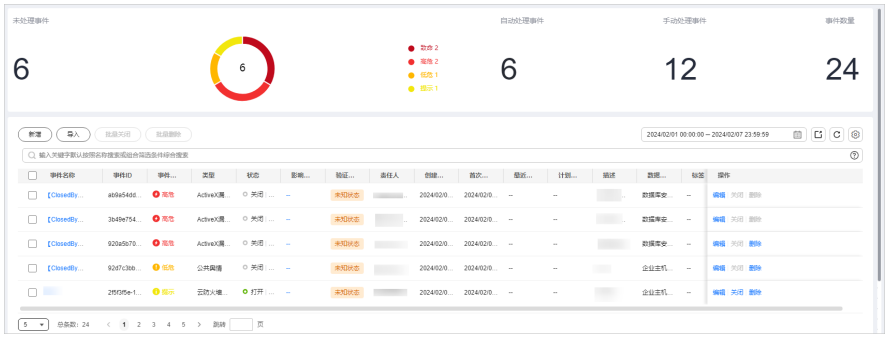


表 10-1 查看事件信息

参数名称	参数说明
未处理事件	当前工作空间在设定的时间范围内未处理事件的数量及其所属等级分布情况。
自动处理事件	当前工作空间在设定的时间范围内通过剧本自动处理的事件数量。
手动处理事件	当前工作空间在设定的时间范围内手动处理的事件数量。
事件数量	当前工作空间在设定的时间范围内的事件总数量。

参数名称	参数说明
事件列表	展示事件的详细信息。 在事件列表中下方可以查看事件总条数。其中，使用翻页查看时最多可查看10000条事件信息，如果需要查看超过10000条以外数据，请优化过滤条件筛选数据。 事件列表中，可以查看事件的名称、等级、来源、状态等信息。如需查看某个事件概览，可单击事件名称，页面右侧将展示事件的概览信息。 • 在事件概览页面可以查看事件的处置建议、基本信息和关联信息（包括关联的威胁指标、告警、事件、攻击信息等）。 • 如果需要查看事件详情，可以在事件概览页面右下角单击“事件详情”，进入事件详情页面。 在详情页面除了可以查看概览页面的信息外，还可以查看事件的时间线和攻击信息。例如：事件首次发生时间、检测时间、攻击进程ID等。 • 在事件概览/详情页面可以在事件等级和状态的下拉箭头中修改事件等级、状态。 • 在事件概览/详情页面可以关联或取消关联告警、事件、情报，还可以查看受影响资产相关信息。

----结束

10.1.2 新增/编辑事件

操作场景

本章节主要介绍如何新增事件，以及如何对已有的事件进行编辑。

新增事件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 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。

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，可选择以下类型：华为产品、第三方产品、租户私有产品。
	（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。

参数名称		参数说明
	（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）调试数据	选择是否开启模拟调试功能。
	（可选）标签	填写事件的标签。
	描述	事件描述信息，输入规则如下： ● 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_()）。 ● 长度不能超过1024个字符。

步骤6 单击“确认”，完成事件创建。

----结束

编辑事件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 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。

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。

参数名称		参数说明
	（可选）阶段	选择您的事件阶段。 • 准备：准备资源处理事件。 • 检测与分析：检测与分析事件发生原因。 • 控制、清除、恢复：进行事件问题处理。 • 事件后活动：事件处理完成后的后续活动。
	（可选）模拟调试项	选择是否开启模拟调试功能，**不支持修改**。
	（可选）标签	填写事件的标签。
	描述	事件描述信息，输入规则如下： • 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。 • 长度不能超过1024个字符。

步骤7 单击“确认”，完成事件编辑。

----结束

10.1.3 导入/导出事件

操作场景

本章节主要介绍如何导入、导出事件。

约束与限制

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

导入事件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 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。

步骤8 选择完成后，单击“确定”，完成导入。

----结束

导出事件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 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。

表 10-4 导出事件

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

步骤7 单击“确定”。

系统将自动下载事件excel表格到本地。

----结束

10.1.4 关闭/删除事件

操作场景

本章节主要介绍如何执行关闭/删除事件操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 事件管理”，进入事件管理页面。

图 10-13 事件管理页面

步骤5 在事件管理页面中，对事件进行关闭或删除操作。

表 10-5 管理事件

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

----结束

10.2 告警管理

10.2.1 查看告警信息

操作场景

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

本章节主要介绍如何查看告警信息。

操作步骤

步骤1 登录管理控制台。

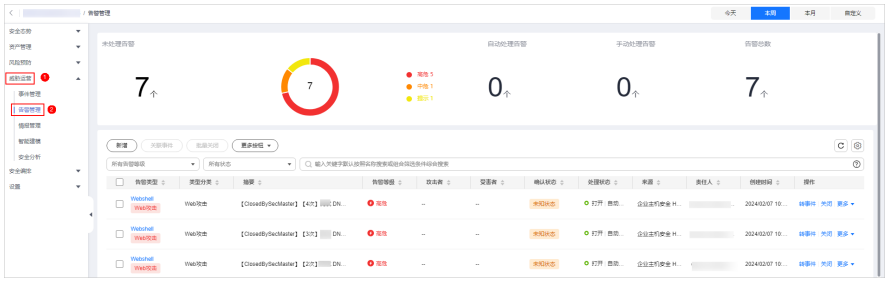
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-15 告警管理页面



步骤5 在告警管理页面查看告警信息。

图 10-16 查看告警信息

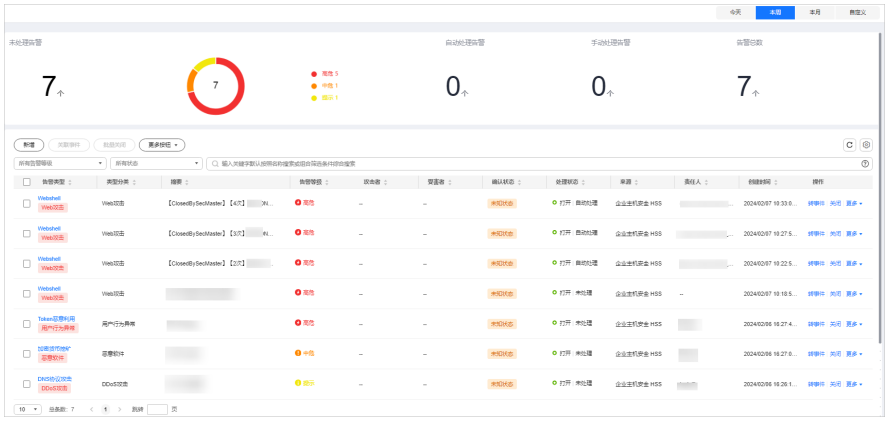


表 10-6 查看告警信息

参数名称	参数说明
设置告警的显示时间范围	右上角可设置展示告警的周期，默认展示本周内告警信息。
未处理告警	当前工作空间在设定的时间范围内未处理告警的数量及其所属等级分布情况。
自动处理告警	当前工作空间在设定的时间范围内通过剧本自动处理的告警数量。
手动处理告警	当前工作空间在设定的时间范围内手动处理的告警数量。
告警总数	当前工作空间在设定的时间范围内告警总数量。

参数名称	参数说明
告警列表	展示告警的详细信息。 在告警列表中下方可以查看告警总条数。其中，使用翻页查看时最多可查看10000条告警信息，如果需要查看超过10000条以外数据，请优化过滤条件筛选数据。 告警列表中，可以查看告警的类型、摘要、等级、来源、处理状态等信息。如需查看某个告警概览信息详情，可单击目标告警名称，页面将展示该条告警的详情信息。 • 在告警详情页面中，可以对该条告警进行评论、一键阻断、一键解封、转事件、关闭、删除、刷新操作。 • 在告警详情页面可以查看告警的总览、上下文、关系图和评论信息。 – 总览：展示该条告警的摘要、处理建议、基础信息、请求详情等信息。 – 上下文：通过JSON和表格两种方式展示该条告警的上下文关键信息和全文信息。 – 关系图：展示该条告警的关联信息，例如关联的告警、事件、情报和受影响的资产信息。 – 评论：展示该条告警的历史评论信息，还可以新增评论。

----结束

10.2.2 告警转事件或关联事件

操作场景

本章节主要介绍如何将告警转为事件，以及告警如何关联事件。

告警转事件

步骤1 登录管理控制台。

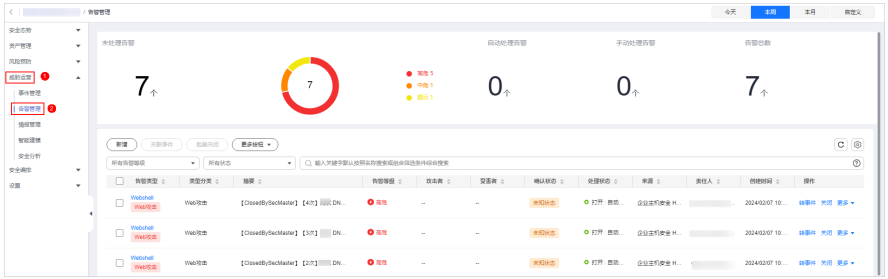
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-17 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-18 告警管理页面



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

同时，还可以在某条告警详情页面，单击页面右上角的“告警转事件”。

步骤6 在转事件配置页面中，填写“事件名称”并设置“事件类型”。

事件名称将自动填入当前告警的名称，可以进行修改。

步骤7 设置完成后，单击“确认”。

----结束

告警关联事件

步骤1 登录管理控制台。

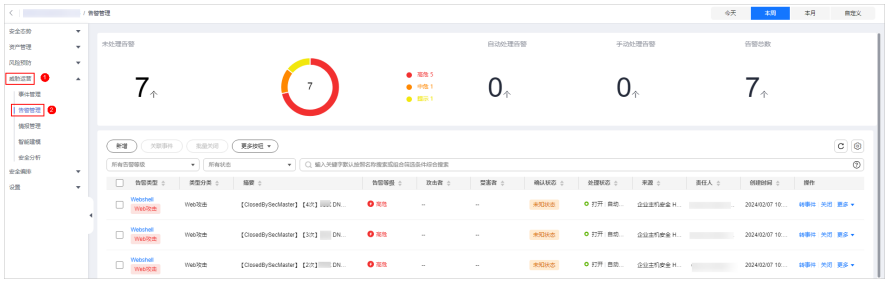
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-20 告警管理页面



步骤5 在告警管理列表中，勾选需要关联事件的告警，并单击列表上方的“关联事件”，弹出绑定事件对话框。

步骤6 在绑定事件对话框中，勾选需要绑定的事件，并单击“确认”。

----结束

10.2.3 新增/编辑告警

操作场景

本章节主要介绍如何新增告警，以及如何对已有的告警进行编辑。

新增告警

步骤1 登录管理控制台。

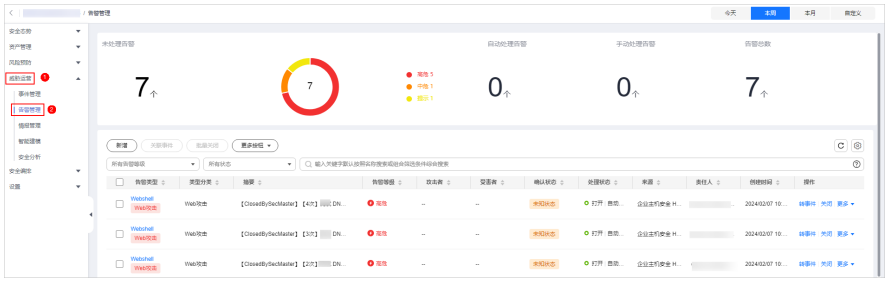
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-21 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-22 告警管理页面



步骤5 在告警管理页面单击“新增”，并在右侧弹出的新增告警管理页面中配置参数，参数配置说明如**表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。
	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，可选择以下类型：华为产品、第三方产品、租户私有产品。
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。

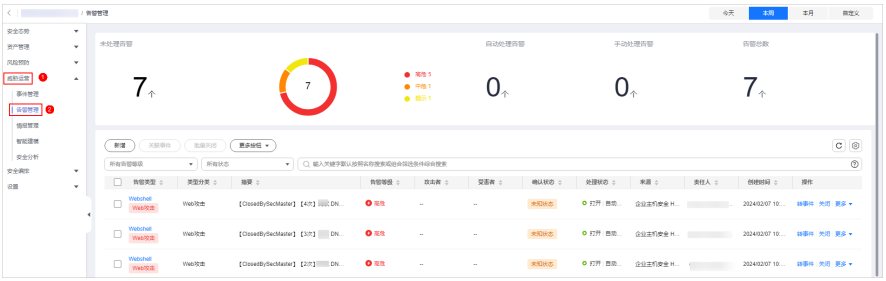
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-23 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-24 告警管理页面



步骤5 在告警管理列表中，单击目标告警所在行“操作”列的“更多 > 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。

参数名称		参数说明
	告警等级	选择告警严重等级，可选择以下等级：提示、低危、中危、高危、致命。
	状态	选择告警状态，可选择以下状态：打开、阻塞、关闭。
	（可选）责任人	选择告警的主要责任人。
	数据源产品名称	选择数据源产品的名称，**不支持修改**。
	数据源类型	选择数据源所属类型，**不支持修改**。
时间线	首次发生时间	该条告警首次发生时间。
	最近发现时间	该条告警最近一次发现的具体时间。
	计划关闭时间	选择告警计划关闭时间。
其他	标签	填写告警的标签。
	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”。

----结束

10.2.4 导入/导出告警

操作场景

本章节主要介绍如何导入、导出告警。

约束与限制

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

导入告警

步骤1 登录管理控制台。

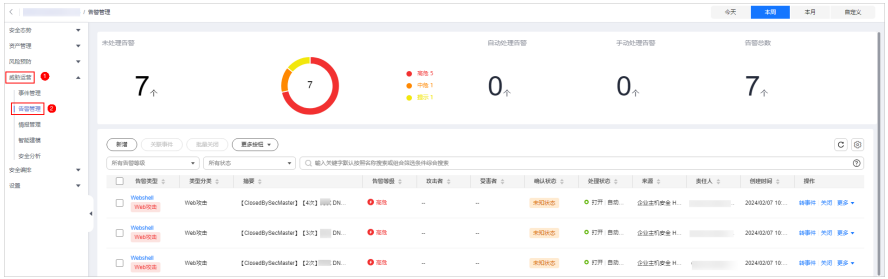
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-25 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-26 告警管理页面



步骤5 在告警管理页面中，单击告警列表左上角的“更多按钮 > 导入”。

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

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

步骤8 选择完成后，单击“确定”，完成导入。

----结束

导出告警

步骤1 登录管理控制台。

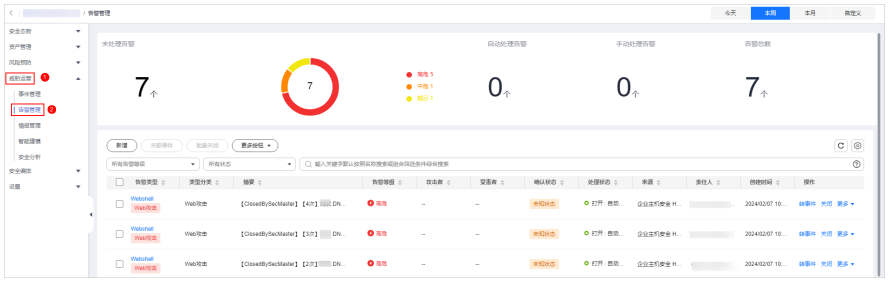
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-27 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-28 告警管理页面



步骤5 在告警管理列表中，勾选您需要导出的告警，并单击告警列表左上角的“更多按钮 > 导出”，弹出导出对话框。

步骤6 在导出告警对话框中，配置参数。

表 10-9 导出告警

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

步骤7 单击“确定”。

系统将自动下载告警excel表格到本地。

----结束

10.2.5 关闭/删除告警

操作场景

本章节主要介绍如何执行关闭/删除告警操作。

操作步骤

步骤1 登录管理控制台。

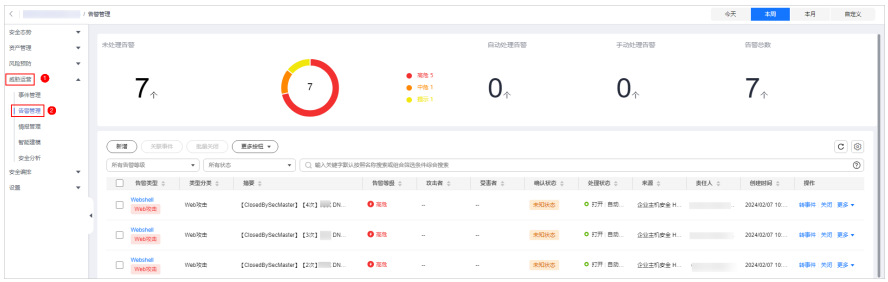
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-29 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-30 告警管理页面



步骤5 在告警管理页面中，对告警进行关闭或删除操作。

表 10-10 管理告警

操作	操作说明
关闭告警	1. 单击目标告警所在行“操作”列的“关闭”，弹出关闭告警确认框。 如果需要关闭多条告警，可以在告警列表中勾选需要关闭的告警，并单击列表上方“批量关闭”。 2. 在关闭确认框中，选择“关闭原因”并填写“关闭评论”后，单击“确认”。
删除告警	1. 单击目标告警所在行“操作”列的“更多 > 删除”，弹出删除告警确认框。 如果需要删除多条告警，可以在告警列表中勾选需要删除的告警，并单击列表上方“更多按钮 > 批量删除”。 2. 在弹出的确认框中，单击“确认”。 **说明** 告警删除后将无法恢复，请谨慎操作。

----结束

10.2.6 告警处置建议

目前安全云脑在数据集成时，可以设置将接入的云服务日志自动转告警。针对转入的告警提供以下处理建议，请根据情进行排查处理。

系统行为异常/高危命令执行

表 10-11 高危命令执行

数据来源	主机安全告警日志
告警呈现	【 dangercmd 】【 HSS 】主机:{{ipList}}执行dangercmd，{{__time}}
监控场景	主机执行高危命令
告警对应字段	高危命令在安全云脑的告警中对应的字段查看方法如下： 1. 进入安全云脑的“安全编排 > 运营对象 > 分类&映射”页面。 2. 单击“主机安全服务告警分类映射”名称，进入分类映射详情页面。 其中高危命令执行对应“msg.appendInfo.event_type=3015”。
调查思路及处理建议	1. 进入安全云脑的“威胁运营 > 安全分析”页面，展开目标数据空间并单击数据管道sec-hss-alarm名称，右侧展示ssec-hss-alarm的查询分析页面。 2. 通过appendInfo.event_type、__time、ipList三个字段对应的值进行检索，查询出当前告警所对应详细日志,定位命令含义和目的： ● 利用appendInfo. process_info字段分析当前高危命令（process_cmdline）和其父进程命令（parent_process_cmdline）是否可疑； ● 同时，可利用sec-hss-log查询相近时间内主机(ipList)行为，通过appendInfo.pid_link(sec-hss-log)等字段与appendInfo. process_info.parent_process_pid(sec-hss-alarm)梳理进程的顺序关系，综合判断命令/进程是否为正常业务运行、是否有可能为黑客执行，同时对黑客入侵后行为有基本判定（查看敏感信息、查看网络环境、提权、网络探测、执行poc等）。 ● 如果综合判断是黑客攻击行为触发，立即联系资产责任人处理。

高危命令	告警所涉及到的高危命令如下： • strace：捕获和记录指定进程的所有系统调用，以及接收的所有信号。 • rz：用于从本地计算机向远程主机上传文件，通常用于SSH会话中。 • sz：用于从远程主机向本地计算机下载文件的命令，通常用于SSH会话中。 • tcpdump：用于数据报嗅探，可以抓取流动在网卡上的数据包。 • nmap：用于网络扫描和嗅探。 • nc/ncat：全称netcat，实现很多网络相关功能，如监听、连接端口等。

Web 攻击/SQL 注入

- **告警对应字段**

  SQL注入在安全云脑的告警中对应的字段查看方法如下：

  a. 进入安全云脑的“安全编排 > 运营对象 > 分类&映射”页面。

  b. 单击“Web应用防火墙告警分类映射”名称，进入分类映射详情页面。

  其中SQL注入对应的“msg.attack”为“sqli”。

- **排查方法及处理建议如下**：

  a. 进入安全云脑的“威胁运营 > 安全分析”页面，展开目标数据空间并单击数据管道sec-waf-attack名称，右侧展示sec-waf-attack的查询分析页面。

  b. 通过attack、__time、sip三个字段对应的值进行检索，查询出当前告警所对应详细日志。关键参数信息如下：

  - hit_data：攻击报文或链接
  - uri：请求url
  - action：处理动作
  - cookie：请求cookie信息

  c. 根据攻击报文判断SQL注入的方式，定位该应用程序是否存在该漏洞。

  如果存在请及时修复，采用使用参数化查询、输入验证、更新和修补软件等处理方法。

Web 攻击/漏洞攻击

- **告警对应字段**

  漏洞攻击在安全云脑的告警中对应的字段查看方法如下：

  a. 进入安全云脑的“安全编排 > 运营对象 > 分类&映射”页面。

  b. 单击“Web应用防火墙告警分类映射”名称，进入分类映射详情页面。

  其中漏洞攻击对应的“msg.attack”为“vuln”。

- **排查方法及处理建议如下**：

a. 进入安全云脑的“威胁运营 > 安全分析”页面，展开目标数据空间并单击数据管道sec-waf-attack名称，右侧展示sec-waf-attack的查询分析页面。
b. 通过attack、__time、sip三个字段对应的值进行检索，查询出当前告警所对应详细日志。关键参数信息如下：
   - hit_data：攻击报文或链接
   - uri：请求url
   - action：处理动作
   - cookie：请求cookie信息
   - header：请求header信息
c. 根据攻击报文判定为哪种漏洞攻击，同时对受攻击的资产进行漏洞查询。
   如果存在此漏洞，请及时修复，防止攻击者再次利用漏洞攻击系统或应用程序。

Web 攻击/命令注入

- **告警对应字段**
  命令注入在安全云脑的告警中对应的字段查看方法如下：
  进入安全云脑的“安全编排 > 运营对象 > 分类&映射”页面，单击“Web应用防火墙告警分类映射”名称，进入分类映射详情页面，其中命令注入对应的“msg.attack”为“cmdi”。
- **排查方法及处理建议如下**：
  a. 进入安全云脑的“威胁运营 > 安全分析”页面，展开目标数据空间并单击数据管道sec-waf-attack名称，右侧展示sec-waf-attack的查询分析页面。
  b. 通过attack、__time、sip三个字段对应的值进行检索，查询出当前告警所对应详细日志。关键参数信息如下：
     - hit_data：攻击报文或链接
     - uri：请求url
     - action：处理动作
     - cookie：请求cookie信息
     - header：请求header信息
  c. 根据攻击报文判断命令注入的方式，定位该应用程序是否存在该漏洞。
     - 如果存在尽快修补漏洞，并更新相关软件或库的版本。
     - 对系统进行全面的检查，确认是否存在其他的漏洞或后门，以保证系统的安全性。
     - 限制系统的访问权限，例如禁用root账户、限制访问来源IP等，以减少攻击者可能的入侵路径等。

系统行为异常/进程异常行为

根据告警对应的影响资产，对受影响资产、服务、业务等有基本定位。

- **告警对应字段**

  进程异常行为在安全云脑的告警中对应的字段查看方法如下：

  a. 进入安全云脑的“安全编排 > 运营对象 > 分类&映射”页面。

  b. 单击“主机安全服务告警分类映射”名称，进入分类映射详情页面。

  其中进程异常行为对应“msg.appendInfo.event_type=3007”。

- **排查方法及处理建议如下**：

  a. 进入安全云脑的“威胁运营 > 安全分析”页面，展开目标数据空间并单击数据管道sec-hss-alarm名称，右侧展示sec-hss-alarm的查询分析页面。

  i. appendInfo.event_type、__time、ipList三个字段对应的值进行检索，查询出当前告警所对应详细日志。

  b. 通过查看appendInfo. process_info中当前进程和父进程的信息，综合判断是否异常，如果异常，则联系对应资源负责人处理。

  - 立即停止受影响的进程或服务，以避免继续受到攻击或造成其他损害；
  - 尽快调查异常行为的原因和来源，例如查看日志、监控系统、分析进程内存等，以确定异常的具体表现和可能的根本原因；
  - 根据异常行为的性质和严重程度，采取适当的应对措施，例如重启进程、修复软件错误、排除系统故障、更换硬件设备等；
  - 对受影响的系统进行全面的检查，确认是否存在其他的漏洞或后门，以保证系统的安全性。

系统行为异常/关键文件目录变更

根据告警对应的影响资产，对受影响资产、服务、业务等有基本定位。

- **告警对应字段**

  关键文件目录变更在安全云脑的告警中对应的字段查看方法如下：

  a. 进入安全云脑的“安全编排 > 运营对象 > 分类&映射”页面。

  b. 单击“主机安全服务告警分类映射”名称，进入分类映射详情页面。

  其中关键文件目录变更对应“msg.appendInfo.event_type=3005”。

- **排查方法及处理建议如下**：

  a. 进入安全云脑的“威胁运营 > 安全分析”页面，展开目标数据空间并单击数据管道sec-hss-alarm名称，右侧展示sec-hss-alarm的查询分析页面。

  b. 通过appendInfo.event_type、__time、ipList三个字段对应的值进行检索，查询出当前告警所对应详细日志。

  其中appendInfo.file_info为文件目录信息，判断是否异常，如果异常，则联系对应资源负责人处理。

  - 确定变更的影响范围：首先需要确定目录变更对哪些文件产生了影响，以及这些文件对业务的影响程度。如果变更的影响范围比较大，需要立即采取措施防止进一步的损失。
  - 恢复关键文件：如果目录/文件异常变更，需要及时恢复。如果文件被删除或损坏，需要从备份中恢复。如果没有备份，需要立即停止相关操作，采取数据恢复措施，尽可能将文件恢复到变更前的状态。

- 更新相关配置：对于一些需要配置文件路径的程序和系统，需要及时更新相关配置，确保这些程序和系统能够正确访问到关键文件。
- 审查变更原因：对于目录变更的原因，需要进行审查和排查。如果是人为错误导致的，需要及时纠正和加强管理。如果是系统自动进行的调整，需要评估调整的必要性和影响，确保变更的合理性和安全性。
- 加强安全措施：对于关键文件的安全管理，需要加强措施，确保文件不会被误删除、恶意篡改或泄露。可以采取加密、备份、访问控制等措施，确保文件的完整性和可用性。

10.2.7 一键阻断/解封

操作场景

应急策略作为告警一键阻断的止血手段，可根据告警来源选择相应的类型对攻击者进行阻断。表10-12中为推荐设置，除此之外，您也可以结合对多条告警的综合调查结果，对单个攻击源采用多种类型进行阻断。

表 10-12 推荐阻断策略

告警类型	对应防线	推荐阻断策略
HSS告警	主机防线	建议优先采用VPC策略阻断
WAF告警	应用防线	建议优先采用WAF策略阻断
CFW告警	网络防线	建议优先采用CFW策略阻断
IAM告警	身份防线	建议优先采用IAM策略阻断
OBS/DBSS告警	数据防线	当前可根据实际攻击场景和调查结果考虑使用VPC策略阻断/CFW策略阻断，隔绝防护资产和攻击源的网络通信等

本章节介绍如何执行一键阻断和一键解封操作。

一键阻断

步骤1 登录管理控制台。

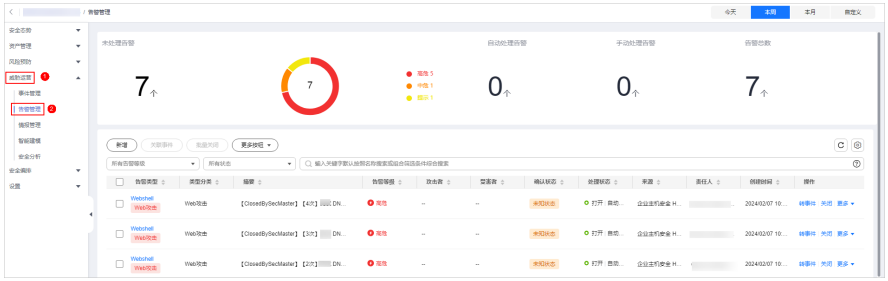
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-31 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-32 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 > 一键阻断”，右侧弹出一键阻断配置页面。

同时，还可以在某条告警详情页面，单击页面右上角的“一键阻断”。

步骤6 在一键阻断配置页面中，配置阻断策略信息。

表 10-13 一键阻断

参数名称	参数说明
阻断对象	• 当阻断对象类型选择IP时，输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 • 当阻断对象类型为IAM时，请填写IAM用户名称。 • 单次下发应急策略最多可新增50个IP地址或地址段、或IAM用户作为阻断对象。
标签	自定义阻断策略的标签。
操作连接	选择该阻断策略的操作连接。
阻断老化	确认是否老化该条阻断策略。 • 如果选择是，请设置策略老化时间，如设置为180天，即该策略在设置后的180天内有效，180天后将不再继续阻断设置的IP地址或IP地址段。 • 如果选择否，则该策略将一直有效，阻断设置的IP地址或IP地址段。
原因描述	自定义该阻断策略的描述信息。

步骤7 确认配置无误后，单击“确定”，并在弹出的提示框中，单击“确认”。

----结束

一键解封

步骤1 登录管理控制台。

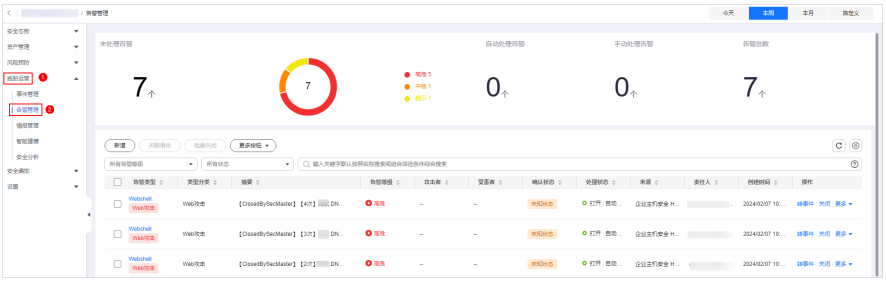
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-33 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 10-34 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 > 一键解封”。

同时，还可以在某条告警详情页面，单击页面右上角的“一键解封”。

步骤6 在弹出的一键解封确认框中，输入解封原因，并单击“确定”。

----结束

10.3 情报管理

10.3.1 新增/编辑情报指标

操作场景

情报指标库列表呈现当前您的所有指标信息。

本章节主要介绍如何新建或编辑情报指标。

新增情报指标

步骤1 登录管理控制台。

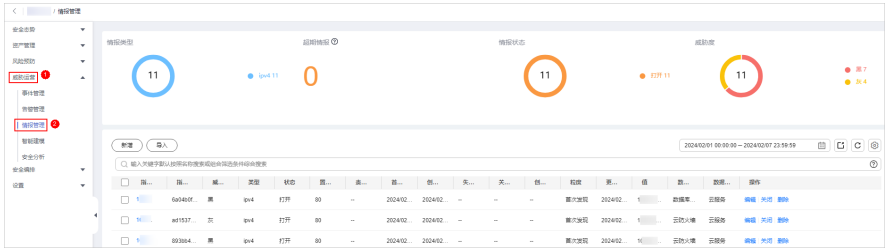
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-35 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 10-36 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 10-14 指标参数说明

参数	说明
指标名称	自定义威胁情报指标名称，命名规则如下： 可输入中文字符、英文大写字母（A～Z）、英文小写字母（a～z）、数字（0～9）和特殊字符（-_ ()）。
类型	选择指标类型。
威胁度	选择威胁度等级。 • 黑：表示危险 • 灰：表示一般 • 白：表示安全
数据源产品名称	选择数据源产品的名称。
数据源类型	选择数据源所属类型，可选择以下类型：华为产品、第三方产品、租户私有产品。
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。

参数	说明
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、邮箱账户、地区等信息。

步骤6 单击“确认”。

----结束

编辑情报指标

步骤1 登录管理控制台。

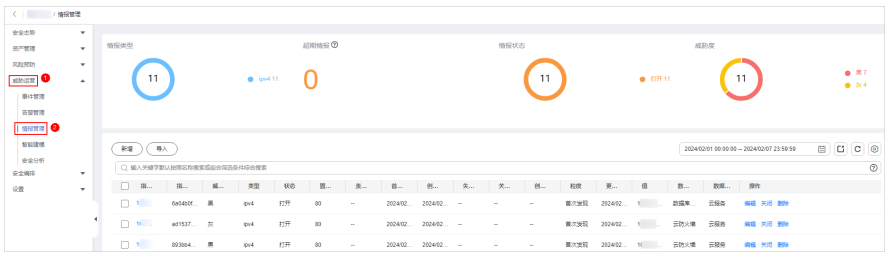
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-37 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 10-38 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。
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、邮箱账户、地区等信息。

步骤7 单击“确认”。

----结束

10.3.2 关闭/删除情报指标

操作场景

本章节主要介绍如何关闭和删除情报指标。

操作步骤

步骤1 登录管理控制台。

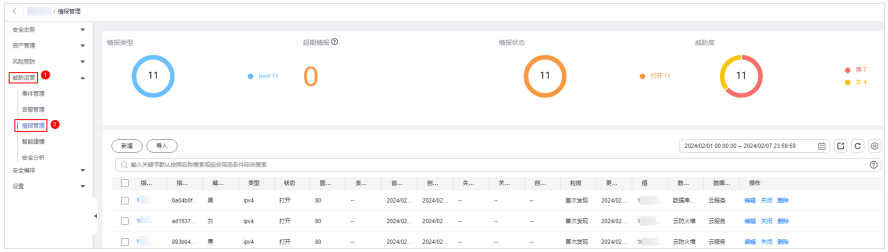
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-39 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 10-40 情报管理页面



步骤5 在情报管理页面中，对情报进行关闭或删除操作。

表 10-16 管理情报

操作	操作说明
关闭情报	1. 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。 2. 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。 3. 单击“确认”。
删除情报	1. 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。 2. 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

10.3.3 导入/导出情报指标

操作场景

本章节主要介绍如何导入、导出情报指标。

约束与限制

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

导入指标

步骤1 登录管理控制台。

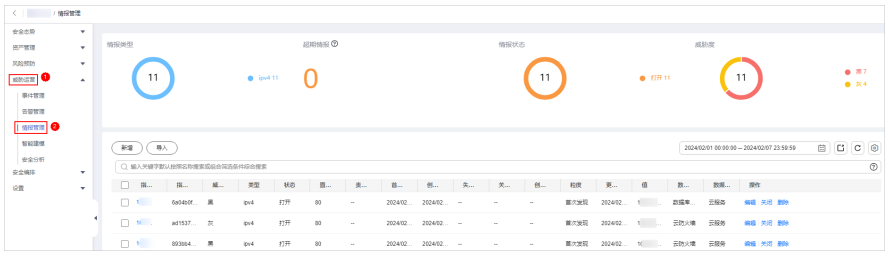
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-41 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 10-42 情报管理页面



步骤5 在情报管理页面中，单击指标列表左上角的“导入”。

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

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

步骤8 选择完成后，单击“确定”，完成导入。

----结束

导出指标

步骤1 登录管理控制台。

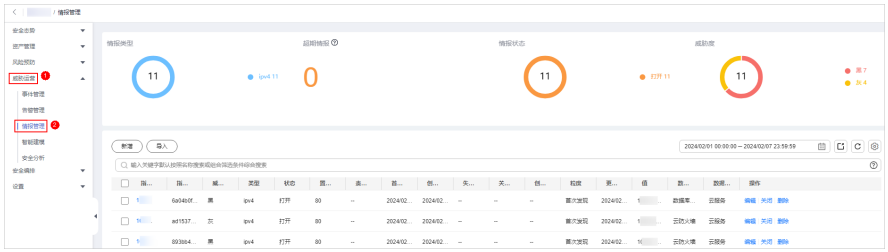
步骤2 在页面左上角单击 ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-43 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 10-44 情报管理页面



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

步骤6 在导出指标对话框中，配置参数。

表 10-17 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 查看情报指标

操作场景

本章节主要介绍如何查看已有情报指标信息。

操作步骤

步骤1 登录管理控制台。

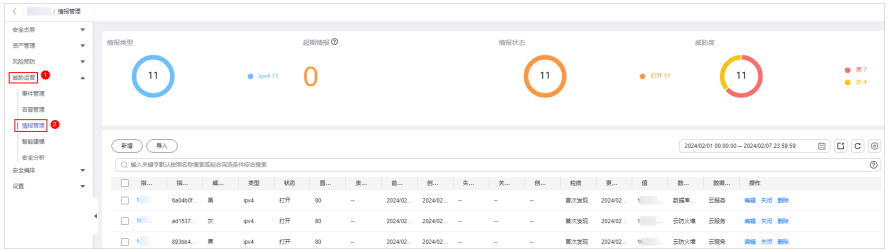
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-45 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 情报管理”，进入情报管理页面。

图 10-46 情报管理页面



步骤5 在情报管理页面查看情报指标信息。

图 10-47 查看情报指标信息

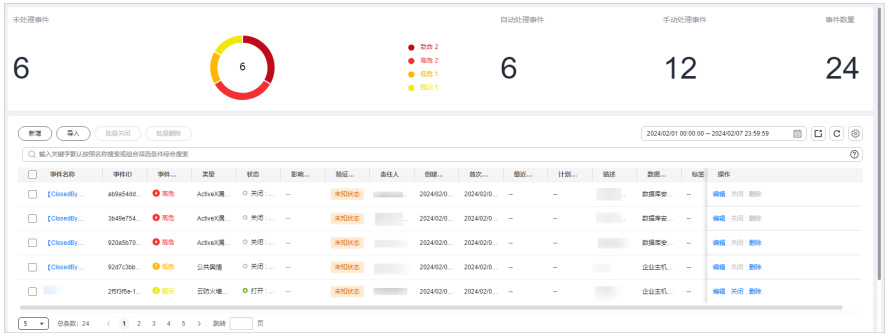


表 10-18 查看情报指标信息

参数名称	参数说明
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。
情报管理列表	展示情报的详细信息。 在情报指标列表中下方可以查看情报指标总条数。其中，使用翻页查看时最多可查看10000条情报指标信息，如果需要查看超过10000条以外数据，请优化过滤条件筛选数据。 情报指标列表中，可以查看情报的威胁度、发现时间、状态等信息。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。 ● 在情报概览页面可以查看情报的基本信息和关联信息（包括关联的威胁指标、告警、事件）。 ● 在**关联信息**中，可以将情报指标和其他情报指标、告警和事件进行绑定或解绑操作。

----结束

10.4 智能建模

10.4.1 查看已有模板

操作场景

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 在页面左上角单击 ☰，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 10-48 进入目标工作空间管理页面

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

图 10-49 模型模板页面

步骤5 在模型模板页面，查看已有模型模板。

表 10-19 查看模板信息

参数名称	参数说明
模型模板统计	显示**可用模板**和**活跃模板**数量。
严重程度	显示当前已有模板的严重程度统计情况，包含致命、高危、中危、低危、提示级别。
模板列表	• 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

操作场景

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**
- **自定义新建告警模型**
- **编辑模型**

约束与限制

- 单账号单Region单workspace最多创建100个告警模型。
- 一个告警模型的运行时间间隔须 ≥ 5分钟，查询数据的时间范围 ≤ 14天。

使用已有模板创建告警模型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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 10-50 进入目标工作空间管理页面

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

图 10-51 模型模板页面

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

步骤6 在模型模板详情页面，单击右下角“创建模型”，进入新建告警模型页面。

步骤7 在新增告警模型页面中，配置告警模型基础信息，参数说明如**表10-20**所示。

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。
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。

参数名称	参数说明
模型类型	默认为规则模型。
描述	该告警模型的描述信息。
启用状态	设置该告警模型的启用状态。 ●  ：表示启用，默认为此状态。 ●  ：表示未启用。 此处设置的状态，可在整个告警模型设置成功后进行更改。

步骤8 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤9 设置模型逻辑，参数说明如表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

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

自定义新建告警模型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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 10-52 进入目标工作空间管理页面

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

图 10-53 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10-22所示。

表 10-22 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10-23**所示。

表 10-23 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**查询与分析语法-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。

参数名称	参数说明
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 在页面左上角单击 ☰，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 10-54 进入目标工作空间管理页面

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

图 10-55 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10-24所示。

表 10-24 告警模型基础配置

参数名称	参数说明
管道名称	选择该告警模型的执行管道。**暂不支持编辑**。
模型名称	自定义该条告警模型的名称。
严重程度	设置该告警模型的严重程度。可以设置致命、高危、中危、低危、提示级别。
告警类型	选择该条告警模型触发后，提示的告警类型。
模型类型	默认为规则模型。
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10-25所示。

表 10-25 设置模型逻辑

参数名称	参数说明
查询规则	设置告警的查询规则，设置完成后可以单击“运行”，查看当前运行结果。
查询计划	设置告警查询计划。 • 运行查询间隔：xx分钟/小时/天。 当运行查询间隔为分钟时，可设置为5-59分钟；当运行查询为小时时，可设置为1-23小时；当运行查询为天时，可设置为1-14天。 • 时间窗口：xx分钟/小时/天。 当时间窗口为分钟时，可设置为5-59分钟；当时间窗口为小时时，可设置为1-23小时；当时间窗口为天时，可设置为1-14天。 • 延迟执行时间：xx分钟，可以设置为0-5分钟。
告警扩充	• 自定义信息：自定义告警扩充信息。 单击“添加”，并设置key+value信息，完成新增。 • 告警详细信息：自定义填写告警名称、描述和处置建议。

参数名称	参数说明
触发条件	设置告警触发条件。可设置为：大于/等于/不等于/小于xx时，触发告警。 如有多条触发条件，可以单击“添加”按钮进行添加。
告警分组	配置将规则查询结果分组到告警的方式。可选择以下方式： • 将所有查询结果分组到一个告警中 • 将每条查询结果独立触发告警
调试模式	设置是否生成调试类告警。
抑制	设置生产告警后是否停止运行查询。 •  ：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

操作场景

本章节将介绍如何查看已新增的模型。

前提条件

已新增模型，详细操作请参见**新建/编辑模型**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-56 进入目标工作空间管理页面

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

图 10-57 可用模型页面

步骤5 在可用模型页面，查看已有模型。

表 10-26 查看已有模型信息

参数名称	参数说明
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	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

操作场景

本章节将介绍如何管理模型，如启用、停用、删除模型等操作。

约束与限制

仅支持对自定义创建的模型进行启用、停用、删除操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-58 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 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 在可用模型页面中，管理模型。

表 10-27 管理模型

操作	操作说明
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。

支持接入的云产品和日志

安全云脑支持集成WAF、HSS、OBS等多种华为云云产品的日志数据。集成后，可以检索并分析所有收集到的日志，且默认存储7天。

具体支持接入的云服务日志请参见**支持接入的日志**。

约束与限制

- 单次查询分析最多支持返回500条结果。
- 一个数据管道内最多创建50个快速查询，即最多可以将50个查询分析条件保存为快速查询。
- 单次查询结果大于50000条时，准确率可能会下降。请通过缩短查询的时间范围、添加查询限制条件等方法减少查询结果的数量。
- 使用聚合查询（例如group by语句）聚合多个字段时，第二个字段默认分桶数量为10，如果超出会有数据丢失的情况，将导致查询结果不准确。

10.5.2 使用流程

安全分析功能使用具体流程如**表10-28**所示。

表 10-28 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、安全等多种华为云云产品的日志数据。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。 接入的云服务日志，默认已为部分保留字段配置索引，具体请参见**日志字段含义**。
查询与分析	对接入的数据进行查询、分析。

子流程	说明
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 日志字段含义

如果您通过控制台接入了WAF、HSS、Anti-DDoS、CFW、OBS、CTS、APIG、IPS、DBSS、DSC等服务日志数据时，安全云脑会将日志来源、时间戳等信息以Key-Value对的形式添加到日志中。

本章节将介绍各字段的含义。

- 通用字段：通用字段含义。
- sec-waf-attack：WAF攻击日志字段含义。
- sec-waf-access：WAF访问日志字段含义。
- sec-obs-access：OBS访问日志字段含义。
- sec-nip-attack：IPS攻击日志字段含义。
- sec-iam-audit：IAM审计日志字段含义。
- sec-hss-vul：HSS主机漏洞扫描结果字段含义。
- sec-hss-alarm：HSS主机安全告警字段含义。
- sec-hss-log：HSS主机安全日志字段含义。
- sec-ddos-attack：DDoS攻击日志字段含义。
- sec-cts-audit：CTS日志字段含义。
- sec-cfw-risk：CFW攻击事件日志字段含义。
- sec-cfw-flow：CFW流量日志字段含义。
- sec-cfw-block：CFW访问控制日志字段含义。
- sec-apig-access：API网关的访问日志字段含义。
- sec-dbss-alarm：DBSS告警日志字段含义。
- sec-dsc-alarm：DSC告警日志字段含义。
- sec-mtd-alarm：MTD告警日志字段含义。

通用字段

表 10-29 通用字段

字段名	字段类型	字段含义
__time	Date	日志产生的时间
__raw	String	原始日志

字段名	字段类型	字段含义
ops.source	String	数据源名称
ops.rgn	String	所属局点
ops.csvc	String	数据源(云服务)
ops.ver	String	数仓版本号
ops.hash	String	extend hash value of original 数据完整性验证
[src_/dest_]asset.domain.id	String	租户id
[src_/dest_]asset.domain.name	String	租户名
[src_/dest_]asset.id	String	资产id
[src_/dest_]asset.name	String	资产名称
[src_/dest_]asset.type	String	资产类型
[src./dest.]asset.region	String	资产局点
[src_/dest_]geo.ip	String	ip地址
[src_/dest_]geo.country	String	国家(中文)
[src_/dest_]geo.prov	String	省份（中文）
[src_/dest_]geo.city	String	城市名称（中文）
[src_/dest_]geo.org	String	注册IP的组织
[src_/dest_]geo.isp	String	运营商
[src_/dest_]geo.loc.lat	Float	纬度
[src_/dest_]geo.loc.lon	Float	经度
[src_/dest_]geo.tz	Integer	时区
[src_/dest_]geo.utc_off	Integer	时区
[src_/dest_]geo.cac	String	时区
[src_/dest_]geo.iddc	String	国际电话前缀码
[src_/dest_]geo.cc	String	国家编码ISO
[src_/dest_]geo.contc	String	大洲编码ISO
[src_/dest_]geo.idc	String	数据中心，机房

字段名	字段类型	字段含义
[src_/dest_]geo.bs	String	移动基站
[src_/dest_]geo.cc3	String	国家代码3位
[src_/dest_]geo.euro	String	欧盟成员国

sec-waf-attack

WAF攻击日志字段含义如下所示：

表 10-30 sec-waf-attack

字段	类型	字段含义
category	String	分类，此处值为“attack”。
time	Date	标识日志时间。
time_iso8601	Date	标识日志的 ISO 8601 格式时间。
policy_id	String	标识防护策略ID。
level	Integer	标识防护策略层级（1为宽松，2为中等，3为严格）。

字段	类型	字段含义
attack	String	标识攻击类型。攻击类型的解释为： ● default：默认 ● xss：跨站脚本攻击 ● sqli：SQL注入攻击 ● cmdi：命令注入攻击 ● lfi：本地文件包含 ● rfi：远程文件包含 ● webshell：WebShell攻击 ● robot：爬虫攻击（根据UA黑名单拦截） ● vuln：漏洞攻击 ● cc：命中CC规则 ● custom_custom：命中精准防护规则 ● custom_whiteip：命中白名单规则 ● custom_geoip：命中地理位置规则 ● illegal：非法请求 ● anticrawler：命中反爬虫规则（JS挑战） ● antitamper：命中防篡改规则 ● leakage：命中隐私泄露规则 ● followed_action：攻击惩罚 ● trojan：网站木马
action	String	标识处理动作。处理动作的解释为： ● block：拦截 ● log：仅记录 ● captcha：人机验证
rule	String	标识触发的规则ID或者自定义的策略类型描述。

字段	类型	字段含义
sub_type	String	当attack为robot时，该字段不为空。标识爬虫的子类型。 ● script_tool：脚本工具 ● search_engine：搜索引擎 ● scaner：扫描工具 ● uncategorized：其他爬虫
location	String	标识触发的payload的位置。
resp_headers	String	标识响应头。
resp_body	String	标识响应体。
hit_data	String	标识触发的payload字符串。
status	String	标识请求的响应状态码。
reqid	String	随机ID标识。
id	String	攻击 ID。
method	String	标识请求方法。
sip	String	标识客户端请求IP。
sport	String	标识客户端请求端口。
host	String	标识请求的服务器域名。
http_host	String	标识请求的服务器端口。
uri	String	标识请求URL。
header	String	标识请求header信息。
mutipart	String	标识请求multipart header（文件上传场景）。
cookie	String	标识请求cookie信息。
params	String	标识请求URI后的参数信息。
body_bytes_sent	String	标识发送给客户端的响应体字节数。
upstream_response_time	String	标识后端服务器响应时间。
process_time	String	标识引擎的检测用时。
engine_id	String	标识引擎的唯一标识。
group_id	String	用于对接LTS服务的日志组ID。
attack_stream_id	String	与group_id相关，是日志组下用户的access_stream的ID。

字段		类型	字段含义
hostid		String	标识防护域名 ID。
tenantid		String	标识防护域名的租户 ID。
projectid		String	标识防护域名的项目 ID。
backend		Object	标识请求转发的后端服务器地址。
backend	type	String	标识当前后端 Host 类型（IP或域名）。
	alive	String	标识当前后端状态。
	host	String	标识当前后端 Host 值。
	protocol	String	标识当前后端协议。
	port	Integer	标识当前后端端口。

sec-waf-access

WAF访问日志字段含义如表10-31所示。

表 10-31 sec-waf-access

字段	类型	字段含义
requestid	String	随机ID标识。
time	Date	标识日志时间。
eng_ip	String	标识引擎IP。
hostid	String	标识防护域名 ID。
tenantid	String	标识防护域名的租户 ID。
projectid	String	标识防护域名的项目 ID。
remote_ip	String	标识请求的客户端 IP。
scheme	String	标识请求协议类型。
response_code	String	标识请求响应码。
method	String	标识请求方法。
http_host	String	标识请求的服务器域名。
url	String	标识请求URL。
request_length	String	标识请求长度。
bytes_send	String	标识发送给客户端的总字节数。

字段	类型	字段含义
body_bytes_sent	String	标识发送给客户端的响应体字节数。
upstream_addr	String	标识选择的后端服务器地址。
request_time	String	标识请求处理时间，从读取客户端的第一个字节开始计时。
upstream_response_time	String	标识后端服务器响应时间。
upstream_status	String	标识后端服务器的响应码。
upstream_connect_time	String	标识后端服务器连接用时。
upstream_header_time	String	标识后端服务器接收到第一个响应头字节的用时。
bind_ip	String	标识引擎回源 IP。
engine_id	String	标识引擎的唯一标识。
time_iso8601	Date	标识日志的 ISO 8601 格式时间。
sni	String	标识通过 SNI 请求的域名。
tls_version	String	标识建立 SSL 连接的协议版本。
ssl_curves	String	标识客户端支持的曲线列表。
ssl_session_reused	String	标识 SSL 会话是否被重用。 ● 重用：r ● 未重用：.
process_time	String	标识引擎的检测用时。
x_forwarded_for	String	标识请求头中 X-Forwarded-For 的内容。
cdn_src_ip	String	标识请求头中 Cdn-Src-Ip 的内容。
x_real_ip	String	标识请求头中 X-Real-Ip 的内容。

sec-obs-access

对象存储服务访问日志字段含义如下所示：

表 10-32 sec-obs-access

字段	类型	字段含义
srcip	String	访问obs的源ip。

字段	类型	字段含义
srcport	String	访问obs的源端口。
logtime	Date	日志记录时间。
ces_log_version	String	内部请求为V0，V0不记录CES审计日志，V1记录CES审计日志。
request_start_time	String	请求开始时间。
ctx_request_id	String	请求ID，请求跟踪的唯一标识。
request_method	String	请求方法（get/post）。
remote_ip	String	客户端IP:端口。
operation	String	操作类型，如GET.OBJECT。
bucket_name	String	桶名。
object_name	String	对象名（文件名）。
query_string	String	请求query。
http_status	String	http请求状态码，如200。
content_length	String	请求内容长度。
user_agent	String	客户端agent。
storage_class	String	对象存储类型。
user_name	String	请求者用户名称。
user_id	String	请求者用户ID。
domain_name	String	请求者账号名称。
domain_id	String	请求者账号ID。
project_id	String	请求者项目ID。
owner_domain_name	String	桶owner租户名称。
owner_domain_id	String	桶owner租户ID。
owner_project_id	String	桶owner项目ID。
transmission_type	String	网络类型： ● 1：内网 ● 2：公网
scheme	String	网络协议。
http_version	String	http版本。
host	String	服务obs域名。
port	String	端口。

字段	类型	字段含义
auth_v2_v4	String	鉴权方式。
host_type	String	访问方式。
x_forwarded_for	String	代理客户端IP。
pub_bkt	String	是否为匿名访问桶。
pub_obj	String	是否为匿名访问对象。
website_req	String	是否为website请求。
crr_req	String	是否为crr请求。
huawei_cloud_service	String	是否为cdn请求。 ● CDN_F：认证失败 ● CDN：认证成功
batch_delete_success_count	String	批删成功个数。
ctc_log_urn	String	委托。
requester	String	委托账号。
is_over_write	String	是否为覆盖写。
error_code	String	错误原因。
detail_error_code	String	详细错误原因。
request_content_type	String	请求对象类型。
request_content_md5	String	请求对象md5。
total_bytes_received	String	接收到内容总数。
response_content_type	String	响应对象类型。
total_bytes_sent	String	发送内容总数响应头+响应BODY体。
referrer	String	引用页。
index_read_count	String	查询元数据表时延。
persistence_read_count	String	读数据的次数。
vpc_id	String	标识请求客户端所属的VPCID。
access_with_security_token	String	使用sts token。
copy_size	String	copy_size。
vpcep_traffic	String	走EP

字段	类型	字段含义
access_key	String	ak。

sec-nip-attack

IPS攻击日志字段含义如下所示：

表 10-33 sec-nip-attack

字段	类型	字段含义
SyslogId	String	日志序号。
Vsys	String	虚拟系统名称。
Policy	String	安全策略名称。
SrcIp	String	报文的源IP地址
DstIp	String	报文的目的IP地址
SrcPort	String	报文的源端口（对于ICMP报文，该字段为0）。
DstPort	String	报文的目的端口（对于ICMP报文，该字段为0）。
SrcZone	String	报文的源安全域。
DstZone	String	报文的目的安全域。
User	String	用户名。
Protocol	String	签名检测到的报文所属协议。
Application	String	签名检测到的报文所属应用。
Profile	String	配置文件的名称。
SignName	String	签名的名称。
SignId	String	签名的ID。
EventNum	String	日志归并引入字段，是否归并需根据归并频率及日志归并条件来确定，不发生归并则为1。
Target	String	签名所检测的报文所攻击的对象。具体情况如下： ● server：攻击对象为服务端。 ● client：攻击对象为客户端。 ● both：攻击对象为服务端和客户端。

字段	类型	字段含义
Severity	String	签名所检测的报文所造成攻击的严重性。具体情况如下： ● information：表示严重性为提示。 ● low：表示严重性为低。 ● medium：表示严重性为中。 ● high：表示严重性为高。
Os	String	签名所检测的报文所攻击的操作系统。具体情况如下： ● all：所有系统。 ● android：安卓系统。 ● ios：苹果系统。 ● unix-like：Unix系统。 ● windows：Windows系统。 ● other：其他系统。
Category	String	签名检测到的报文攻击特征所属的威胁分类。
Action	String	签名动作。 ● alert：签名动作为告警。 ● block：签名动作为阻断。
Reference	String	签名的参考信息。
Extend	String	增强模式下的取证字段。

sec-iam-audit

统一身份认证审计日志字段含义如下所示：

表 10-34 sec-iam-audit

字段	类型	字段含义
uid	String	用户id。
un	String	用户名。
did	String	租户id。
dn	String	租户名。
src	String	请求域名。
opl	String	操作级别。
op	String	操作类型。

字段	类型	字段含义
res	String	IAM服务调用结果。
ter	String	源ip。
dtl	String	iam认证详情。
tn	Date	发生时间。
ts	Long	iam服务调用的发生时间戳。
tid	String	traceid。
evnt	String	事件。
tobj	String	操作服务。

sec-hss-vul

主机漏洞扫描结果字段含义如下所示：

表 10-35 sec-hss-vul

字段	类型	字段含义
agentUuid	String	agent的UUID。
alarmCsn	String	告警UUID，master生成告警时随机生成。
alarmKey	String	告警关键字。对于告警，当前透传agent上报的信息msg_id；对于漏洞，由master生成。
alarmVersion	String	agent版本号。
occurTime	Int64	漏洞检测时间（ms）。
severity	Int32	HSS定义的漏洞等级。
hostUuid	String	受影响主机UUID。
hostName	String	受影响主机名。
hostIp	String	受影响主机通信IP。
ipList	String	受影响主机IP列表。
cloudId	String	cloudagent sn。
region	String	受影响主机所在区域。
projectId	String	受影响租户ID。
enterpriseProjectId	String	受影响企业租户ID。

字段		类型	字段含义
appendInfo		Object	漏洞详情。
appendInfo	vulId	String	漏洞官方ID。
	type	Int32	漏洞类型。 ● 0：linux ● 1：windows ● 2：webcms
	repairNecessity	Int32	漏洞修复必要性级别。 ● 1：低危 ● 2&3：中危 ● 4：高危
	status	Int32	保留字段。
	cve_ids	String	CVE ID列表，通过英文逗号连接。
	url	String	漏洞详情官网连接。
	vulNameEn	String	漏洞英文名。
	vulNameCn	String	漏洞中文名。
	severityLevel	String	漏洞危害级别，分为如下等级： ● Critical：严重 ● High：高 ● Medium：中 ● Low：低
	descriptionEn	String	漏洞英文描述。
	descriptionCn	String	漏洞中文描述。
	solutionEn	String	解决方案英文描述。
	solutionCn	String	解决方案中文描述。
	repairCmd	String	修复命令。
	needBoot	Int32	是否需要重启；当前默认1，暂时不用。
	errorInfo	String	修复失败原因。
	appName	String	存在漏洞的软件名（linux漏洞特有）。
	version	String	存在漏洞的软件版本（linux漏洞特有）。

字段		类型	字段含义
	createTime	Int64	首次检测时间（ms）。
	updateTime	Int64	漏洞修复时间（ms）；初始值同createTime。
	agentId	String	关联主机agent的UUID。
	projectId	String	受影响租户ID。

sec-hss-alarm

主机安全告警日志字段含义如下所示：

表 10-36 sec-hss-alarm

字段		类型	字段含义
agentUuid		String	agent的UUID。
alarmCsn		String	告警UUID。
alarmKey		String	告警关键字。对于告警，当前透传agent上报的信息msg_id；对于漏洞，由master生成。
alarmVersion		String	agent版本号。
occurTime		Long	事件发生时间（ms）。
severity		Long	风险等级。
hostUuid		String	受影响主机UUID。
hostName		String	受影响主机名。
hostIp		String	受影响主机通信IP。
ipList		String	受影响主机IP列表。
cloudId		String	cloudagent sn。
region		String	受影响主机所在区域。
projectId		String	受影响租户ID。
enterpriseProjectId		String	受影响企业租户ID。
appendInfo		Object	告警详情。
appendInfo	agent_id	String	AGENT ID。
	version	String	事件版本。
	container_name	String	容器ID（容器安全场景）。

字段		类型	字段含义
	image_name	String	镜像名称（容器安全场景）。
	event_id	String	事件ID，GUID。
	event_name	String	事件名称。
	event_classid	String	事件唯一标识。
	occur_time	Long	发生时间（秒）。
	recent_time	Long	最近一次发生时间（秒）。
	event_category	Integer	事件大类。
	event_type	Integer	事件类型。
	event_count	Integer	事件次数。
	severity	Integer	严重级别。
	attack_phase	Integer	攻击阶段。
	attack_tag	Integer	攻击标识。
	confidence	Integer	置信度。
	action	Integer	动作类型。
	detect_module	String	检测模块。
	report_source	String	上报源。
	related_events	String	相关事件ID。
	resource_info	Object	资源信息。
	network_info	Object	网络信息。
	app_info	Object	应用信息。
	system_info	Object	系统信息。
	process_info	list	进程信息。
	user_info	list	用户信息。
	file_info	list	文件信息。
	geo_info	Object	地理信息。
	malware_info	Object	恶意软件信息。
	forensic_info	String	取证字段。
	recommendation	String	处置建议。
	extend_info	String	事件扩展信息。

字段			类型	字段含义
	resource_info	project_id	String	项目ID。
		region_name	String	Region名称。
		vpc_id	String	VPC ID。
		host_name	String	主机名称。
		host_ip	String	主机IP。
		host_id	String	主机ID（ECS对应ID）。
		cloud_id	String	CloudAgent SN。
		vm_name	String	虚拟机名称。
		vm_uuid	String	虚拟机UUID。
		container_id	String	容器id。
		image_id	String	镜像id。
		sys_arch	String	系统CPU架构。
		os_bit	String	操作系统位数。
		os_type	String	操作系统类型。
		os_name	String	操作系统名称。
		os_version	String	操作系统版本。
	network_info	local_address	String	本地地址。
		local_port	Integer	本地端口。
		remote_address	String	远程地址。
		remote_port	Integer	远程端口。
		src_ip	String	源IP。
		src_port	Integer	源端口。
		src_domain	String	源域。
		dest_ip	String	目的IP。
		dest_port	Integer	目的端口。

字段			类型	字段含义
		dest_domain	String	目的域。
		protocol	String	协议。
		app_protocol	String	应用层协议。
		flow_direction	String	流量方向。
	app_info	sql	String	执行的sql语句。
		domain_name	String	DNS域名。
		url_path	String	URL路径。
		url_method	String	URL方法。
		req_refer	String	URL请求refer信息。
		email_subject	String	邮件主题。
		email_sender	String	邮件发送者。
		email_receiver	String	邮件接收者。
		email_keyword	String	邮件关键字。
	process_info	process_name	String	进程名称。
		process_path	String	进程文件路径。
		process_pid	Integer	进程id。
		process_uid	Integer	进程用户id。
		process_username	String	运行进程的用户名。
		process_cmdline	String	进程文件命令行。
		process_filename	String	进程文件名。

字段			类型	字段含义
		process_start_time	Long	进程启动时间。
		process_gid	Integer	进程组ID。
		process_egid	Integer	进程有效组ID。
		process_euid	Integer	进程有效用户ID。
		parent_process_name	String	父进程名称。
		parent_process_path	String	父进程文件路径。
		parent_process_pid	Integer	父进程id。
		parent_process_uid	Integer	父进程用户id。
		parent_process_cmdline	String	父进程文件命令行。
		parent_process_filename	String	父进程文件名。
		parent_process_start_time	Long	父进程启动时间。
		parent_process_gid	Integer	父进程组ID。
		parent_process_egid	Integer	父进程有效组ID。
		parent_process_euid	Integer	父进程有效用户ID。
		child_process_name	String	子进程名称。
		child_process_path	String	子进程文件路径。

字段			类型	字段含义
		child_process_pid	Integer	子进程id。
		child_process_uid	Integer	子进程用户id。
		child_process_cmdline	String	子进程文件命令行。
		child_process_filename	String	子进程文件名。
		child_process_start_time	Long	子进程启动时间。
		child_process_gid	Integer	子进程组ID。
		child_process_egid	Integer	子进程有效组ID。
		child_process_euid	Integer	子进程有效用户ID。
		virt_cmd	String	虚拟化命令。
		virt_process_name	String	虚拟化进程名称。
		escape mode	String	逃逸方式。
		escape cmd	String	逃逸后执行的命令。
	user_info	user_id	Integer	用户uid。
		user_gid	Integer	用户gid。
		user_name	String	用户名称。
		user_group_name	String	用户组名称。
		user_home_dir	String	用户home目录。
		login_ip	String	用户登录ip。
		service_type	String	登录的服务类型。

字段			类型	字段含义
		service_port	Integer	登录服务端口。
		login_mode	String	登录方式。
		login_last time	Long	用户最后一次登录时间。
		login_fail_count	Integer	用户登录失败次数。
		pwd_hash	String	口令hash。
		pwd_with_fuzzing	String	匿名化处理后的口令。
		pwd_used_days	Integer	密码使用的天数。
		pwd_min_days	Integer	口令的最短有效期限。
		pwd_max_days	Integer	口令的最长有效期限。
		pwd_warn_left_days	Integer	口令无效时提前告警天数。
	file_info	file_path	String	文件路径/名称。
		file_alias	String	文件别名。
		file_size	Integer	文件大小。
		file_mtime	Long	文件最后一次修改时间。
		file_atime	Long	文件最后一次访问时间。
		file_ctime	Long	文件最后一次状态改变时间。
		file_hash	String	文件hash。
		file_md5	String	文件md5。
		file_sha256	String	文件sha256。
		file_type	String	文件类型。
		file_content	String	文件内容。
		file_attr	String	文件属性。

字段			类型	字段含义
		file_operation	String	文件操作类型。
		file_change_attr	String	变更前后的属性。
		file_new_path	String	新文件路径。
		file_desc	String	文件描述。
		file_key_word	String	文件关键字。
		is_dir	Boolean	是否目录。
		fd_info	String	文件句柄信息。
		fd_count	Integer	文件句柄数量。
	forensic_info	monitor_process	String	监控进程。
		escape_mode	String	逃逸方式。
		abnormal_port	String	异常端口。
	geo_info	src_country	String	源国家。
		src_city	String	源城市。
		src_latitude	Long	源纬度。
		src_longitude	Long	源经度。
		dest_country	String	目的国家。
		dest_city	String	目的城市。
		dest_latitude	Long	目的纬度。
		dest_longitude	Long	目的经度。
	malware_info	malware_family	String	恶意家族。
		malware_class	String	恶意软件分类。

字段			类型	字段含义
	system_info	pwd_valid	Boolean	口令结果是否有效。
		pwd_min_len	Integer	口令长度。
		pwd_digit_credit	Integer	口令中数字要求。
		pwd_uppercase_letter	Integer	口令中大写字母。
		pwd_lowercase_letter	Integer	口令中小写字母。
		pwd_special_characters	Integer	口令中特殊字符。
	extend_info	hit_rule	String	特征规则。
		rule_name	String	规则名称。
		rulesetname	String	规则集名称。
		report_type	String	上报数据类型。
	ti_info	ti_source	String	情报来源。
		ti_class	String	情报分类。
		ti_threat_type	String	情报威胁类型。
		ti_first_time	Long	第一次发现时间。
		ti_last_time	Long	最近一次发现时间。

sec-hss-log

主机安全日志字段含义如下所示：

表 10-37 sec-hss-log

字段	类型	字段含义
agentUuid	String	agent的UUID。

字段		类型	字段含义
alarmCsn		String	告警UUID。
alarmKey		String	告警关键字。对于告警，当前透传agent上报的信息msg_id；对于漏洞，由master生成。
alarmVersion		String	agent版本号。
occurTime		Long	事件发生时间（ms）。
severity		Long	风险等级。
hostUuid		String	受影响主机UUID。
hostName		String	受影响主机名。
hostIp		String	受影响主机通信IP。
ipList		String	受影响主机IP列表。
cloudId		String	cloudagent sn。
region		String	受影响主机所在区域。
projectId		String	受影响租户ID。
enterpriseProjectId		String	受影响企业租户ID。
appendInfo		Object	告警详情。
appendInfo	agent_id	String	AGENT ID。
	version	String	事件版本。
	container_name	String	容器ID（容器安全场景）。
	image_name	String	镜像名称（容器安全场景）。
	event_id	String	事件ID，GUID。
	event_name	String	事件名称。
	event_classid	String	事件唯一标识。
	occur_time	Long	发生时间（秒）。
	recent_time	Long	最近一次发生时间（秒）。
	event_category	Integer	事件大类。
	event_type	Integer	事件类型。
	event_count	Integer	事件次数。
	severity	Integer	严重级别。
	attack_phase	Integer	攻击阶段。
	attack_tag	Integer	攻击标识。

字段			类型	字段含义
	confidence		Integer	置信度。
	action		Integer	动作类型。
	detect_module		String	检测模块。
	report_source		String	上报源。
	related_events		String	相关事件ID。
	resource_info		Object	资源信息。
	network_info		Object	网络信息。
	app_info		Object	应用信息。
	system_info		Object	系统信息。
	process_info		list	进程信息。
	user_info		list	用户信息。
	file_info		list	文件信息。
	geo_info		Object	地理信息。
	malware_info		Object	恶意软件信息。
	forensic_info		String	取证字段。
	recommendation		String	处置建议。
	extend_info		String	事件扩展信息。
	resource_info	project_id	String	项目ID。
		region_name	String	Region名称。
		vpc_id	String	VPC ID。
		host_name	String	主机名称。
		host_ip	String	主机IP。
		host_id	String	主机ID（ECS对应ID）。
		cloud_id	String	CloudAgent SN。
		vm_name	String	虚拟机名称。
		vm_uuid	String	虚拟机UUID。
		container_id	String	容器id。
		image_id	String	镜像id。

字段			类型	字段含义
		sys_arch	String	系统CPU架构。
		os_bit	String	操作系统位数。
		os_type	String	操作系统类型。
		os_name	String	操作系统名称。
		os_version	String	操作系统版本。
	network_info	local_address	String	本地地址。
		local_port	Integer	本地端口。
		remote_address	String	远程地址。
		remote_port	Integer	远程端口。
		src_ip	String	源IP。
		src_port	Integer	源端口。
		src_domain	String	源域。
		dest_ip	String	目的IP。
		dest_port	Integer	目的端口。
		dest_domain	String	目的域。
		protocol	String	协议。
		app_protocol	String	应用层协议。
		flow_direction	String	流量方向。
	app_info	sql	String	执行的sql语句。
		domain_name	String	DNS域名。
		url_path	String	URL路径。
		url_method	String	URL方法。
		req_refer	String	URL请求refer信息。

字段			类型	字段含义
		email_subject	String	邮件主题。
		email_sender	String	邮件发送者。
		email_receiver	String	邮件接收者。
		email_keyword	String	邮件关键字。
	process_info	process_name	String	进程名称。
		process_path	String	进程文件路径。
		process_pid	Integer	进程id。
		process_uid	Integer	进程用户id。
		process_username	String	运行进程的用户名。
		process_cmdline	String	进程文件命令行。
		process_filename	String	进程文件名。
		process_start_time	Long	进程启动时间。
		process_gid	Integer	进程组ID。
		process_egid	Integer	进程有效组ID。
		process_euid	Integer	进程有效用户ID。
		parent_process_name	String	父进程名称。
		parent_process_path	String	父进程文件路径。
		parent_process_pid	Integer	父进程id。

字段			类型	字段含义
		parent_process_uid	Integer	父进程用户id。
		parent_process_cmdline	String	父进程文件命令行。
		parent_process_filename	String	父进程文件名。
		parent_process_start_time	Long	父进程启动时间。
		parent_process_gid	Integer	父进程组ID。
		parent_process_egid	Integer	父进程有效组ID。
		parent_process_euid	Integer	父进程有效用户ID。
		child_process_name	String	子进程名称。
		child_process_path	String	子进程文件路径。
		child_process_pid	Integer	子进程id。
		child_process_uid	Integer	子进程用户id。
		child_process_cmdline	String	子进程文件命令行。
		child_process_filename	String	子进程文件名。
		child_process_start_time	Long	子进程启动时间。
		child_process_gid	Integer	子进程组ID。
		child_process_egid	Integer	子进程有效组ID。

字段			类型	字段含义
		child_process_euid	Integer	子进程有效用户ID。
		virt_cmd	String	虚拟化命令。
		virt_process_name	String	虚拟化进程名称。
		escape mode	String	逃逸方式。
		escape cmd	String	逃逸后执行的命令。
	user_info	user_id	Integer	用户uid。
		user_gid	Integer	用户gid。
		user_name	String	用户名称。
		user_group_name	String	用户组名称。
		user_home_dir	String	用户home目录。
		login_ip	String	用户登录ip。
		service_type	String	登录的服务类型。
		service_port	Integer	登录服务端口。
		login_mode	String	登录方式。
		login_last time	Long	用户最后一次登录时间。
		login_fail_count	Integer	用户登录失败次数。
		pwd_hash	String	口令hash。
		pwd_with_fuzzing	String	匿名化处理后的口令。
		pwd_used_days	Integer	密码使用的天数。
		pwd_min_days	Integer	口令的最短有效期限。
		pwd_max_days	Integer	口令的最长有效期限。

字段			类型	字段含义
		pwd_warn_left_days	Integer	口令无效时提前告警天数。
	file_info	file_path	String	文件路径/名称。
		file_alias	String	文件别名。
		file_size	Integer	文件大小。
		file_mtime	Long	文件最后一次修改时间。
		file_atime	Long	文件最后一次访问时间。
		file_ctime	Long	文件最后一次状态改变时间。
		file_hash	String	文件hash。
		file_md5	String	文件md5。
		file_sha256	String	文件sha256。
		file_type	String	文件类型。
		file_content	String	文件内容。
		file_attr	String	文件属性。
		file_operation	String	文件操作类型。
		file_change_attr	String	变更前后的属性。
		file_new_path	String	新文件路径。
		file_desc	String	文件描述。
		file_key_word	String	文件关键字。
		is_dir	Boolean	是否目录。
		fd_info	String	文件句柄信息。
		fd_count	Integer	文件句柄数量。
	forensic_info	monitor_process	String	监控进程。
		escape_mode	String	逃逸方式。

字段			类型	字段含义
		abnormal_port	String	异常端口。
	geo_info	src_country	String	源国家。
		src_city	String	源城市。
		src_latitude	Long	源纬度。
		src_longitude	Long	源经度。
		dest_country	String	目的国家。
		dest_city	String	目的城市。
		dest_latitude	Long	目的纬度。
		dest_longitude	Long	目的经度。
	malware_info	malware_family	String	恶意家族。
		malware_class	String	恶意软件分类。
	system_info	pwd_valid	Boolean	口令结果是否有效。
		pwd_min_len	Integer	口令长度。
		pwd_digit_credit	Integer	口令中数字要求。
		pwd_uppercase_letter	Integer	口令中大写字母。
		pwd_lowercase_letter	Integer	口令中小写字母。
		pwd_special_characters	Integer	口令中特殊字符。
	extend_info	hit_rule	String	特征规则。
		rule_name	String	规则名称。

字段			类型	字段含义
		rulesetname	String	规则集名称。
		report_type	String	上报数据类型。
	ti_info	ti_source	String	情报来源。
		ti_class	String	情报分类。
		ti_threat_type	String	情报威胁类型。
		ti_first_time	Long	第一次发现时间。
		ti_last_time	Long	最近一次发现时间。

sec-ddos-attack

DDoS攻击日志字段含义如下所示：

表 10-38 sec-ddos-attack

字段	类型	字段含义
log_type	String	日志类型。
time	Date	本地时间。
device_ip	String	设备IP。
device_type	String	设备类型（清洗：CLEAN；检测：DETECT）。
direction	String	日志方向（inbound，outbound）。
zone_id	String	防护对象ID。
zone_name	String	防护对象名称。
zone_ip	String	IP。
biz_id	String	业务ID。
is_deszone	String	是否网段流量（是：true；否：false）。
is_ipLocation	String	是否地址位置流量（是：true，否：false）。
ipLocation_id	String	地理位置ID。

字段	类型	字段含义
total_pps	String	总pps。
total_kbps	String	总Kbps。
tcp_pps	String	到目标的TCP总包速率pps。
tcp_kbps	String	到目标的TCP总流量Kbps。
tcpfrag_pps	String	到目标的TCP碎片包速率pps。
tcpfrag_kbps	String	到目标的TCP碎片流量Kbps。
udp_pps	String	到目标的UDP总包速率pps。
udp_kbps	String	到目标的UDP总流量Kbps。
udpfrag_pps	String	到目标的UDP碎片包速率pps。
udpfrag_kbps	String	到目标的UDP碎片流量Kbps。
icmp_pps	String	到目标的ICMP总包速率pps。
icmp_kbps	String	到目标的ICMP总流量Kbps。
other_pps	String	到目标的Other总包速率pps。
other_kbps	String	到目标的Other总流量Kbps。
syn_pps	String	到目标的SYN报文数。
synack_pps	String	到目标的SYN/ACK报文数pps。
ack_pps	String	到目标的ACK报文数pps。
finrst_pps	String	到目标的FIN/Rst报文数pps。
http_pps	String	到目标的HTTP总包速率pps。
http_kbps	String	到目标的HTTP总流量Kbps。
http_get_pps	String	到目标的HTTP请求总包速率pps。
https_pps	String	到目标的HTTPS总包速率pps。
https_kbps	String	到目标的HTTPS总流量Kbps。
dns_request_pps	String	到目标业务DNS Query包速率pps。
dns_request_kbps	String	到目标业务DNS Query总流量Kbps。
dns_reply_pps	String	到目标业务DNS Reply包速率pps。
dns_reply_kbps	String	到目标业务DNS Reply总流量Kbps。
sip_invite_pps	String	到目标业SIP包速率pps。
sip_invite_kbps	String	到目标业务SIP总流量Kbps。
tcp_increase_con	String	到目标的tcp每秒新建连接数统计。

字段	类型	字段含义
udp_increase_con	String	到目标的udp每秒新建连接数统计。
icmp_increase_con	String	到目标的icmp每秒新建连接数统计。
other_increase_con	String	到目标的other协议每秒新建连接数统计。
tcp_concur_con	String	到目标的tcp并发连接数统计。
udp_concur_con	String	到目标的udp并发连接数统计。
icmp_concur_con	String	到目标的icmp并发连接数统计。
other_concur_con	String	到目标的other协议并发连接数统计。
total_average_pps	String	到目标的所有流量的平均pps。
total_average_kbps	String	到目标的所有流量的平均Kbps。

sec-cts-audit

云审计服务日志字段含义如下所示：

表 10-39 sec-cts-audit

字段	类型	字段含义
time	Date	事件发生时间。以当地标准时间（采用格林威治时间加当地时区形式）进行展示，例如：2022/11/08 11:24:04 GMT+08:00。
user	Object	发起操作的云账户信息。
request	Object	操作的请求内容。
response	Object	操作的响应内容。
service_type	String	操作来源。
resource_type	String	资源类型。
resource_name	String	资源名称。
resource_id	String	资源的唯一标识。
source_ip	String	发起本次操作的用户的IP，如果为系统内调用，则为空。
trace_name	String	操作名称。

字段	类型	字段含义
trace_rating	String	操作事件等级，分为以下等级： ● normal：代表本次操作成功。 ● warning：代表本次操作失败。 ● incident：代表本次操作引起了比失败更严重的后果，比如会造成节点故障或用户业务故障等情况。
trace_type	String	操作类型，分为以下几种： ● ConsoleAction：表示通过管理控制台执行的操作。 ● SystemAction：表示系统内部触发的操作。 ● ApiCall：表示调用ApiGateway触发的操作。 ● ObsSDK：表示通过调用OBS 提供的SDK 触发的关于OBS桶相关操作。 ● Others：表示除去通过“ObsSDK”触发的关于OBS桶相关的操作。
api_version	String	作为操作来源的云服务的API版本号。
message	Object	备注信息。
record_time	Long	记录操作的时间，表示方式为时间戳。
trace_id	String	操作的唯一标识。
code	Integer	事件http返回码，例如200，400。
request_id	String	记录本次请求的request id。
location_info	String	记录本次请求出错后，问题定位所需要的辅助信息。
endpoint	String	该操作涉及云资源的详情页面的endpoint。
resource_url	String	该操作涉及云资源的详情页面的访问链接（不含endpoint）。
user_agent	String	OBS桶相关操作中非ObsSDK方式调用时的操作类型。
content_length	Long	OBS桶相关操作中请求消息体的长度。
total_time	Long	OBS桶相关操作中请求的响应时间。

sec-cfw-risk

云防火墙攻击事件日志字段含义如下所示：

表 10-40 sec-cfw-risk

字段	类型	字段含义
event_time	Date	检测到的攻击时间。
action	String	云防火墙当前的响应动作。 ● permit：放行 ● deny：阻断
app	String	应用类型。
attack_rule	String	检测到攻击的防御规则。
attack_rule_id	String	检测到攻击的防御规则ID号。
attack_type	String	发生攻击的类型： ● Vulnerability Exploit Attack：漏洞攻击 ● Vulnerability Scan：漏洞扫描 ● Trojan：木马病毒 ● Worm：蠕虫病毒 ● Phishing：网络钓鱼攻击 ● Web Attack：Web攻击 ● Application DDoS：DDoS攻击 ● Buffer Overflow：缓冲区溢出攻击 ● Password Attack：密码攻击 ● Mail：邮件相关类型的攻击行为 ● Access Control：访问控制行为 ● Hacking Tool：黑客工具 ● Hijacking：劫持行为 ● Protocol Exception：存在异常协议 ● Spam：存在垃圾邮件 ● Spyware：存在间谍软件 ● DDoS Flood：DDoS泛洪攻击 ● Suspicious DNS Activity：可疑DNS活动 ● Other Suspicious Behavior：其他可疑行为
dst_ip	String	目的IP地址。
dst_port	String	目的端口号。
packet	String	攻击日志的原始数据包。
protocol	String	协议类型。

字段	类型	字段含义
level	String	表示检测到威胁的等级： ● CRITICAL：严重 ● HIGH：高 ● MIDDLE：中 ● LOW：低
source	String	检测到攻击的防御模式： ● 0：基础防御 ● 1：虚拟补丁
src_ip	String	源IP地址。
src_port	String	源端口号。
direction	String	流量方向： ● out2in：入方向 ● in2out：出方向

sec-cfw-flow

云防火墙流量日志字段含义如下所示：

表 10-41 sec-cfw-flow

字段	类型	字段含义
app	String	应用类型。
dst_ip	String	目的IP地址。
dst_port	String	目的端口号。
end_time	Date	流结束时间。
protocol	String	协议类型。
to_c_bytes	String	服务端向客户端发送的字节数。
to_c_pkts	String	服务端向客户端发送的报文数。
to_s_bytes	String	客户端向服务端发送的字节数。
to_s_pkts	String	服务端向客户端发送的报文数。
src_ip	String	源IP地址。
src_port	String	源端口号。
start_time	Date	流开始时间。

sec-cfw-block

云防火墙访问控制日志字段含义如下所示：

表 10-42 sec-cfw-block

字段	类型	字段含义
hit_time	Date	访问发生的时间。
action	String	云防火墙当前的响应动作： ● permit：放行 ● deny：阻断
app	String	应用类型。
dst_ip	String	目的IP地址。
dst_port	String	目的端口号。
protocol	String	协议类型。
rule_id	String	触发规则的ID。
src_ip	String	源IP地址。
src_port	String	源端口号。

sec-apig-access

API网关访问日志字段含义如下所示：

表 10-43 sec-apig-access

字段	类型	字段含义
region_id	String	局点。
api_id	String	API ID。
body_bytes_sent	String	返回Body大小。
bytes_sent	String	整个返回大小。
domain	String	公网域名。
errorType	String	是否被流控（1：被流控）。
http_user_agent	String	用户代理标识。
http_x_forwarded_for	String	X-Forwarded-For头。
opsuba_api_url	String	请求的URI。
out_times	String	网关内部与周边组件交互耗时。

字段	类型	字段含义
remote_addr	String	远端ip。
request_id	String	请求id。
request_length	String	整个请求大小。
request_method	String	HTTP请求方法。
request_time	String	访问耗时。
scheme	String	协议。
server_protocol	String	请求协议。
status	String	状态。
time_local	Date	时间。
upstream_addr	String	远端ip。
upstream_connect_time	String	远端连接耗时。
upstream_header_time	String	远端头耗时。
upstream_response_time	String	远端返回耗时。
upstream_status	String	远端状态。
upstream_uri	String	请求后端的URI。
user_name	String	用户projectid或appid。

sec-dbss-alarm

DBSS告警日志字段含义如下所示：

表 10-44 dbss-alarm

字段	类型	字段含义
domain_id	String	账号ID。
project_id	String	项目ID。
region	String	region
tenant_vpc_id	String	租户的VPC ID。
tenant_subnet_id	String	租户的子网ID。
instance_id	String	实例ID。

字段		类型	字段含义
instance_name		String	实例名。
alarm		Object	告警对象。
source_type		String	dbss。
alarm	alarm_risk	String	告警等级。
	client_ip	String	连接IP。
	database_ip	String	数据库访问IP。
	count	Long	告警次数。
	user_name	String	数据库用户名。
	schema	String	oracle schema。
	rule_name	String	规则名称。
	rule_id	String	规则ID。
	sql_type	String	SQL执行类型。
	sql_result	String	SQL执行结果。
	db_type	String	数据库类型。

sec-dsc-alarm

DSC告警日志的保留字段根据日志类型有所不同，具体如下：

表 10-45 AK SK 泄露（ aksk_leakage ）

字段	类型	字段含义
log_type	String	告警类型。
region_id	String	region。
domain_id	String	账号ID。
project_id	String	项目id。
leakage_ak	String	AK。
source	String	泄漏源。
find_time	String	发现时间。
account	String	账号名。
file_name	String	文件名。
file_suffix	String	文件后缀。

字段	类型	字段含义
leakage_user_id	String	泄露子用户ID。
leakage_user_name	String	泄露子用户名。
leakage_domain_id	String	泄露主账号ID。
leakage_domain_name	String	泄露主账号名。
url	String	泄露网址。

表 10-46 风险 OBS 桶文件（obs_risk）

字段	类型	字段含义
log_type	String	告警类型。
region_id	String	region。
domain_id	String	账号ID。
project_id	String	项目id。
bucket_policy	String	公开桶/私有桶。
bucket_domain_id	String	桶所属账号ID。
bucket_project_id	String	桶所属项目ID。
bucket_name	String	桶名称。
file_name	String	文件名称。
file_path	String	文件路径。
risk_level	Integer	敏感风险等级。
sensitive_data_type	String[]	敏感数据类型。
privacy_detail	String	个人隐私数据明细。
file_type	String	文件类型。
mimetypes	String	文件类型。
rule_list	List<Map<String,String>>	匹配规则列表。
keyword	String	匹配敏感数据规则关键字。
available_zone	String	可用区。
encrypted	String	是否加密。

表 10-47 数据敏感字段信息（db_risk）

字段	类型	字段含义
log_type	String	告警类型。
region_id	String	region。
domain_id	String	账号ID。
project_id	String	项目id。
vpc_id	String	VPC ID。
db_instance_type	String	RDS PUB。
db_instance_id	String	数据库实例ID。
db_instance_type	String	数据库实例类型。
db_instance_ip	String	数据库实例IP。
db_instance_domain_id	String	数据库实例所属账号ID。
db_instance_project_id	String	数据库实例所属项目ID。
db_instance_name	String	数据库实例名称。
db_name	String	数据库名称。
table_name	String	表名称。
field_name	String	字段名称。
data_type	String	字段数据类型。
risk_level	Integer	敏感风险等级。
sensitive_data_type	String[]	敏感数据类型。
privacy_detail	String	个人隐私数据明细。
rule_list	List<Map<String,String>>	匹配规则列表。
keyword	String	匹配敏感数据规则关键字。

sec-mtd-alarm

MTD告警日志字段含义如下所示：

表 10-48 sec-mtd-alarm

字段		类型	字段含义
version		String	事件对象的版本，该字段的值必须为服务确定的官方发布版本之一。 在当前版本中，事件对象格式的版本为1.2.0。
environment		Object	事件产生的环境坐标信息。
environment	type	string	环境供应商。
	domain_id	string	HWC special，域名ID。
	region_id	string	HWC special，区域ID。
	project_id	string	HWC special，项目ID。
data_source		Object	数据源。
data_source	type	Int	数据源类型。取值范围如下： ● 1：华为产品 ● 2：第三方产品 ● 3：租户私有产品
	domain_id	String	数据源产品所属账号的ID，最大36个字符。
	project_id	String	数据源产品所属项目的ID，最大36个字符。
	region_id	String	数据源产品所在区域，具体取值范围查看华为云地区和终端节点定义，例如cn-north-4a。
	company_name	String	数据源产品所属公司的名称，最大16个字符。
	product_name	String	数据源产品的名称，最大24个字符。
	product_feature	String	产品功能特性名称，用来指明检测到当前事件的产品的功能特性，最大24个字符。
first_observed_time		Timestamp	首次发现时间，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。

字段		类型	字段含义
last_observed_time		Timestamp	最近发现时间，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。
create_time		Timestamp	记录时间，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	接收时间，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。
event_id		String	事件唯一标识，UUID格式，最大36个字符。
title		String	事件标题，最大255字符。
title_en		String	事件标题英文，最大255字符。
title_zh		String	事件标题中文，最大255字符。
description		String	事件描述信息，最大1024个字符。
source_url		String	事件URL链接，指向数据源产品中有关当前事件说明的页面。
count		Int	事件发生次数。
confidence		Int	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。
severity		Object	严重性。
severity	label	String	严重性等级，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。

字段		类型	字段含义
	normalize_score	Int	严重性评分，取值范围：0-100。与严重性等级的对应关系： ● TIPS：0 ● LOW：1-39 ● MEDIUM：40-69 ● HIGH：70-89 ● FATAL：90-100
	original_score	Int	严重性原始评分，指在数据源产品中的评分。
criticality		Int	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。
type		Object	事件分类。
type	business	String	安全运营过程，弱点的分类维度 事件所属业务领域标签，可选类别如下： ● attack：攻击 ● vulnerability：漏洞 ● compliance check：合规检查 ● risk：风险 ● public opinion：舆情 ● illegal&violation：违法违规 ● security bulletin：公告
	namespace	String	安全运营过程，弱点的分类维度。 事件所属业务领域标签，可选类别如下： ● attack：攻击 ● vulnerability：漏洞 ● compliance check：合规检查 ● risk：风险 ● public opinion：舆情 ● illegal&violation：违法违规 ● security bulletin：公告

字段		类型	字段含义
	category	String	类别，推荐使用预定义的类型分类。
	classifier	String	分类器，推荐使用预定义的分类器。如果指定了分类器，则必须指定类别。
	tech_domain	String	技术领域标签： ● OS：主机 ● APP：应用 ● NET：网络 ● CS：云服务 ● CSP：平台云服务
	properties	Object	见对象type.properties
type.properties	killchain	String	Kill chain事件分类，仅当namespace为ATTACK有效。
	ttps	String	Mitre Array 事件分类，仅当namespace为ATTACK有效。
	effects	String	影响，全部类型。
compliance		Object	合规检查信息。
compliance	checkitem_id	String	检查项（检查规则）编号。
	checkpoint_id	String	检查点（检查结果）编号，检查项对同一个资源的检查结果。
	spec_id	String	检查规范编号，默认选第一个。
	reason	String	原因。
	status	String	合规检查结果，取值定义： ● QUALIFIED：没有失败的，也没有有风险的就是合格的。 ● RISK：没有失败的，但是只要有一个有风险的就是有风险的。 ● FAILED：只要有一个失败的就是失败。
	properties	Object	主机基线字段全量维持（不固定，包含主机基线和sa基线）。
network		Object	网络信息。

字段		类型	字段含义
network	direction	String	方向，取值范围：IN | OUT
	protocol	String	协议。
	src_ip	String	源IP地址。
	src_port	int	源端口，0–65535。
	src_domain	String	源域名，最大128个字符。
	src_geo	Object	源IP的地理位置信息。
	dest_ip	String	目标IP地址。
	dest_port	int	目标端口，0–65535。
	dest_domain	String	目标域名，最大128个字符。
	dest_geo	Object	目标IP的地理位置信息。
geo	latitude	Float	纬度。
	longitude	Float	经度。
	city_code	String	城市编码。
	country_code	String	国家简码ISO。
vulnerability_patch		Object	漏洞补丁信息。
vulnerability_patch	patch_id	String	补丁编号。
	patch_name	String	补丁名称。
	type	String	补丁类型。 ● 0：linux ● 1：windows ● 2：web-cms
	major_level	String	重要等级。
	status	String	补丁状态。
	release_time	Timestamp	发布时间，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。
	repair_cmd	String	修复命令。
	repair_necessity	Int	修复必要程度。 ● 1：需立刻修复 ● 2：可延后修复 ● 3：暂可以不修复

字段		类型	字段含义
	vendor_name	String	漏洞报告提供者信息（厂商）。
	vulnerable_package	String	受影响软件版本列表。
	reference_url	String	参考链接。
	cve_ids	String	漏洞列表。
malware		Object	恶意软件。
malware	name	String	恶意软件名称，最大64个字符。
	sha256	String	恶意软件sha256。
	type	String	恶意软件类型，遵循STIX规范： adware|backdoor|bot|bootkit|ddos|downloader|dropper|exploit-kit|keylogger|ransomware|remote-access-trojan|resource-exploitation|rogue-security-software|rootkit|screen-capture|spyware|trojan|unknown|virus|webshell|wiper|worm
	path	String	恶意软件在系统中的路径，最大512个字符（包含软件名称）。
	state	String	恶意软件状态，取值范围： OBSERVED | REMOVAL_FAILED | REMOVED。
	properties	Object	见对象malware.properties。
malware.properties	pid	String	进程ID。
	user	String	系统角色（例如：root，service）。
	mod	String	系统权限（例如：777，755）。
	start_time	String	进程启动时间，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。
threat_intel		Object	威胁情报。

字段		类型	字段含义
threat_intel	id	String	情报ID。
	indicator_type	String	威胁情报类型。
	labels	String	标签。
	confidence	Int	置信度，不同来源目前置信度分值定义不一样（分数）。
	information_source	String	威胁情报源。
	severity	Int	严重程度，不同渠道定义值不一样（分数）。
	value	String	威胁情报指标值，最大512个字符，如：ip、url、domain等。
	description_en	string	威胁情报描述-英文。
	description_zh	String	威胁情报描述-中文。
	description	String	威胁情报描述。
	modified	Timestamp	威胁情报的更新时间，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。
	valid_from	String	有效期开始（可读字符串）。
	valid_until	String	有效期结束（可读字符串）。
	properties	Object	见对象threat_intel.properties。
threat_intel.properties	file_md5	String	恶意软件Md5。
	file_sha1	String	恶意软件Sha1。
	file_sha256	String	恶意软件Sha256值。
	file_name	String	文件名称。
	create_time	Timestamp	编译时间。
	file_class	String	文件类别，TEXT、XCODE。
	file_family	String	家族，例如：wannacry（勒索软件）。
	file_maltype	String	类别，例如：trojan（特洛伊）。

字段		类型	字段含义
	ip_resolves_to_refs	String	mac地址。
	belongs_to_refs	String	IP AS 自治系统
	ip_location	String	地区。格式：country/province/city/lngwgs/latwgs。
	domain_family	String	域名家族。
	domain_resolves_to_refs	String	解析的IP地址。
	domain_dns_type	String	DNS类别。
	url_host	String	URL地址。
	url_resolves_to_refs	String	IP地址。
	display_name	String	显示名称。
	url_belongs_to_ref	String	邮箱账户，@之前部分。
resource		Object	受影响资源。
resource	id	String	云服务资源ID。
	name	String	资源名称；最大长度255个字符。
	type	String	资源类型，引用RMS type字段。
	provider	String	云服务名称，引用RMS provider字段。
	region_id	String	区域。
	domain_id	String	资源所属账号ID，UUID。
	project_id	String	资源所属项目ID，UUID。
	ep_id	String	企业项目id。
	ep_name	String	企业项目名称。
	tags	Object	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,+, -, =, ., _, :, /,@

字段		类型	字段含义
remediation		Object	补救措施。
remediation	recommendation_zh	String	推荐处理方法-中文。
	recommendation_en	String	推荐处理方法-英文。
	recommendation	String	推荐处理方法。
	url	String	链接，指向该事件的一般修复信息。该URL必须可以从公网访问，不需要提供凭证。

data_source_fields		Object	数据源自定义信息，最多支持50个key/value对，约束条件：
			● 该对象不能包含冗余数据，并且不能与已定义的事件格式字段冲突。
			● 字段名称可以包含字母数字字符、空格和以下符号：_ . / = + \ - @。
			示例：
			"data_source_fields": {
			"key1": "value1",
			"key2", "value2",
			}

verification_state		String	验证状态，标识事件的准确性。可选类型如下： ● Unknown：未知 ● True_Positive：确认 ● False_Positive：误报 默认填写Unknown。
handle_status		String	事件处理状态，可选类型如下： ● New：未知 ● Ignored：忽略 ● Resolved：已解决 默认填写New。
phase		String	阶段：Preparation|Detection and Analysis|Containment，Eradication& Recovery| Post-Incident-Activity

字段	类型	字段含义
sla	Int	约束闭环时间，单位：天。设置风险接受持续时间。

10.5.4 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。

约束与限制

仅自定义新增的管道支持自定义配置索引，新增管道详细操作请参见**创建管道**。

配置字段索引

步骤1 登录管理控制台。

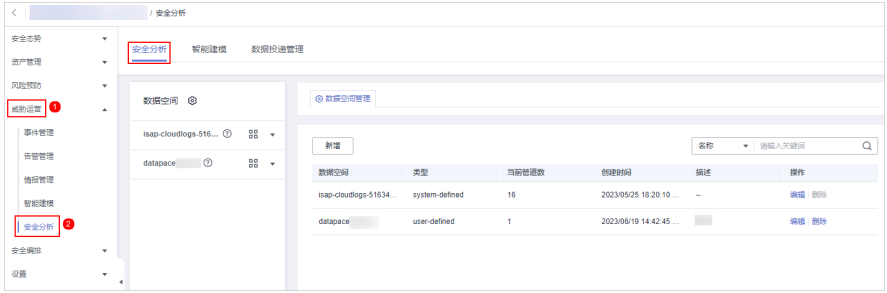
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-60 进入目标工作空间管理页面

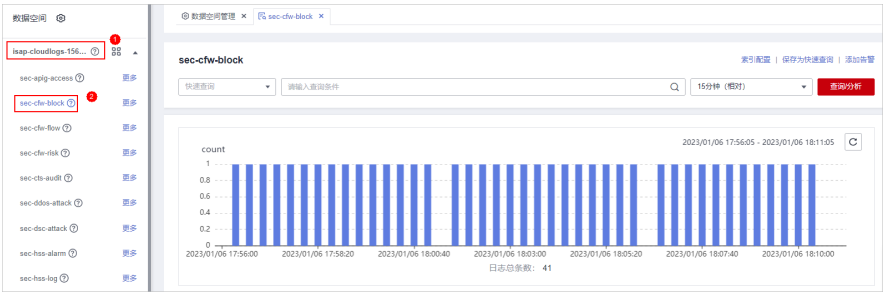
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-61 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 10-62 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10-49所示。

表 10-49 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

10.5.5 查询与分析

操作场景

数据收集成功后，您可以在查询分析页面对收集到的日志数据进行实时查询分析。

本章节将介绍如何对日志数据进行查询分析，请根据您的需要选择查询分析方式：

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

前提条件

已完成数据接入，详细操作请参见数据集成。

输入查询条件进行查询分析

步骤1 登录管理控制台。

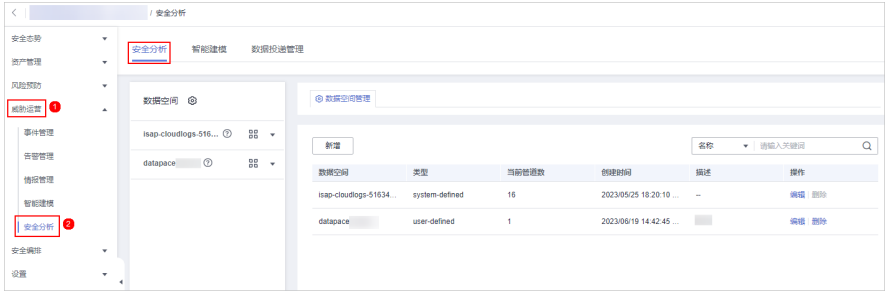
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

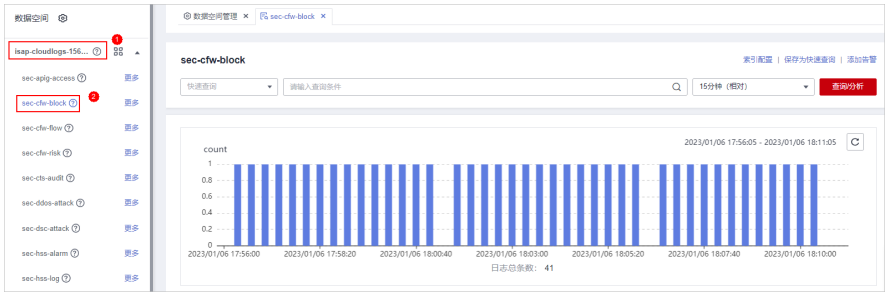
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-64 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 10-65 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-SQL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 10-66 查询与分析

步骤7 单击“15分钟（相对）”，设置查询时间范围。

您可以选择相对时间（15分钟、1小时、24小时），或自定义查询时间。

步骤8 单击“查询/分析”，查看查询分析结果。

----结束

使用已有字段进行查询分析

本部分将介绍如何使用已有字段对接入日志进行查询分析。

步骤1 登录管理控制台。

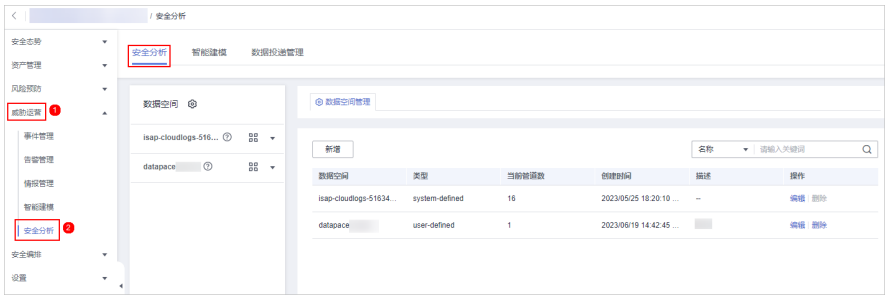
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-67 进入目标工作空间管理页面

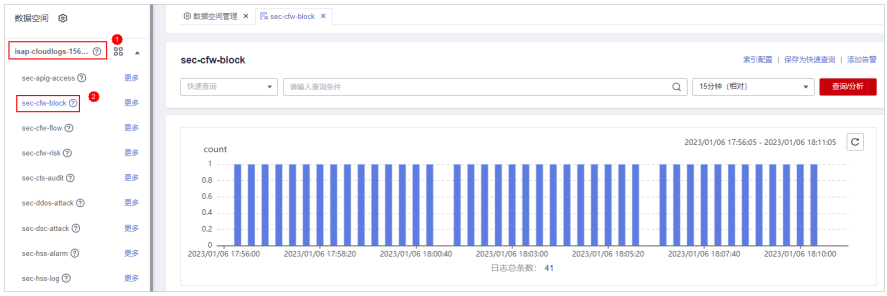
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-68 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 10-69 管道数据页面



步骤6 设置查询条件。

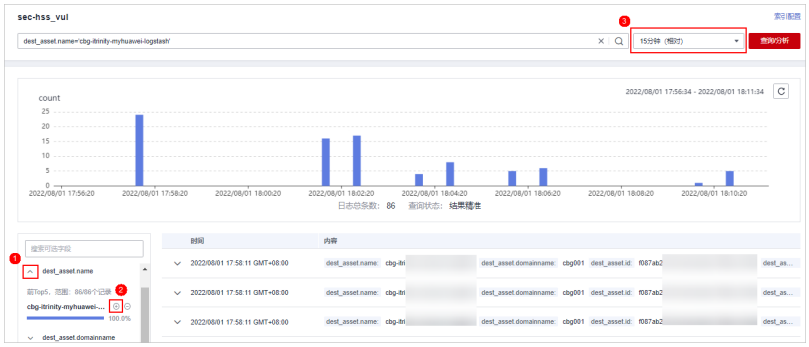
接入数据已有字段详细说明请参见日志字段含义。

说明

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

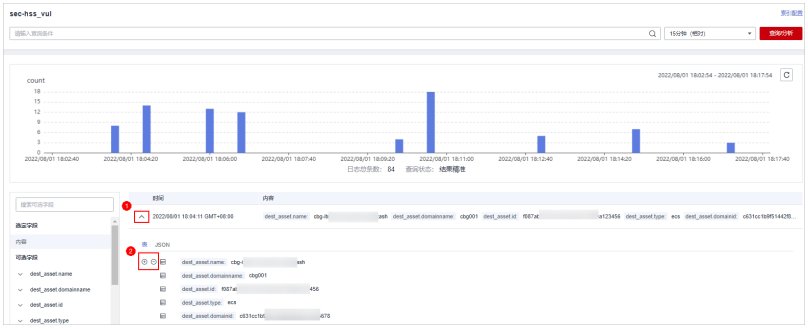
- 单击左侧可选字段前的 ，并单击待筛选或待排查字段名称后的（筛选某字段值）或（排除某字段值），查询框中将按照已筛选或排查的字段进行查询。

图 10-70 筛选某字段值（一）



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

图 10-71 筛选某字段值（二）



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

----结束

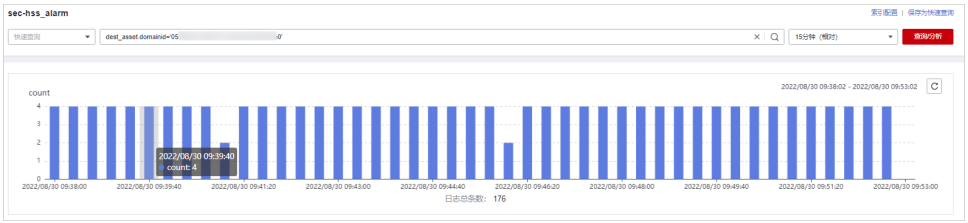
操作查询分析结果

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。

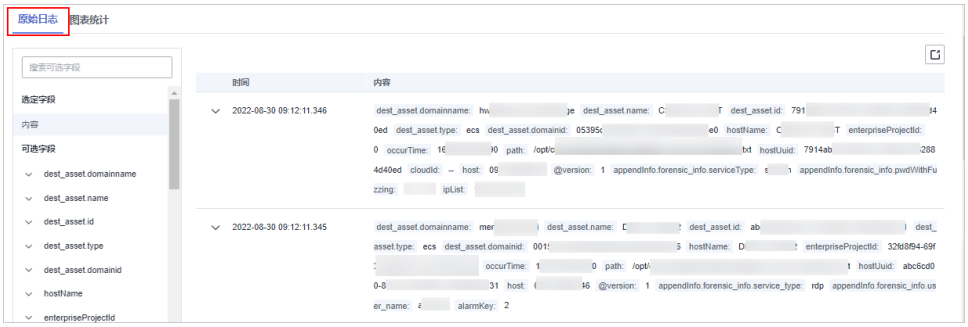
图 10-72 日志分布直方图



- **原始日志**

  在“原始日志”页签将展示当前查询结果。

图 10-73 原始日志



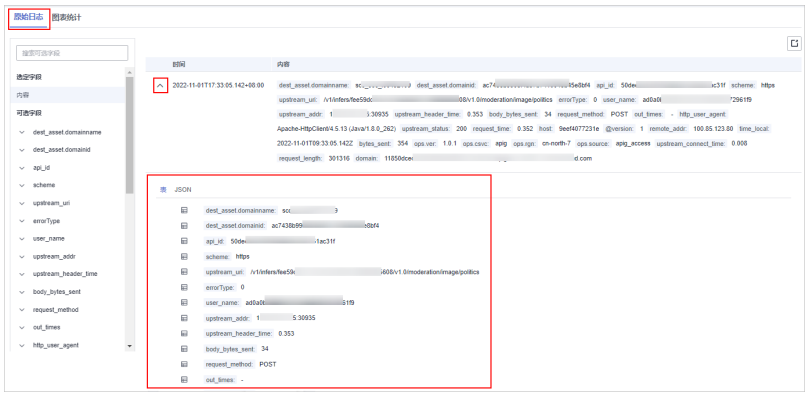
  - 设置显示日志数据信息：
    - 页面中默认展示最近15分钟内的日志数据，如果需要展示其他时间数据，可以在右上角选择展示的时间。

图 10-74 选择显示时间

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

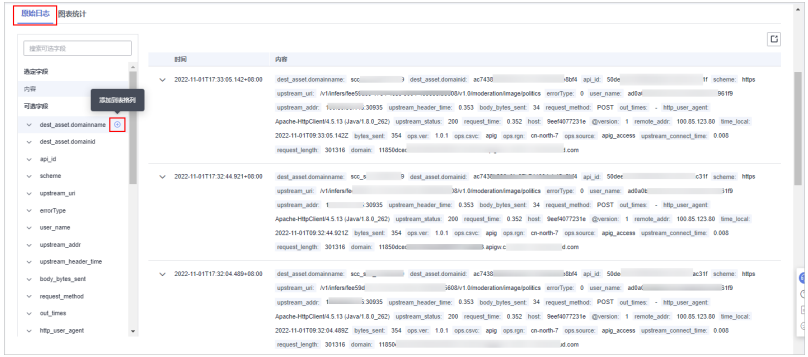
  如需查看JSON格式数据，可以选择“JSON”页签，页面将展示JSON格式的数据。

图 10-75 展开显示数据



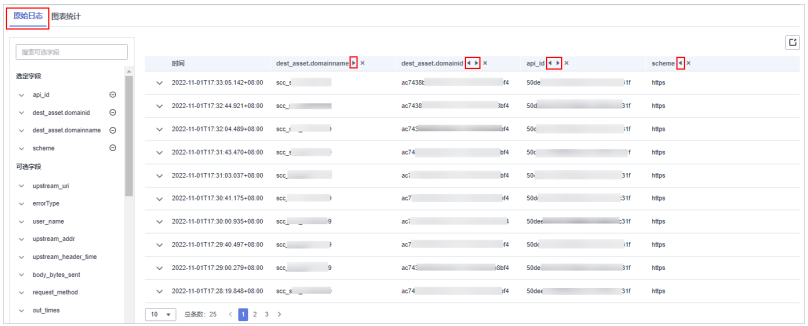
- 如需在列表中展示/筛选某些字段信息，可在右侧可选字段中选择需展示的字段，并单击字段名称后的 ，该字段将显示在右侧日志数据列表中。

图 10-76 选中显示字段



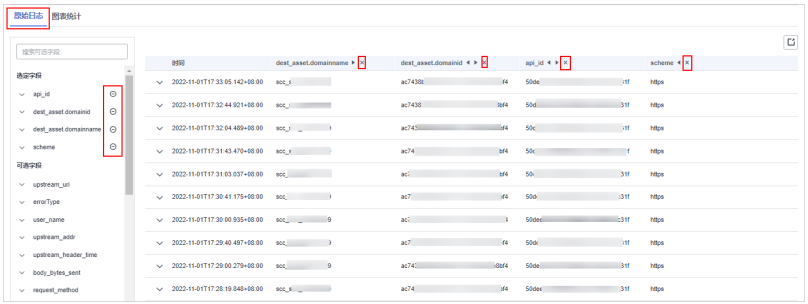
  - 字段选中后，如需**调整显示先后顺序**，可在右侧日志数据列表的表头列单击该字段名称后的 （向左移一列）、 （向右移一列）按钮来进行调整。

图 10-77 调整顺序



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

图 10-78 取消选择



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

- **图表统计**

  查询语句查询后，在“图表统计”页签可以查看可视化的查询分析结果。

  图表统计是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**。

10.5.6 下载日志

操作场景

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 在页面左上角单击 ☰，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。

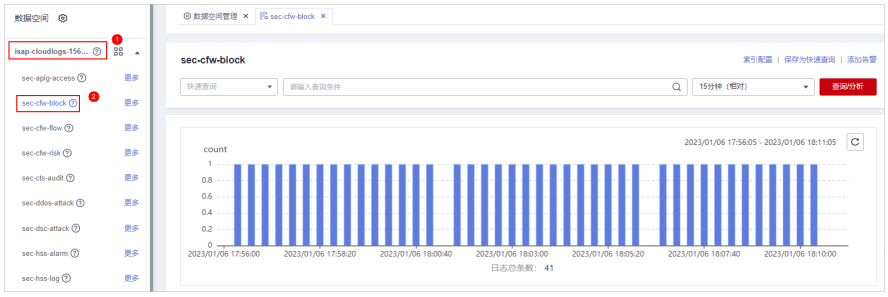
图 10-79 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 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



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

10.5.7 查询与分析语法-SQL 语法

10.5.7.1 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 10-50 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。

10.5.7.2 约束与限制

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

10.5.7.3 查询语句

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

本章节将介绍查询语句以及使用示例。

语法

查询语句有两种形式：

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

查询子句基本结构如下所示：

```
字段名称 操作符 字段值
```


其中，可使用的操作符如**操作符**所示。

操作符

表 10-51 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 10-52 普通查询示例

查询需求	查询语句
查询所有日志	*
查询GET请求成功（状态码为200~299）的日志。	request_method = 'GET' AND status BETWEEN 200 AND 299
查询GET请求或POST请求的日志。	request_method = 'GET' OR request_method = 'POST'
查询非GET请求的日志。	NOT request_method = 'GET'
查询GET请求或POST请求，且请求成功的日志。	(request_method = 'GET' OR request_method = 'POST') AND status BETWEEN 200 AND 299
查询GET请求或POST请求，且请求失败的日志。	(request_method = 'GET' OR request_method = 'POST') NOT status BETWEEN 200 AND 299

查询需求	查询语句
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

10.5.7.4 分析语句语法

完整的分析语句语法如下：

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

10.5.7.5 分析语句-SELECT

指定查询的字段。

使用*查询所有字段

```
SELECT *
```

表 10-53 使用*查询所有字段

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

查询指定字段

```
SELECT firstname, lastname
```

表 10-54 查询指定字段

firstname	lastname
Amber	Duke
Hattie	Bond

firstname	lastname
Nanette	Bates
Dale	Adams

使用 AS 给字段定义别名

```
SELECT account_number AS num
```

表 10-55 使用 AS 给字段定义别名

num
1
16
13
18

使用 DISTINCT 去重

```
SELECT DISTINCT age
```

表 10-56 使用 DISTINCT 去重

age
32
36
28

使用 SQL 函数

函数相关内容请参见**函数**。

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

表 10-57 使用 SQL 函数

len	firstname
4	Amber
6	Hattie
7	Nanette

len	firstname
4	Dale

10.5.7.6 分析语句-GROUP BY

按值分组。

按字段的值分组

```
SELECT age GROUP BY age
```

表 10-58 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 10-59 按字段别名分组

num
1
16
13
18

按多个字段分组

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

表 10-60 按多个字段分组

num	age
1	32
16	36
13	28

num	age
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 10-61 使用 SQL 函数

len	count
4	2
5	2

10.5.7.7 分析语句-HAVING

在分组的基础上，结合**聚合函数**来筛选数据。

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

表 10-62 HAVING

age	MAX(balance)
28	32838
32	39225

10.5.7.8 分析语句-ORDER BY

按字段值排序。

使用字段值排序

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

表 10-63 使用字段值排序

age
28
32
32

age
36

10.5.7.9 分析语句-LIMIT

指定返回数据的条数。

指定返回的条数

```
SELECT * LIMIT 1
```

表 10-64 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 10-65 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

10.5.7.10 分析语句-函数

数学类

表 10-66 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

函数	作用	定义	示例
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
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

函数	作用	定义	示例
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 10-67 三角函数

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

时间函数

表 10-68 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
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 10-69 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

其他

表 10-70 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

函数	作用	定义	示例
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

10.5.7.11 分析语句-聚合函数

表 10-71 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

10.5.8 快速查询

操作场景

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 在页面左上角单击 ☰，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。

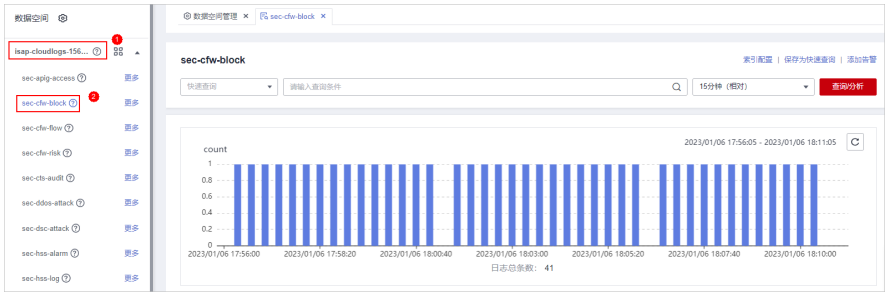
图 10-82 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-83 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 10-84 管道数据页面



步骤6 输入查询分析语句，设置时间范围，并单击“查询分析”。

更多查询分析详细操作请参见**查询与分析**。

步骤7 单击页面右上角“保存为快速查询”，在右侧页面中配置查询参数。

表 10-72 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

10.5.9 快速添加日志告警模型

操作场景

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。

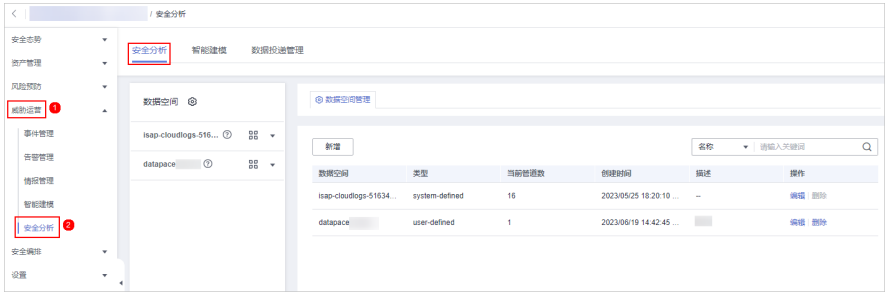
步骤2 在页面左上角单击☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-85 进入目标工作空间管理页面

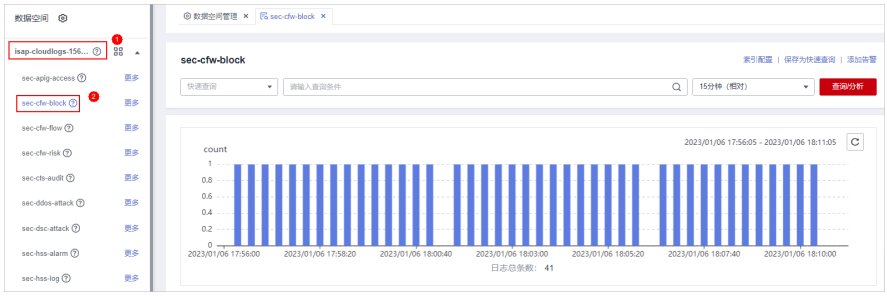
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-86 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 10-87 管道数据页面

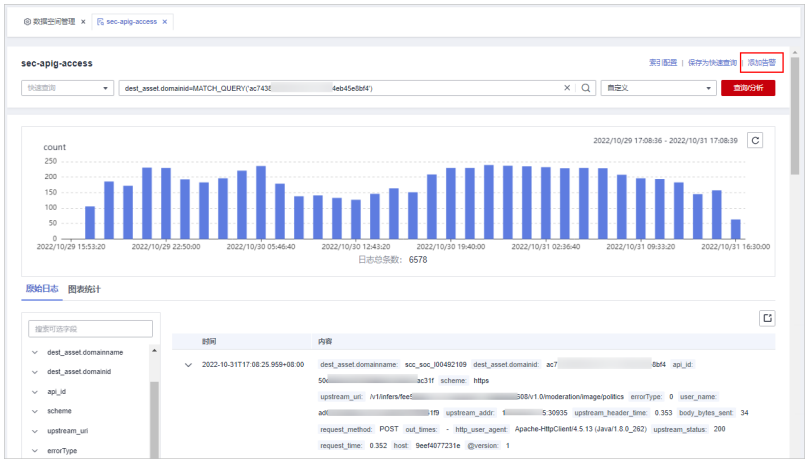


步骤6 输入查询分析语句，设置时间范围，并单击“查询分析”，显示查询分析结果。

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。

图 10-88 添加告警



步骤8 配置告警基础信息，参数说明如**表10-73**所示。

表 10-73 告警模型基础配置

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

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

步骤9 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。

步骤10 设置模型逻辑，参数说明如表10-74所示。

表 10-74 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。

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

10.5.10 图表统计

10.5.10.1 图表统计概述

当您执行了查询和分析语句后，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，您可以根据分析需求选择合适的统计图表类型展示查询和分析结果。

安全云脑可以通过以下图表类型展示查询和分析结果：

- 表格
- 折线图
- 柱状图
- 饼图

10.5.10.2 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 在页面左上角单击  ，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。

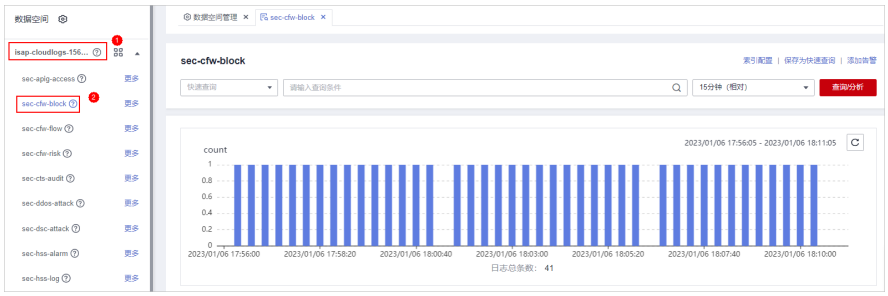
图 10-89 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-90 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。

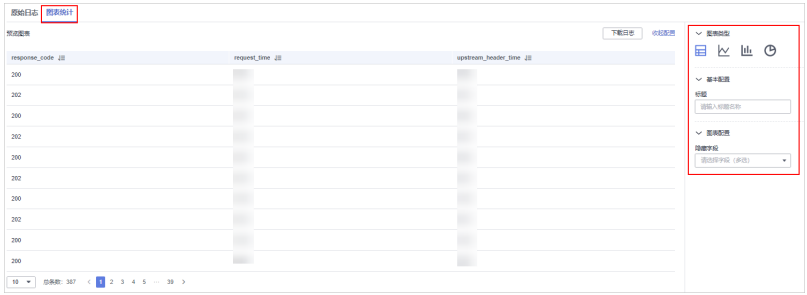
图 10-91 管道数据页面



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 10-92 表格统计



步骤8 配置表格参数。

表 10-75 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”。

10.5.10.3 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。

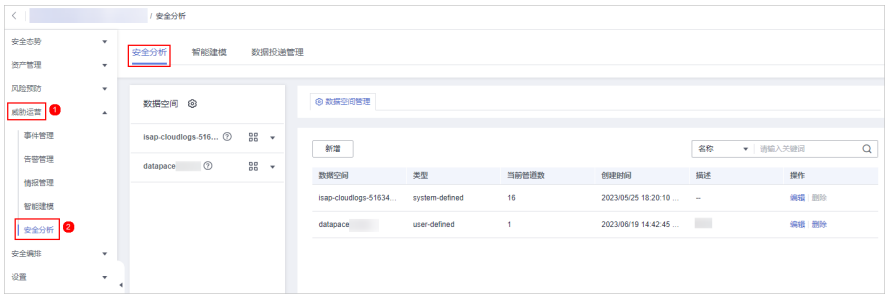
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-93 进入目标工作空间管理页面

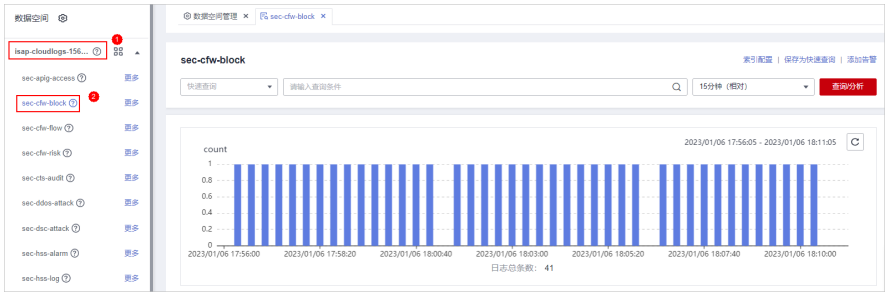
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-94 进入安全分析页面



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

图 10-95 管道数据页面



步骤6 输入查询分析语句，设置时间范围，并单击“查询分析”。

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

图 10-96 折线图统计

步骤8 配置折线图参数。

表 10-76 折线图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	X轴标题	自定义X轴标题名称。
	Y轴标题	自定义Y轴标题名称。
	X轴字段	选择X轴显示字段。

参数类别	参数名称	参数说明
	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”。

10.5.10.4 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。

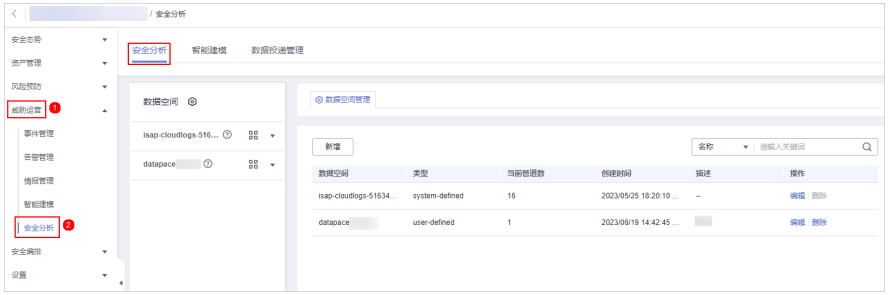
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-97 进入目标工作空间管理页面

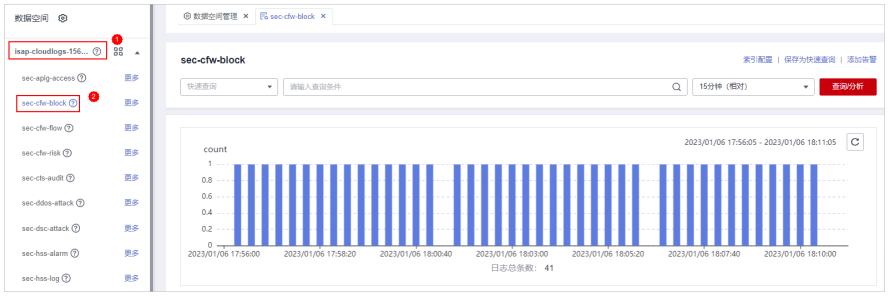
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-98 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。

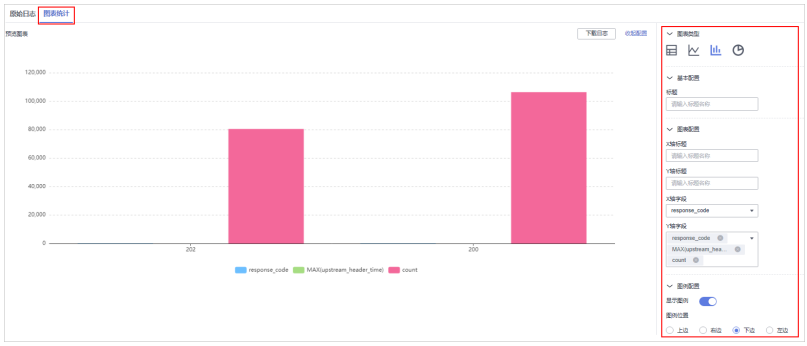
图 10-99 管道数据页面



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 10-100 柱状图统计



步骤8 配置柱状图参数。

表 10-77 柱状图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	X轴标题	自定义X轴标题名称。

参数类别	参数名称	参数说明
	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”。

10.5.10.5 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 在页面左上角单击 ☰，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。

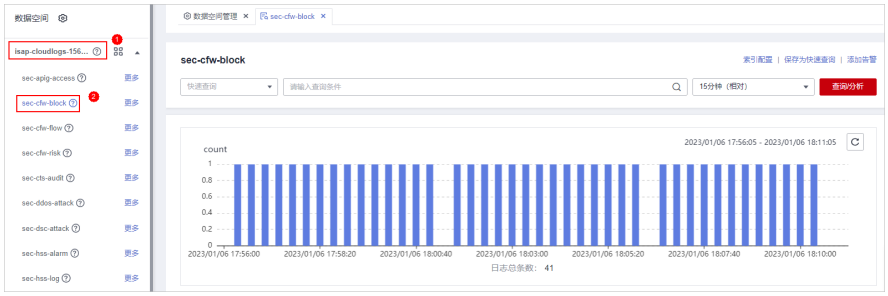
图 10-101 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-102 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。

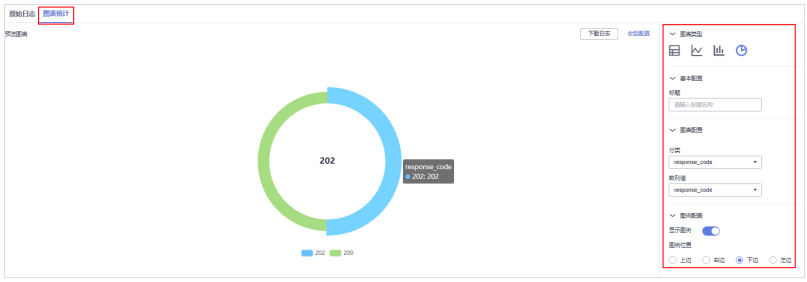
图 10-103 管道数据页面



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 10-104 饼图统计



步骤8 配置饼图参数。

表 10-78 饼图参数配置

参数类别	参数名称	参数说明
基本配置	标题	自定义线图标题名称。
图表配置	分类	数据分类。
	数列值	分类数据对应的数值。

参数类别	参数名称	参数说明
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”。

10.5.11 管理数据空间

10.5.11.1 新增数据空间

操作场景

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

当您需要使用安全云脑提供的**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。

约束与限制

- 单账号单Region单Workspace最多创建5个数据空间。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-105 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-106 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 10-107 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10-79所示。

表 10-79 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（整个华为云上）唯一，不能与其他数据空间名称相同。
描述	可选参数，设置该数据空间的备注信息。

步骤7 单击“确定”，完成数据空间的新增。

新增完成后，可以在数据空间列表中查看已新增的数据空间。

----结束

10.5.11.2 查看数据空间详情

操作场景

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-108 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-109 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10-80所示。

表 10-80 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。

参数名称	参数说明
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 10-110 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10-81**所示。

表 10-81 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

10.5.11.3 编辑数据空间

操作场景

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击，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 10-111 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-112 进入安全分析页面

步骤5 在待编辑数据空间所在行“操作”列，单击“编辑”。

步骤6 在弹出编辑数据空间界面，修改数据空间描述信息。

步骤7 单击“确定”。

----结束

10.5.11.4 删除数据空间

操作场景

如果不再需要某个数据空间，可以参照本章节进行删除。

约束与限制

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 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”。

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

10.5.12 管理管道

10.5.12.1 创建管道

操作场景

数据传输消息主题和存储索引组合为数据管道。

当您需要使用安全云脑提供的**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

- 单账号单Region单数据空间最多创建20个数据管道。

操作步骤

步骤1 登录管理控制台。

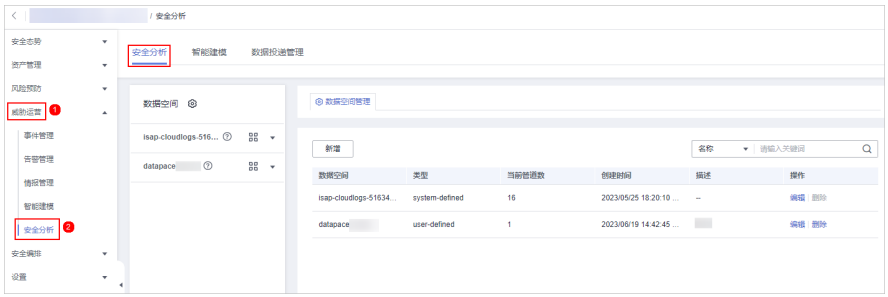
步骤2 在页面左上角单击 ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-115 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-116 进入安全分析页面



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

图 10-117 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10-82所示。

表 10-82 创建管道

参数名称	参数说明
数据空间	该管道所属的数据空间，系统默认生成。

参数名称	参数说明
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

10.5.12.2 查看管道详情

操作场景

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

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰ ，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 10-118 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-119 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 10-120 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 10-83 管道参数说明

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

----结束

10.5.12.3 编辑管道

操作场景

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

本章节介绍如何修改管道参数信息。

约束与限制

系统创建的数据管道**不支持**编辑操作。

操作步骤

步骤1 登录管理控制台。

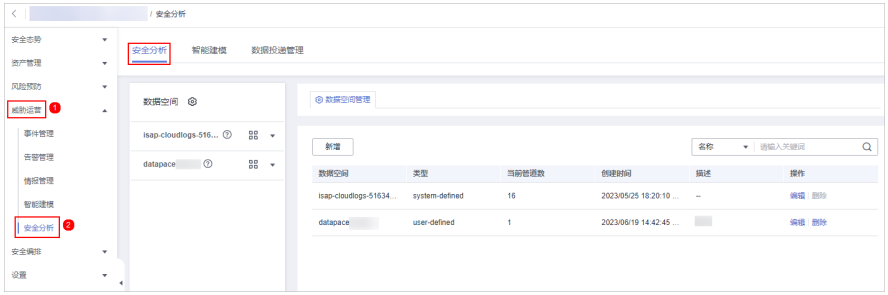
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-121 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-122 进入安全分析页面

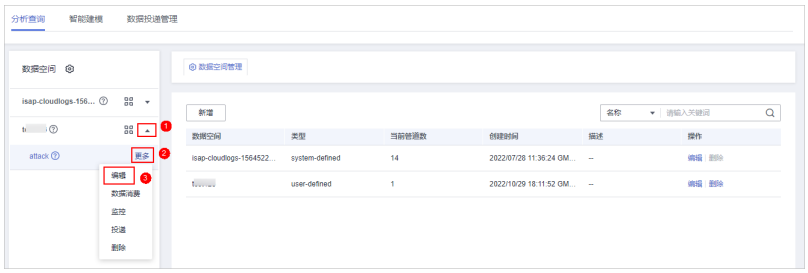


步骤5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的 ▼，展开已创建的管道。

图 10-123 查看管道

步骤6 单击管道名称后的“更多 > 编辑”。

图 10-124 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10-84**所示。

表 10-84 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

10.5.12.4 删除管道

操作场景

本章节介绍如何删除管道。

数据将会被同步删除，且不可恢复，请谨慎操作。

约束与限制

系统创建的数据管道**不支持**删除操作。

操作步骤

步骤1 登录管理控制台。

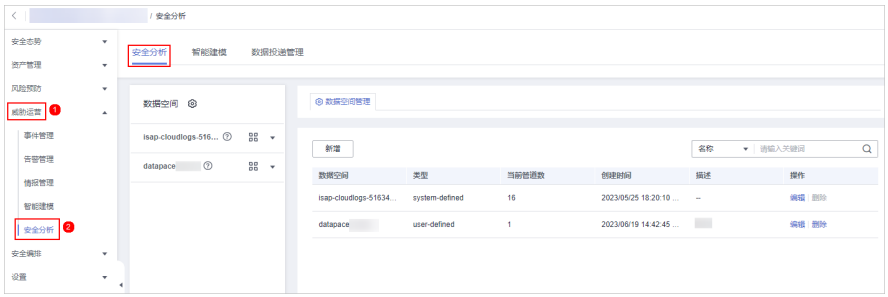
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-125 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-126 进入安全分析页面

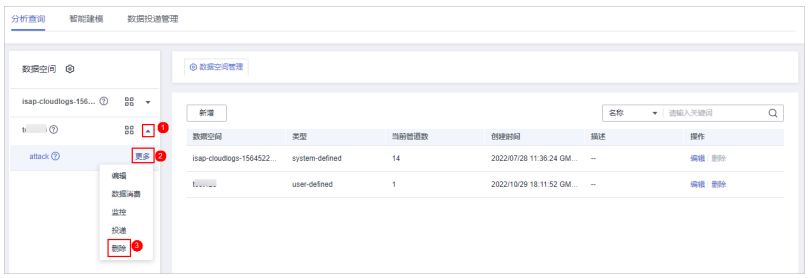


步骤5 在左侧数据空间导航栏中，单击数据空间栏或数据空间栏后的 ▼ ，展开已创建的管道。

图 10-127 查看管道

步骤6 单击管道名称后的“更多 > 删除”。

图 10-128 删除管道



步骤7 在弹出的删除确认框中，单击“确认”，完成删除管道的操作。

----结束

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 在页面左上角单击 ，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。

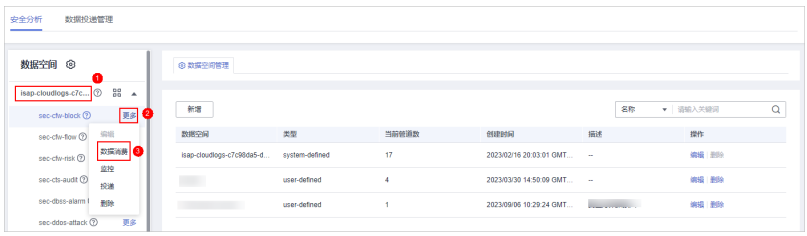
图 10-129 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-130 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 10-131 进入数据消费页面



步骤6 在数据消费页面中，单击当前状态后的 ，开启数据消费。

开启后，将显示消费配置信息，具体说明如表10-85所示。

表 10-85 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

操作场景

安全云脑支持将数据实时投递至其他管道或其他华为云产品中，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）。

本章节介绍如何新增数据投递。

前提条件

- 如需投递到OBS中，需要已有一个**桶策略**为**公共读写**的可用的桶。如需创建，详细操作请参见**创建OBS桶**。
- 如需投递到LTS中，需要已有可用的日志组和日志流。如需创建，详细操作请参见**创建LTS日志组**、**创建LTS日志流**。

约束与限制

跨账号投递仅支持投递到其他账号管道中，不支持投递到其他云服务。

新增数据投递

步骤1 登录管理控制台。

步骤2 在页面左上角单击  ，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。

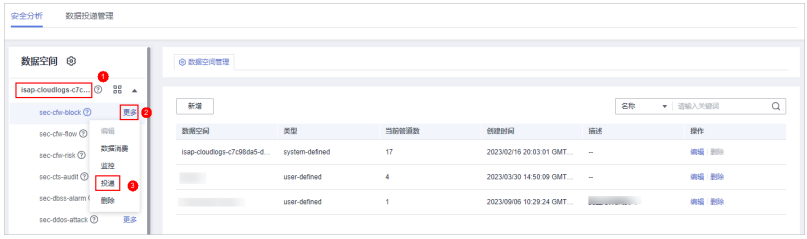
图 10-132 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-133 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 10-134 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 10-86 基本信息

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

2. 配置数据源。

数据源配置中，显示当前管道数据的详细信息，**无需配置**。

表 10-87 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账号其他管道或其他账号的管道中，请根据您的需要进行选择配置。
     - 本账号投递：将当前管道数据投递到本账号的其他管道中，参数配置说明如表10-88所示。

       表 10-88 配置数据目的-本账号 PIPE

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

     - 跨账号投递：将当前管道数据投递到其他账号的管道中，参数配置说明如表10-89所示。

       表 10-89 配置数据目的-跨账号 PIPE

参数名称	参数说明
账号类型	选择数据投递目的地的账号类型，此处选择“跨账号”。
投递类型	选择投递类型，此处选择PIPE。
账号ID	输入目的PIPE所在账号的ID。

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10-90**所示。

  投递到LTS中，需要已有可用的日志组和日志流。如需创建，详细操作请参见**创建LTS日志组**、**创建LTS日志流**。

  表 10-90 配置数据目的-LTS

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

- OBS：将当前管道数据投递到OBS服务，参数配置说明如**表10-91**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。如需创建，详细操作请参见**创建OBS桶**。

  表 10-91 配置数据目的-OBS

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

4. 在“访问授权”中，查看**步骤6**中授予的权限。

   投递请求需要获取访问您云资源的读写权限，授权后，投递任务才能拥有对您云资源相应的访问权限。

步骤8 单击“确定”。

----结束

后续处理

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

10.7.2 数据投递授权

操作场景

数据投递新增后，需进行投递权限授予操作，接受授权后，投递才会生效。

本章节介绍如何执行数据投递投递授权。

前提条件

已新增数据投递。

约束与限制

如果新增的数据投递为跨账号投递，则需要登录目的账号进行授权操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-135 进入目标工作空间管理页面

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

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

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

图 10-136 数据投递授权

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况，详细操作请参见**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 10-92 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

操作场景

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

- **投递到其他数据管道**
- **投递到OBS桶**
- **投递到LTS**

前提条件

已完成数据投递操作，具体操作请参见**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。

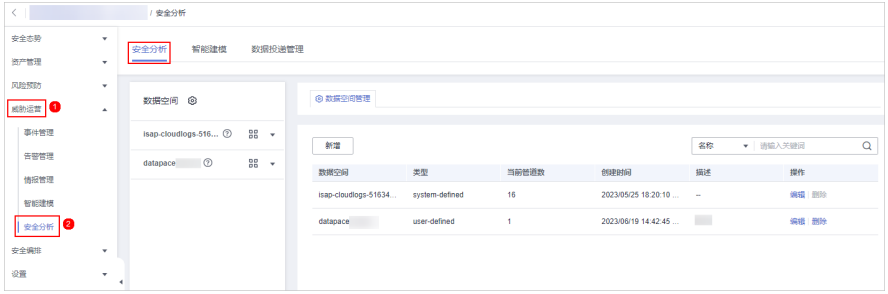
步骤2 在页面左上角单击 ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-137 进入目标工作空间管理页面

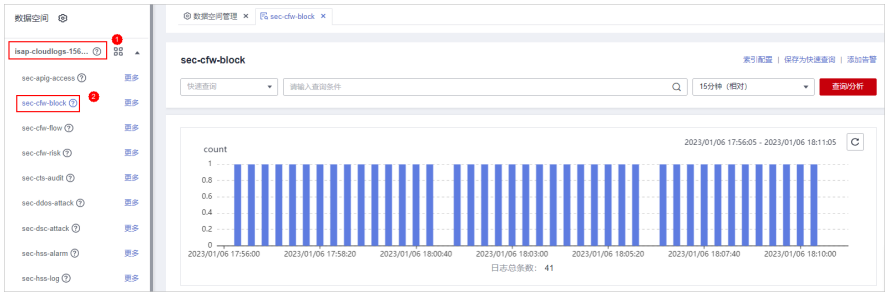
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-138 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 10-139 管道数据页面



步骤6 在目标管道中，查看投递的日志信息。

----结束

投递到 OBS 桶

步骤1 登录管理控制台。

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

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

步骤4 在OBS桶详情页面，查看投递的日志信息。

----结束

投递到 LTS

步骤1 登录管理控制台。

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

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

步骤4 展开后，单击新增数据投递时选择的日志流的名称，进入日志流详情页面。

步骤5 在日志流详情页面，查看投递的日志信息。

----结束

10.7.4 管理数据投递任务

操作场景

本章节介绍管理投递任务，请根据您的需要选择对应操作：

- **查看数据投递任务**：查看数据投递任务相关信息。
- **挂起投递任务**：数据投递成功后，如需停止投递，可挂起目标投递任务。
- **启动投递任务**：数据投递任务停止投递后，如需重启投递，可启动目标投递任务。
- **删除投递任务**：如果不在需要某个投递任务，可删除投递任务。

前提条件

已新增数据投递。

查看数据投递任务

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-140 进入目标工作空间管理页面

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

图 10-141 进入数据投递管理页面

步骤5 在投递任务列表页面中，查看已有投递任务。

表 10-93 投递任务

操作	操作说明
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 在页面左上角单击 ☰，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 10-142 进入目标工作空间管理页面

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

图 10-143 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 在页面左上角单击 ☰，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 10-144 进入目标工作空间管理页面

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

图 10-145 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

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 在页面左上角单击 ☰，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 10-146 进入目标工作空间管理页面

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

图 10-147 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

10.7.5 投递日志数据至 LTS

操作场景

安全云脑支持集成WAF、HSS、CFW等其他云产品日志，具体集成操作及支持集成的云服务请参见**数据集成**。

集成后的日志还支持投递至云日志服务（Log Tank Service，简称LTS），方便用户快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

本章节将介绍如何将集成的日志数据投递至LTS。

前提条件

- 已完成需投递日志的数据集成至安全云脑操作，详细操作请参见**数据集成**。
- 投递到LTS中，需要已有可用的日志组和日志流。如需创建，详细操作请参见**创建LTS日志组**、**创建LTS日志流**。

操作步骤

新增数据投递

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

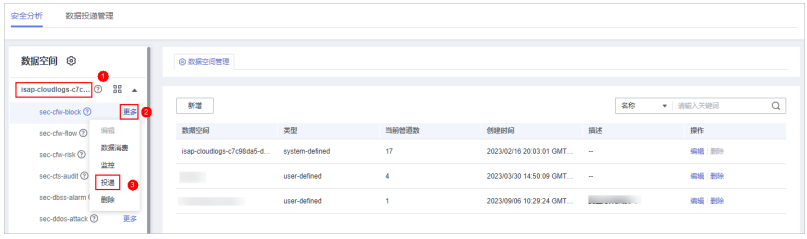
图 10-148 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-149 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 10-150 进入投递设置页面



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

在弹出的授权提示中，确认无误后，单击“确认”，完成授权。

步骤7 在新增投递配置页面中，配置数据投递相关参数。

- 投递名称：自定义数据投递名称。
- 账号类型：此处请选择“本账号”。投递到LTS服务仅支持投递本账号内的日志数据。
- 投递类型：此处请选择“LTS”。
- 日志组：选择LTS日志组。如果无可用日志组，需进行创建，详细操作请参见**创建LTS日志组**。
- 日志流：选择目的LTS日志流。如果无可用日志流，需进行创建，详细操作请参见**创建LTS日志流**。

其他配置参数，系统默认生成，无需配置。

步骤8 在“访问授权”中，查看**步骤6**中授予的权限。

投递请求需要获取访问您云资源的读写权限，授权后，投递任务才能拥有对您云资源相应的访问权限。

步骤9 单击“确定”。

数据投递授权

步骤10 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 10-151 数据投递授权

授权授予后，目标投递任务授权状态更新为“已授权”，更新后，可前往投递目的地查看投递情况。

查看数据投递情况

步骤11 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12 在日志管理页面的“日志组列表”栏中，找到新增数据投递是填写的日志组，并单击日志组名称前的 ∨ 按钮。

步骤13 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14 在日志流详情页面，查看投递的日志信息。

----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。

查看监控指标

步骤1 登录管理控制台。

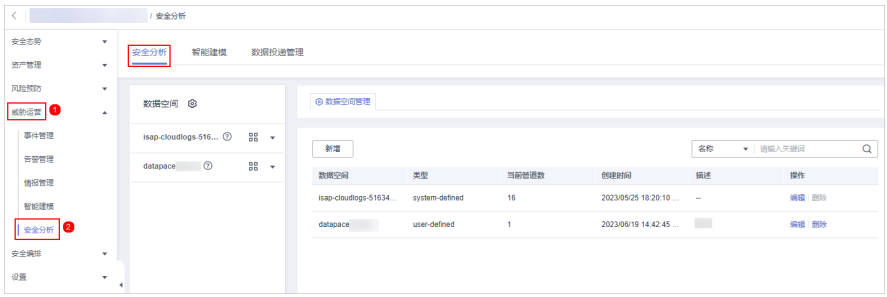
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 10-152 进入目标工作空间管理页面

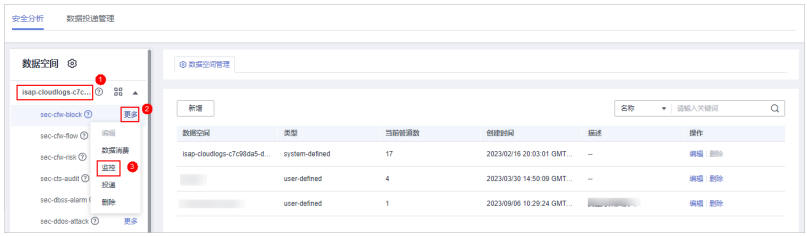
步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 10-153 进入安全分析页面



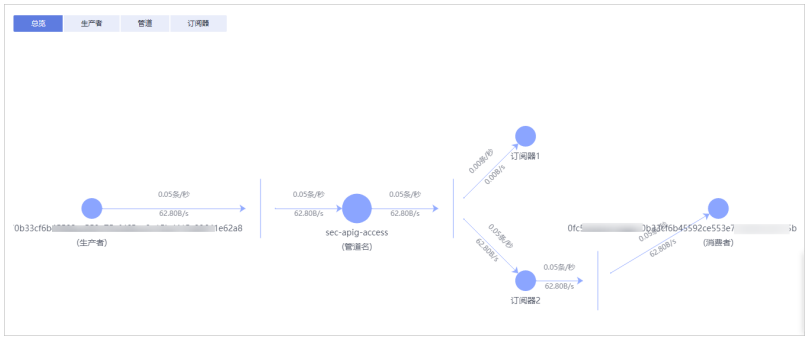
步骤5 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，单击目标管道名称后的“更多 > 监控”，进入管道监控页面。

图 10-154 进入数据监控页面



步骤6 在数据管道的监控页面，查看监控指标。

图 10-155 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

10.9 舆情监测

安全云脑的舆情监测是一个基于互联网信息聚合、文本挖掘和智能检索等技术的功能，用于发现和挖掘互联网安全态势变化。可以及时发现和挖掘与您有关的安全事件、安全漏洞、社会影响、品牌舆情、热搜分析等，并将监测形成分析报告，协助您掌握舆情动态，并对潜在的各类舆情风险点进行监测和综合研判。

说明

目前，仅“华北-北京四”region支持使用该功能，其他region如需使用该功能，需先**提交工单**申请开通使用权限。

使用须知

- 舆情监测提供按需计费模式，根据报告份数（一份报告仅包含一个监测主题）按次进行收费。
- 舆情监测提供有专报、月报和年包三种类型的报告供您选择。
  - 专报：根据具体事件的实际发生时间自动配置，购买后5个工作日内提供1份报告。
  - 月报：监测周期为自定义设置的1个月。在监测周期结束后，7个工作日内提供1份报告。
  - 年包：监测周期为自定义设置的1年。每月监测任务结束后，7个工作日内提供1份月报，一年的监测任务结束后，15个工作日内提供1份年报。

购买舆情监测报告

舆情监测功能可以根据监测主题对指定信息源及行业进行监测，监测后提供有专报、月报和年包三种类型的报告供您选择。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 10-156 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 舆情监测”，进入舆情监测页面后，单击“购买舆情报告”。

图 10-157 舆情监测页面

步骤5 在购买舆情报告页面，配置参数信息。

表 10-94 购买舆情报告

参数名称	参数说明
监测任务标题	自定义输入监测任务的标题。
报告类型	选择报告类型，可以选择专报、月报和年包。 • 专报：根据具体事件的实际发生时间自动配置，购买后5个工作日内提供1份报告。 • 月报：监测周期为自定义设置的1个月。在监测周期结束后，7个工作日内提供1份报告。 • 年包：监测周期为自定义设置的1年。每月监测任务结束后，7个工作日内提供1份月报，一年的监测任务结束后，15个工作日内提供1份年报。
监测周期	• 当“报告类型”选择月报或年包时，可以手动设置监测周期。 • 当“报告类型”选择专报时，监测周期根据事件实际发生时间自动配置，无需手动设置。
监测集群	选择监测的集群。
监测区域	选择监测的区域。
监测信息源	选择监测信息的来源。
监测行业	勾选监测的行业。默认选择全部行业，未选中的行业会进行排除。
监测主题配置	1. 输入监测主题。 – 主题填写的字符要求在2到50个字符内。 – 监测主题上限为100个。 2. 单击“生成监测主题(Enter)”或按“Enter”。 系统将在下方表格中生成监测主题。 **说明** 一份报告中仅包含一个监测主题。

参数名称	参数说明
（可选）添加任务	如需购买多种类型的报告，可单击“添加任务”，并配置购买参数。 添加后，如果不再需要某个任务，可以单击监测任务栏右上角“收起”，收起后再单击“删除”，确认并删除某个任务。

步骤6 配置完成并核对无误后，请仔细阅读重要提示信息，并勾选“我已知晓”。

说明

监测任务创建后，一次性扣费，不支持修改和暂停任务，请您仔细核对监测任务中设置的信息。

步骤7 单击“下一步”，进入订单详情页面。

步骤8 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9 在支付页面，选择付款方式完成付款，完成购买操作。

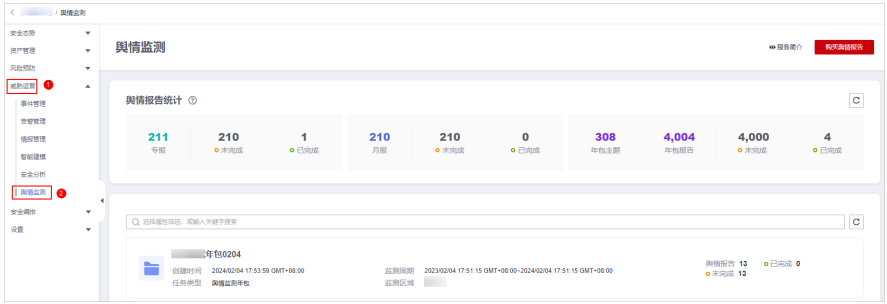
----结束

查看及下载舆情报告

舆情报告购买成功后，安全云脑将按照您设置的主题在指定的信息源中进行监测。监测完成后，您可以查看舆情监测的情况。

步骤1 在左侧导航栏选择“威胁运营 > 舆情监测”，进入舆情监测页面。

图 10-158 舆情监测页面



步骤2 在舆情监测页面，查看舆情报告统计信息和监测任务信息。

表 10-95 舆情报告统计信息和监测任务信息

参数名称	参数说明
舆情报告统计	页面上方舆情报告统计中，展示专报、月报和年包三种类型报告的数量，以及各类型未完成、已完成状态的数量。 其中，专报、月报统计每个监测主题的报告信息，年包统计每个监测主题的13份报告的信息。

参数名称	参数说明
监测任务	• 页面下方监测任务列表中，展示监测任务主题、创建时间、任务类型、监测周期、监测区域、报告数量、已完成报告数量和未完成报告数量。 • 当监测任务较多时，可以通过搜索功能，选择搜索类型并输入关键字后单击“Enter”，即可快速查询指定监测任务。

步骤3 单击目标监测任务名称，进入监测任务详细信息页面，查看某个监测任务、某个监测任务中监测报告详情以及**下载舆情报告**。

- 在监测任务详情页面上方，显示着监测任务主题、创建时间、任务类型、监测周期、监测区域、监测信息源、监测行业等信息。
- 如果监测任务已完成，将生成监测报告，单击监测报告名称，右侧将展示监测报告详细信息，报告参数说明如**表10-96**所示。

表 10-96 舆情报告详情

参数名称	参数说明
概述	说明报告的类型、监测主题、监测时间等信息。
舆情总览	– 监测概述：展示监测主题相关内容信息数、敏感信息数、敏感占比、非敏感信息数、非敏感占比、中性信息数和中性占比。 – 信息情感分布：以饼图的样式展示敏感、非敏感和中性信息的分布情况。 – 媒体来源明细：展示该事件监测范围内，活跃媒体声量TOP2的媒体来源及其数据量。
主要舆情	展示此次报告的主要舆情信息，包括舆情标题、产生时间及舆情来源。
传播走势	展示此次监测的信息传播的走势、详情和路径。
数据透视	展示此次监测的信息属性的走势、地域分析、平台活跃度占比、热点网民、事件实体识别、群体情绪识别等信息。
处置建议	基于当前舆情监测报告的监测结果，为您当前的资产提供最佳处置建议。

- 如果需要**下载舆情报告**，可以在报告详细信息页面中单击“下载报告”，系统将自动下载报告至本地。

----结束

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。

在安全编排中，剧本和流程是两个核心元素，它们相互关联、依赖，并协同工作以确保安全运营的有效性和高效性。剧本和流程的含义、关系说明如下：

- 含义：
  - 剧本（Playbook）：是安全运营流程在安全编排系统中的形式化表述，它是将人读安全运营流程和规程转换为机读工作流的过程。

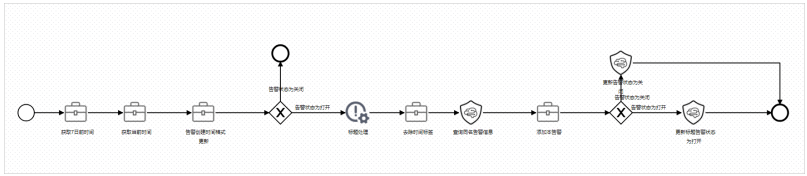
    剧本体现了安全防护的逻辑，指示如何调度安全能力。剧本具有灵活性和可扩展性，可以根据实际需求进行修改和扩展，以适应不断变化的安全威胁和业务需求。

图 11-1 剧本详情示例-重复告警自动关闭

- 流程（Workflow）：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，形成一种协同工作方式。它由多个相连接的组件构成，流程定义完成后可被外部触发，例如，当新工单产生时自动触发自动审核工单流程。您可以通过可视化流程编辑画布，定义每个节点的组件动作。

  流程是剧本触发时响应的方式，它负责将剧本中的指令和规程转化为具体的操作和执行步骤。

图 11-2 流程详情示例-重复告警自动关闭



- 联系与区别
  - 联系：剧本提供了安全运营的指导和规则，而流程则负责将这些规则转化为具体的执行步骤和操作。剧本和流程相互依赖，剧本指导流程的执行，而流程则实现了剧本的意图和要求。
  - 区别：剧本和流程之间也存在一定的区别。首先，剧本更侧重于定义和描述安全运营的流程和规程，它关注的是整体的框架和策略；而流程则更侧重于具体的操作和执行步骤，它关注的是如何将剧本中的要求转化为实际的行动。其次，剧本具有较大的灵活性和可扩展性，可以根据需要进行修改和扩展；而流程则相对固定，一旦设计完成，就需要按照规定的步骤执行。

  示例：以一个具体的网络安全事件响应案例为例，当组织遭受到一次网络攻击时，安全编排系统会首先根据预设的剧本识别出攻击的类型和严重程度。然后，系统会根据剧本中定义的流程，自动触发相应的安全措施，如隔离被攻击的系统、收集攻击数据、通知安全团队等。在这个过程中，剧本和流程紧密配合，确保安全响应的准确性和及时性。

约束与限制

- 单账号单workspace内，单剧本调度频率时间 ≥ 5分钟。
- 单账号单workspace内一天内的重试次数限制如下：
  - 手动重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。
  - API接口重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。
- 分类&映射约束与限制如下：
  - 单账号单workspace内，分类&映射模板 ≤ 50个。
  - 单账号单workspace内，分类和映射的映射关系规格为1:100。
  - 单账号单workspace内，最多可新增分类&映射100个。

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 内置剧本和流程

安全编排根据需求内置了剧本、流程，可以根据需要直接进行使用。

内置剧本

默认已启用以下剧本：

主机告警状态同步、高危漏洞自动通知、主机防线告警关联历史处置信息、云脑WAF地址组关联策略、应用防线告警关联历史处置信息、网络防线告警关联历史处置信息、重复告警自动关闭、告警ip指标打标、资产防护状态统计通知、未关闭告警自动统计通知、高危告警自动通知

表 11-1 内置剧本

安全防线	剧本名	描述	数据类
主机安全	主机告警状态同步	自动同步主机告警状态	Alert
	高危漏洞自动通知	对威胁等级为High的漏洞进行邮件或者短信通知	Vulnerability

安全防线	剧本名	描述	数据类
	攻击链路分析告警通知	针对攻击链路进行分析，如果主机产生告警，就会查看关联主机所属的网站，如果有对应网站信息且有告警，就进行告警通知	Alert
	主机资产风险统计通知	查询资产管理中绑定EIP的主机资产，将其漏洞信息统计通知给客户	CommonContext
	HSS文件隔离查杀	自动隔离查杀恶意软件	Alert
	挖矿主机隔离	当主机告警类型是挖矿程序/挖矿软件，对当前主机进行隔离，添加安全组，对入方向和出方向全部阻断	Alert
	勒索主机隔离	当主机告警类型是勒索软件，对当前主机进行隔离，添加安全组，对入方向和出方向全部阻断	Alert
	主机防线告警关联历史处置信息	针对主机类告警，关联HSS告警历史处置信息，并添加至该告警评论中	Alert
应用安全	云脑WAF地址组关联策略	将安全云脑指定WAF地址组(黑IP地址组)绑定WAF所有企业项目全部策略的黑白名单	CommonContext
	WAF删除空防护策略	每周一9点查询WAF防护策略，对空防护策略进行删除	CommonContext
	应用防线告警关联历史处置信息	针对WAF告警，关联WAF告警历史处置信息，并添加至该告警评论中	Alert
运维安全	关键运维操作实时通知	针对模型产生的运维告警，进行实时通知。目前支持挂载网卡、peering对等连接、资源绑定EIP三种关键运维操作进行smn通知	Alert
身份安全	身份防线告警关联历史处置信息	针对IAM告警，关联IAM告警历史处置信息，并添加至该告警评论中	Alert
网络安全	网络防线告警关联历史处置信息	针对CFW告警，关联CFW告警历史处置信息，并添加至该告警评论中	Alert
其他/通用	高危告警自动通知	对威胁级别为High或者Fatal的告警进行邮件或者短信通知	Alert
	告警指标提取	将告警中IP信息抽取，通过情报系统进行验证，如果为恶意IP，可以将IP信息设置成指标，并与源告警相互关联	Alert
	重复告警自动关闭	将近7日内第二次及第二次以上出现的告警状态置为关闭，并关联7日内同名告警	Alert

安全防线	剧本名	描述	数据类
	自动更新告警名称	根据客户需要，筛选关键字段信息，拼接告警名称	Alert
	告警ip指标打标	告警添加告警关联攻击源IP及目标IP的标签信息	Alert
	关联内外部IP画像情报	告警关联云脑情报、微步情报（优先关联内部情报）	Alert
	资产防护状态统计通知	每周统计客户资产防护状态，同时发送邮件/短信通知给客户	CommonContext
	未关闭告警自动统计通知	每天晚上7点，统计未关闭的告警，并发送邮件/短信通知给客户	Alert
	高危告警自动化安全封堵	针对高危和致命告警，源IP地址攻击次数达到阈值(次数>3)且命中微步在线的恶意标签，根据告警来源将该ip对应策略阻断(WAF、VPC、CFW、IAM)	Alert

内置流程

表 11-2 内置流程

安全防线	流程名称	描述	数据类
主机安全	主机告警状态同步	自动同步主机告警状态	Alert
	高危漏洞自动通知	对威胁等级为High的漏洞进行邮件或者短信通知	Vulnerability
	漏洞处理	调用主机安全接口修复主机漏洞	Vulnerability
	策略管理-安全组阻断	将目标IP添加到所有安全组中	Policy
	策略管理-安全组取消阻断	将目标IP从所有安全组中取消	Policy
	主机一键隔离	将目标主机进行全端口的隔离	Alert
	主机一键解封	将目标主机从隔离安全组中移除	Alert
	攻击链路分析告警通知	针对攻击链路分析，主机告警影响资产关联网站资产有对应攻击告警进行告警通知	Alert

安全防线	流程名称	描述	数据类
	主机资产风险统计通知	查询资产管理中绑定EIP的主机资产，将其漏洞信息统计通知给客户	CommonContext
	HSS文件隔离查杀	自动隔离查杀恶意软件	Alert
	主机防线告警关联历史处置信息	父流程，根据主机告警判断调用哪类子流程(主机防线告警关联历史处置信息-威胁建模-进程类、主机防线告警关联历史处置信息-威胁建模-登录类、主机防线告警关联历史处置信息-自动转告警)去关联历史处置信息，将其添加至告警评论	Alert
	主机防线告警关联历史处置信息-威胁建模-进程类	子流程，针对威胁建模构建的进程类告警，关联历史处置信息，将其添加到该告警的评论中	Alert
	主机防线告警关联历史处置信息-威胁建模-登录类	子流程，针对威胁建模构建的登录类告警，关联历史处置信息，将其添加到该告警的评论中	Alert
	主机防线告警关联历史处置信息-自动转告警	子流程，针对HSS自动转告警产生的告警，关联历史处置信息，将其添加到该告警的评论中	Alert
	主机隔离-恶意软件	当主机存在恶意软件(勒索、挖矿等)，触发人工审核节点，会显示恶意软件的详细内容(类型、受影响的主机、进程命令、文件路径等信息)供运营人员审核，审核通过后，会将受影响的主机进行自动化隔离	Alert
应用安全	WAF一键拦截	对目标IP封堵在该账号的WAF服务里的所有中策略	Alert
	WAF一键解封	对目标IP从该账号的WAF服务里的目标策略组中解封	Alert
	策略管理-WAF阻断	将目标IP添加到WAF的黑名单中	Policy
	策略管理-WAF取消阻断	将目标IP从WAF的黑名单中移除	Policy
	WAF地址组绑定策略	将安全云脑指定WAF地址组绑定WAF策略黑白名单	CommonContext
	应用防线告警关联历史处置信息	针对WAF类告警，关联历史处置信息，将其添加至告警评论	Alert
	WAF删除空防护策略	每周一9点查询WAF防护策略，对空防护策略进行删除	CommonContext

安全防线	流程名称	描述	数据类
网络安全	CFW一键拦截	将目标IP添加到CFW的黑名单中	Alert
	CFW一键解封	将目标IP从CFW的黑名单中移除	Alert
	策略管理-CFW阻断	将目标IP添加到CFW的黑名单中	Policy
	策略管理-CFW取消阻断	将目标IP从CFW的黑名单中移除	Policy
	网络防线告警关联历史处置信息	针对CFW类告警，关联历史处置信息，将其添加至告警评论	Alert
身份防线	身份防线告警关联历史处置信息	针对IAM类告警，关联历史处置信息，将其添加至告警评论	Alert
	策略管理-IAM阻断	通过策略管理，应急策略触发，将IAM用户名的状态修改为停用状态	Policy
	策略管理-IAM取消阻断	通过策略管理，应急策略触发，将IAM用户名的状态修改为启用状态	Policy
其他/通用	高危告警自动通知	对威胁级别为High或者Fatal的告警进行邮件或者短信通知	Alert
	告警指标提取	将告警中ip信息抽取，进行微步外部验证，置成指标，并与源告警相互关联	Alert
	重复告警自动关闭	7日内第二次及第二次以上出现的告警状态置为关闭，并关联7日内同名告警	Alert
	自动更新告警名称	根据客户需要，筛选关键字段信息，拼接告警名称	Alert
	告警打ip标签	告警添加告警关联攻击源IP及目标IP的标签信息	Alert
	一键解封	根据不同的告警数据源产品选择执行不同的解封子流程	Alert
	一键阻断	根据不同的告警数据源产品选择执行不同的阻断子流程	Alert
	关联内外部IP画像情报	告警关联云脑情报、微步情报（优先关联内部情报）	Alert
	资产防护状态统计通知	每周统计客户资产防护状态，同时发送邮件/短信通知给客户	CommonContext
	未关闭高风险告警统计自动通知	每天晚上7点，统计未关闭的告警，并发送邮件/短信通知给客户	Alert

安全防线	流程名称	描述	数据类
	高危告警自动化安全封堵	针对高危和致命告警，源IP地址攻击次数达到阈值(次数>3)且命中微步在线的恶意标签，根据告警来源将该ip对应策略阻断(WAF、VPC、CFW、IAM)	CommonContext
	实时自动关闭告警	对当前告警进行关闭	CommonContext
	关键运维操作实时通知	针对模型产生的运维告警，进行实时通知。目前支持挂载网卡、peering对等连接、资源绑定EIP三种关键运维操作进行SMN通知	Alert
	查询历史告警	告警关联历史处置信息子流程 查询自定义天数的历史告警的评论信息，返回去重后的评论	CommonContext

11.3 安全编排使用流程

安全编排的使用流程如下：

图 11-3 安全编排使用流程

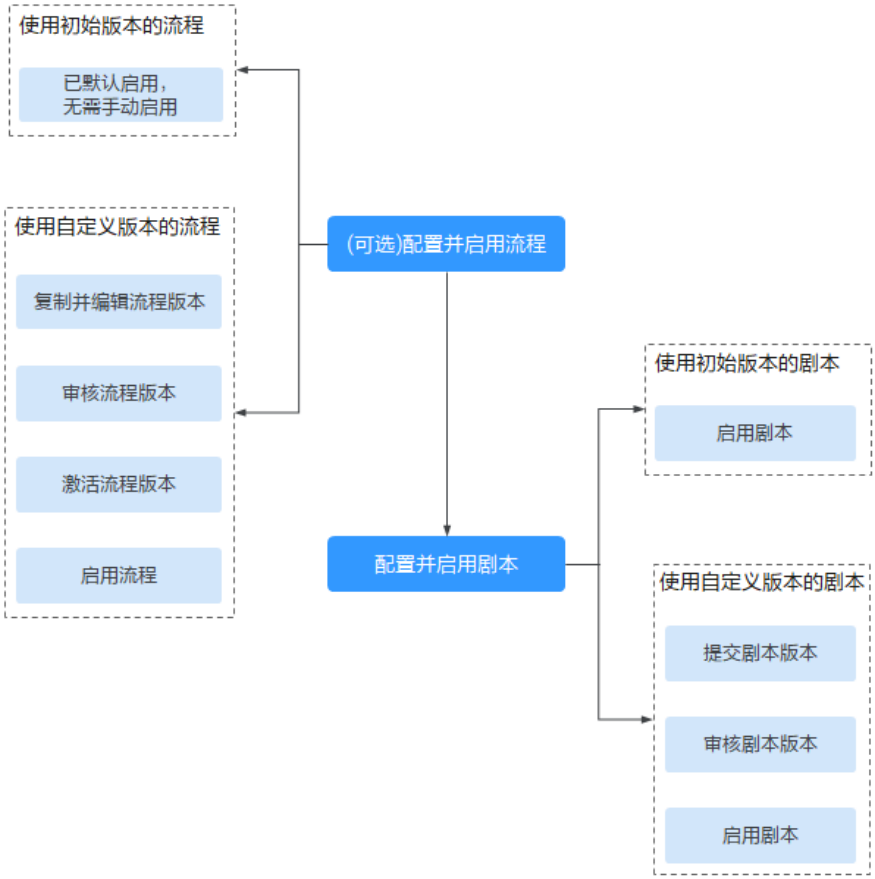


表 11-3 使用流程

序号	操作项	说明
1	（可选）**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）也已启用，无需手动启用。 同时，如果需要对某个流程进行编辑，可以复制初始版本进行处理。

序号	操作项	说明
2	（可选）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。其中，多个剧本已默认启用，无需手动启用。默认已启用以下剧本： 主机告警状态同步、高危漏洞自动通知、主机防线告警关联历史处置信息、云脑WAF地址组关联策略、应用防线告警关联历史处置信息、网络防线告警关联历史处置信息、重复告警自动关闭、告警ip指标打标、资产防护状态统计通知、未关闭告警自动统计通知、高危告警自动通知 如果需要使用某个未启用剧本，可以启用剧本的初始版本（V1，默认已激活），或者对剧本进行修改后再启用。

11.4 （可选）配置并启用流程

操作场景

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）也已启用，无需手动启用。

同时，还支持对已有流程进行自定义编辑，使用自定义流程。本章节将介绍如何配置并启用自定义版本的流程。

启用自定义版本的流程

进入流程管理页面

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-4 进入目标工作空间管理页面

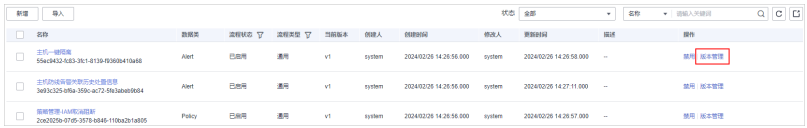
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 11-5 流程管理页面

复制流程版本

步骤5 在目标流程“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 11-6 进入流程版本管理页面



步骤6 在**流程版本管理**页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“复制”，弹出确认框。

步骤7 在弹出的确认框中，单击“确认”。

编辑并提交流程版本

步骤8 在**流程版本管理**页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤9 在流程图绘制页面中，从左侧资源库（提供基础节点、流程节点、插件节点）拖拽节点到右边画布，进行设计。

表 11-4 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11-5**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。

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(如果有一条失败，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(如果有一条失败，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 11-5 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账号中的IAM用户。设置后如有流程需审批，仅设置的责任人可在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10 设计完成后，单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

如果流程校验失败，请根据失败提示进行检查。

审核流程版本

步骤11 编辑并提交流程版本后，页面返回流程管理页面。在**流程管理**页面中，单击目标流程“操作”列“版本管理”，右侧弹出流程版本管理页面。

图 11-7 进入流程版本管理页面

步骤12 在**流程版本管理**页面中，单击目标流程所在行的“操作”列的“审核”，弹出审核确认框。

步骤13 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

激活流程版本

步骤14 在**流程版本管理**页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“激活”。

步骤15 在弹出确认框中，单击“确认”。

启用流程

步骤16 在**流程管理**页面中，单击目标流程所在行的“操作”列的“启用”，页面弹出启用确认框。

步骤17 在弹出的确认框中，选择启用的流程版本后，单击“确定”。

----结束

11.5 （可选）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。其中，多个剧本已默认启用，无需手动启用。默认已启用以下剧本：

主机告警状态同步、高危漏洞自动通知、主机防线告警关联历史处置信息、云脑WAF地址组关联策略、应用防线告警关联历史处置信息、网络防线告警关联历史处置信息、重复告警自动关闭、告警ip指标打标、资产防护状态统计通知、未关闭告警自动统计通知、高危告警自动通知

如果需要使用某个未用剧本，可以启用剧本的初始版本（V1，默认已激活），或者对剧本进行修改后再启用。

本章节主要介绍配置并启用剧本。

- 启用初始版本的剧本
- 启用自定义版本的剧本

启用初始版本的剧本

步骤1 登录管理控制台。

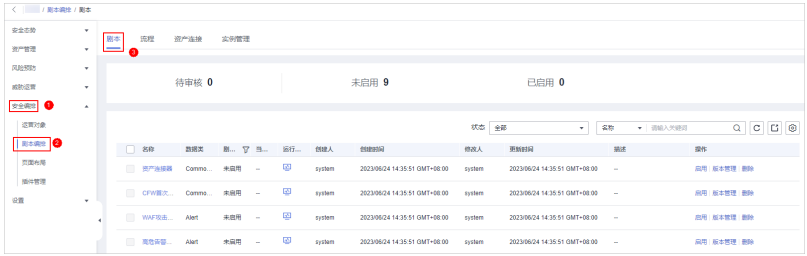
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-8 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-9 进入剧本管理页面



步骤5 在待启用剧本所在行“操作”列，单击“启用”，弹出启用确认信息框。

步骤6 选择启用的剧本版本后，单击“确认”。

----结束

启用自定义版本的剧本

进入剧本管理页面

步骤1 登录管理控制台。

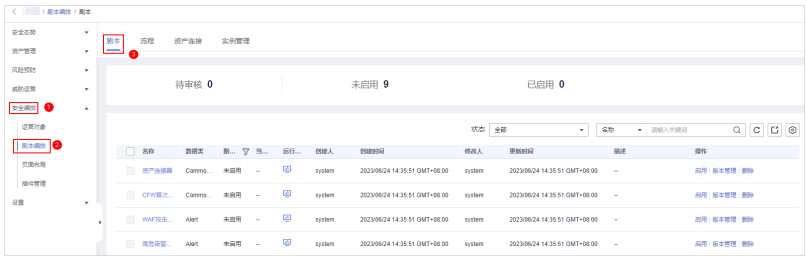
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

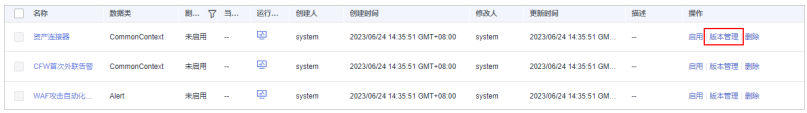
图 11-11 进入剧本管理页面



复制剧本版本

步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-12 进入剧本版本管理页面



步骤6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“复制”，弹出复制版本页面。

步骤7 在弹出复制版本信息框中，单击“确认”。

编辑并提交剧本版本

步骤8 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“编辑”，弹出编辑版本页面。

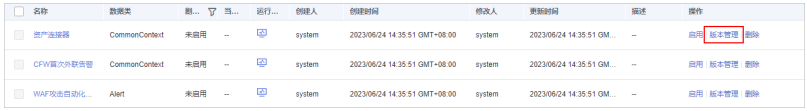
步骤9 在剧本版本编辑页面，编辑版本信息。

步骤10 单击“确定”。

审核剧本版本

步骤11 编辑并提交剧本版本后，页面返回剧本管理页面。在**剧本管理**页面中，单击目标剧本“操作”列“版本管理”，右侧弹出剧本版本管理页面。

图 11-13 进入剧本版本管理页面



步骤12 在**剧本版本管理**页面中，单击目标剧本版本所在行的“操作”列的“审核”，弹出审核确认框。

步骤13 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

启用剧本

步骤14 在**剧本管理**页面中，单击目标剧本所在行的“操作”列的“启用”，页面弹出启用确认框。

步骤15 在弹出的确认框中，选择启用的剧本版本后，单击“确定”。

----结束

11.6 运营对象管理

11.6.1 数据类

11.6.1.1 查看已有数据类

操作场景

安全编排与响应中的剧本和流程的运行都需要绑定数据类，由数据对象（数据类的实例）触发剧本。

本章节介绍如何查看已有数据类。

操作步骤

步骤1 登录管理控制台。

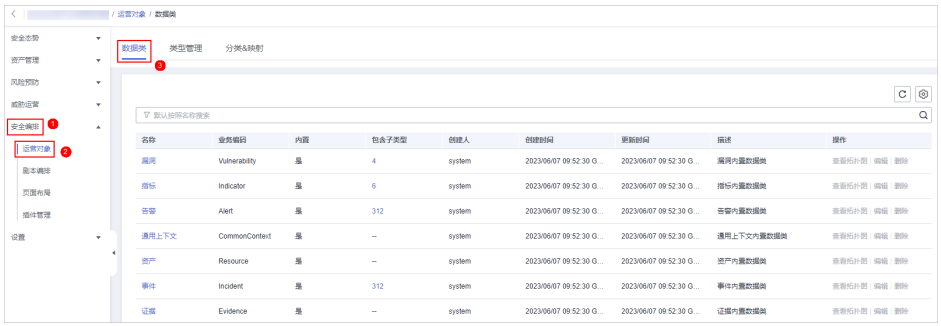
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-14 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 运营对象”，默认进入运营对象的数据类管理页面。

图 11-15 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 11-6 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

11.6.2 类型管理

11.6.2.1 管理告警类型

操作场景

本章节介绍如何管理告警类型，详细操作如下：

- **查看已有告警类型**：**查看**已有的告警类型及其详细信息。
- **新增告警类型**：介绍如何自定义**新增**告警类型。
- **告警类型关联布局**：介绍如何将自定义新增的告警类型**关联已有布局**。
- **编辑已有告警类型**：介绍如何**编辑**自定义新增的告警类型。
- **管理已有告警类型**：介绍如何**启用**、**禁用**、**删除**自定义新增的告警类型。

约束与限制

- 系统内置告警类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置告警类型默认处于启用状态，且暂**不支持**进行编辑、禁用、删除操作。
- 自定义告警类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

查看已有告警类型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-16 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-17 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11-7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。

表 11-7 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 在页面左上角单击 ☰，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 11-18 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-19 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 11-8 新增告警类型参数说明

参数名称	参数说明
类型名称	自定义新增告警类型的名称。
类型标识	填写告警类型标识。标识关键字需遵循大驼峰命名规范，例如TypeTag。
子类型	填写告警类型的子类型。
子类型标识	填写告警子类型标识。标识关键字需遵循大驼峰命名规范，例如SubTypeName。
启动状态	设置告警类型的启动状态。 •  ：表示启用。 •  ：表示禁用。

参数名称	参数说明
SLA	设置告警的SLA处理时间。
描述	自定义告警类型描述信息。

说明

自定义告警类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

步骤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

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 在页面左上角单击 ☰，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 11-20 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-21 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。

步骤2 在页面左上角单击 ☰，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 11-22 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-23 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 11-9 编辑告警类型参数说明

参数名称	参数说明
类型名称	告警类型的名称，**不支持修改**。
类型标识	告警类型标识，**不支持修改**。
子类型	填写告警类型的子类型。
子类型标识	告警子类型标识，**不支持修改**。
启动状态	设置告警类型的启动状态。 •  ：表示启用。 •  ：表示禁用。
SLA	设置告警的SLA处理时间。
描述	自定义告警类型描述信息。

步骤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 在页面左上角单击 ☰，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 11-24 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-25 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。

表 11-10 管理已有告警类型

操作	操作说明
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. 在弹出的确认框中，单击“确认”。

----结束

11.6.2.2 管理事件类型

操作场景

本章节介绍如何管理事件类型，详细操作如下：

- **查看已有事件类型**：**查看**已有的事件类型及其详细信息。
- **新增事件类型**：介绍如何自定义**新增**事件类型。
- **事件类型关联布局**：介绍如何将自定义新增的事件类型**关联已有布局**。
- **编辑已有事件类型**：介绍如何**编辑**自定义新增的事件类型。
- **管理已有事件类型**：介绍如何**启用**、**禁用**、**删除**自定义新增的事件类型。

约束与限制

- 系统内置事件类型已默认关联已有布局，暂**不支持**自定义关联布局。
- 系统内置事件类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义事件类型新增成功后，**不支持**修改“类型名称”、“类型标识”、“子类型标识”参数信息。

查看已有事件类型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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，查看已有事件类型的详细信息，参数说明如**表11-11**所示。

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。
子类型/子类型标识	事件子类型的名称和标识。
关联布局	事件类型已关联的布局。
启用状态	事件类型的启用状态。 • 启用：当前类型已启用。 • 禁用：当前类型已被禁用。
SLA	事件类型的SLA处理时间。
描述	事件类型的描述信息。
操作	可以对事件类型进行编辑、删除等操作。

----结束

新增事件类型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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单击“新增”，右侧弹出新增事件类型页面。在新增事件类型页面中，配置事件类型参数。

表 11-12 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。

参数名称	参数说明
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 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-31 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 在页面左上角单击 ☰，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 11-32 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-13 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 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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“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 11-14 管理已有事件类型

操作	操作说明
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. 在弹出的确认框中，单击“确认”。

----结束

11.6.2.3 查看威胁情报

操作场景

本章节介绍如何查看威胁情报类型。

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。

查看已有威胁情报类型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-36 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-37 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，查看已有威胁情报的详细信息，参数说明如表11-15所示。

表 11-15 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

11.6.2.4 管理漏洞类型

操作场景

本章节介绍如何管理漏洞类型，详细操作如下：

- **查看已有漏洞类型**：**查看**已有的漏洞类型及其详细信息。
- **新增漏洞类型**：介绍如何自定义**新增**漏洞类型。
- **漏洞类型关联布局**：介绍如何将自定义新增的漏洞类型**关联已有布局**。
- **编辑已有漏洞类型**：介绍如何**编辑**自定义新增的漏洞类型。
- **管理已有漏洞类型**：介绍如何**启用**、**禁用**、**删除**自定义新增的漏洞类型。

约束与限制

- 系统内置漏洞类型暂**不支持**自定义关联布局。
- 系统内置漏洞类型默认处于启用状态，暂**不支持**进行编辑、启用、禁用、删除操作。
- 自定义漏洞类型新增成功后，**不支持**修改类型标识。

查看已有漏洞类型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-38 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-39 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11-16所示。

表 11-16 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 在页面左上角单击 ☰，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 11-40 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-41 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 11-17 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。

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 在页面左上角单击  ，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 11-42 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-43 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

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 在页面左上角单击 ☰，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 11-44 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-45 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 11-18 漏洞类型参数说明

参数名称	参数说明
类型名称	自定义漏洞类型的名称。
类型标识	漏洞类型标识，**不支持修改**。
启动状态	设置漏洞类型的启动状态。 •  ：表示启用。 •  ：表示禁用。
描述	自定义漏洞的描述信息。

步骤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 在页面左上角单击 ☰，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 11-46 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-47 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。

表 11-19 管理已有漏洞类型

操作	操作说明
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. 在弹出的确认框中，单击“确认”。

----结束

11.6.2.5 查看自定义类型

操作场景

本章节介绍如何查看自定义类型。

约束与限制

系统内置的类型和子类型**不支持**关联布局、编辑、删除、启用和禁用。

其中，内置的**IP**和**主机**（物理机和虚拟机）类型可以执行启用和禁用操作，实现“资产管理”页面中展示类型的控制，详细操作请参见**如何自定义导入主机资产？**、**如何让IP类型资产在资产管理页面中显示？**。

查看已有的自定义类型/子类型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-48 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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“自定义类型”页签，进入自定义类型管理页面后，查看已有自定义类型/子类型的详细信息。

- 左侧显示类型列表，展示已有的类型。
- 如需查看某个类型的详细信息，请单击左侧类型列表中类型的名称，右侧将展示类型的详细信息。具体信息如下：
  - 目标类型的基本信息：名称、创建人、创建时间、关联布局。
  - 子类型列表：已有子类型、子类型名称、子类型关联的布局等信息。

----结束

11.6.3 分类&映射

11.6.3.1 查看已有分类映射

操作场景

分类和映射是对云服务告警进行类型匹配和字段映射。

本章节介绍如何查看已有分类映射。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-51 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。

表 11-20 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。

参数名称	参数说明
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

11.6.3.2 创建/复制/编辑分类映射

操作场景

分类和映射是对云服务告警进行类型匹配和字段映射。

本章节介绍如何创建、编辑、复制分类映射。

约束与限制

- 单账号单workspace内，分类&映射模板 ≤ 50个。
- 单账号单workspace内，分类和映射的映射关系规格为1:100。
- 单账号单workspace内，最多可新增分类&映射100个。

创建分类映射

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-53 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 11-54 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。
5. 在右侧“映射”页签中，选择映射方式，并配置对应参数。
6. 完成分类映射后，单击页面右上角，保存配置。
7. 在右侧“预处理”页签中，设置预处理映射参数参数。
8. 完成预处理配置后，单击页面右上角，保存配置。

----结束

复制已有的分类映射

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-55 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-56 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“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

编辑分类映射

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-57 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-58 进入分类&映射管理页面

步骤5 在分类映射管理页面中，单击目标分类映射名称，进入编辑页面。

步骤6 在编辑分类映射页面，编辑分类映射参数信息。

1. 在左侧“基本信息配置”栏中，配置分类映射的基本信息，参数说明如表11-21所示。

   表 11-22 配置基本信息

参数名称	参数说明
名称	自定义分类映射名称。
数据类	选择对应的数据类，暂不支持编辑
描述	自定义分类映射描述信息。

2. 选择左侧“数据源”栏中，选择分类映射的数据源。

   当“数据源”选择“上传JSON文件”时，需要单击“上传JSON文件”，并上传JSON文件。
3. 在右侧“分类”页签中，选择分类方式，并配置对应参数。
4. 完成分类配置后，单击页面右上角，保存配置。
5. 在右侧“映射”页签中，选择映射方式，并配置对应参数。
6. 完成分类映射后，单击页面右上角，保存配置。
7. 在右侧“预处理”页签中，设置预处理映射参数参数。
8. 完成预处理配置后，单击页面右上角，保存配置。

----结束

11.6.3.3 管理分类映射

操作场景

本章节介绍如何管理分类映射，如启用、禁用、删除操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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，对分类映射进行管理。

表 11-23 管理分类映射

操作	操作说明
启用 **说明** 自定义新增的分类映射暂不支持启用操作。	在分类映射管理页面中，单击目标分类映射所在行“启用状态”列的禁用按钮。 当“启用状态”更新为“启用”时，表示启用成功。
禁用 **说明** 自定义新增的分类映射暂不支持禁用操作。	在分类映射管理页面中，单击目标分类映射所在行“启用状态”列的启用按钮。 当“启用状态”更新为“禁用”时，表示禁用成功。
删除 **说明** 暂不支持删除系统内置分类映射。	1. 在分类映射管理页面中，单击目标分类映射所在行“操作”列的“删除”。 2. 在弹出的删除映射确认框中，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

11.7 剧本编排管理

11.7.1 剧本

11.7.1.1 提交剧本版本

操作场景

本章节主要介绍如何提交剧本版本。

前提条件

已启用剧本绑定的流程，具体操作请参见**启用流程**。

操作步骤

步骤1 登录管理控制台。

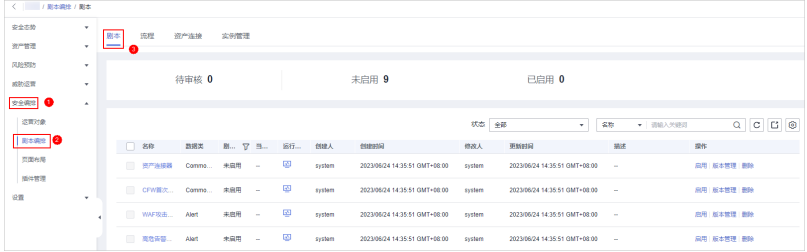
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

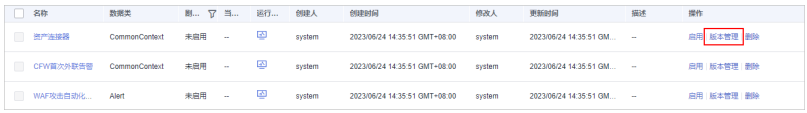
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-62 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-63 进入剧本版本管理页面



步骤6 在剧本版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“提交”，弹出提交审核确认框。

步骤7 在确认框中，单击“确认”，提交剧本版本。

说明

- 剧本版本提交后“版本状态”变为“待审核”。
- 剧本版本提交后不可以再编辑，如果需要编辑可以新建版本，或者在审核中驳回提交。

----结束

后续处理

剧本版本提交后，需要进行审核，详细操作请参见**审核剧本版本**。

11.7.1.2 审核剧本版本

操作场景

本章节主要介绍如何审核剧本版本。

前提条件

已提交剧本，具体操作请参见**提交剧本版本**。

操作步骤

步骤1 登录管理控制台。

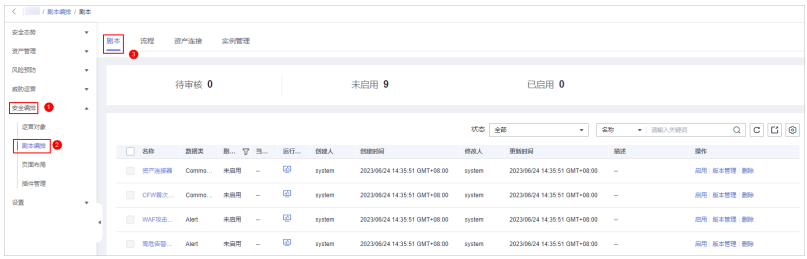
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-64 进入目标工作空间管理页面

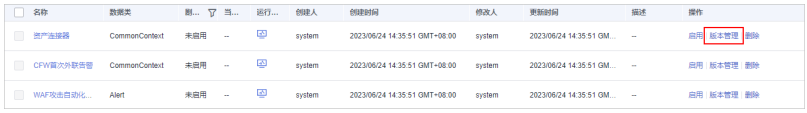
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-65 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-66 进入剧本版本管理页面



步骤6 在版本管理页面中，单击“审核”，弹出审核剧本版本页面。

步骤7 在审核剧本版本页面，填写审核信息，审核剧本版本参数说明如表11-24所示。

表 11-24 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**。

11.7.1.3 启用剧本

操作场景

完成剧本版本审核后可启用剧本，本章节主要介绍如何启用剧本。

前提条件

已激活剧本版本，具体操作请参见**激活/失活剧本版本**。

操作步骤

步骤1 登录管理控制台。

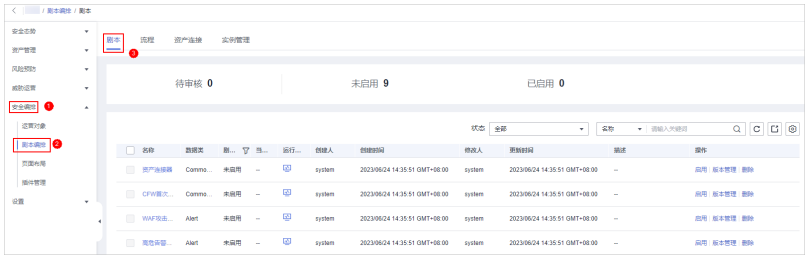
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-68 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

11.7.1.4 管理剧本

操作场景

本章节将介绍如何执行**查看已有剧本**、**导出剧本信息**、**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。

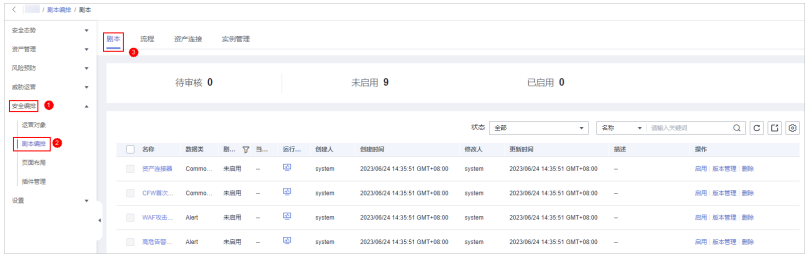
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

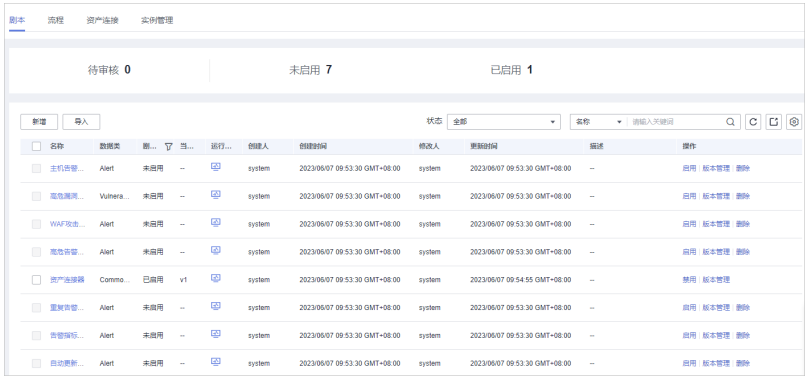
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-70 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 11-71 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 11-25 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。

参数名称	参数说明
剧本状态	剧本当前状态。当前分为已启用和未启用两种状态。
当前版本	剧本当前版本。
运行监控	单击，查看剧本运行监控。 – 选择时间：选择查看的监控时间。支持最近24小时、最近3天、最近30天和最近90天的查询。 – 版本：选择查看的监控版本。支持全部、当前有效和已删除类型的查询。 – 运行次数：提供查看剧本的运行总次数、定时触发次数和事件触发次数。 – 平均运行时长：提供查看平均运行时长、最长运行时长和最短运行时长。其中，平均运行时长=实例运行总时长/实例总个数。 – 实例状态统计：提供查看实例运行总个数、运行成功个数、运行中的实例个数、运行失败个数和终止个数。
创建人	创建该剧本的用户。
创建时间	剧本的创建时间。
修改人	最近一次修改该剧本的用户。
更新时间	剧本最近一次更新的时间。
描述	剧本的描述信息。

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。

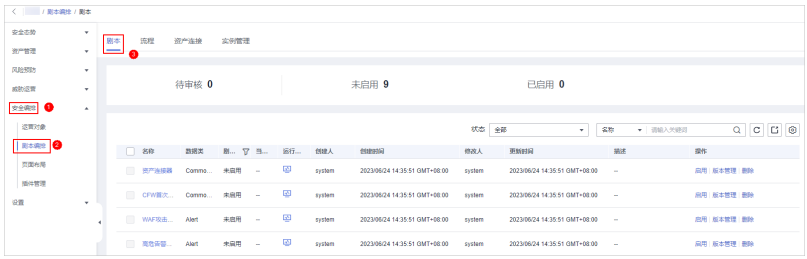
步骤2 在页面左上角单击，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-72 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-73 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

禁用剧本

步骤1 登录管理控制台。

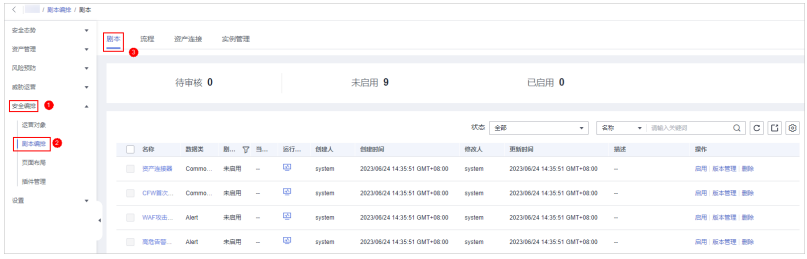
步骤2 在页面左上角单击，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-74 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-75 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。

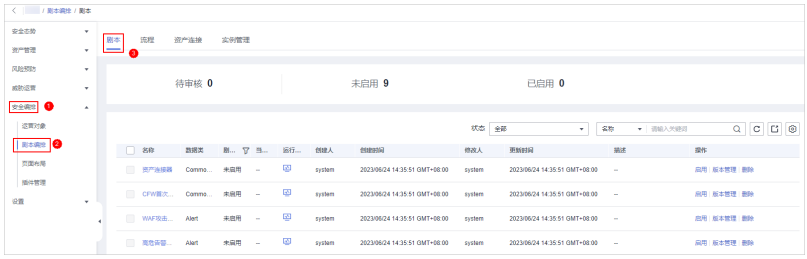
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-76 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-77 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

11.7.1.5 管理剧本版本

操作场景

本章节将介绍如何执行**预览剧本版本**、**编辑剧本版本**、**激活/失活剧本版本**、**复制剧本版本**、**删除剧本版本**等操作。

预览剧本版本

说明

草稿版本暂不支持预览。

步骤1 登录管理控制台。

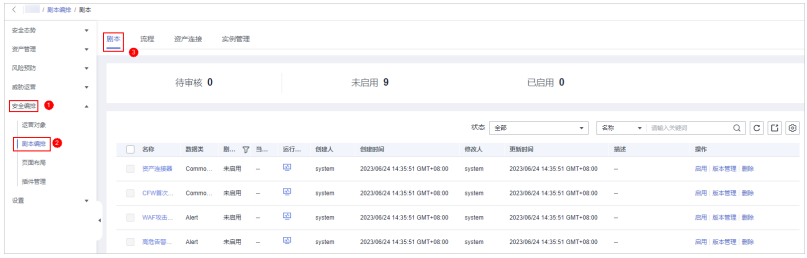
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

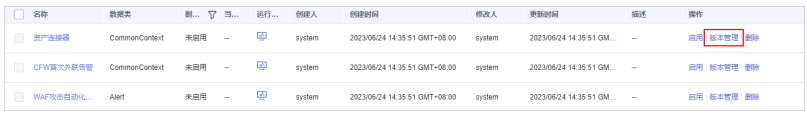
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-79 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-80 进入剧本版本管理页面



步骤6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“预览”，弹出预览版本页面。

步骤7 在剧本版本预览页面，查看目标剧本版本的详情，包括“基本信息”、“版本信息”、“匹配流程”等。

----结束

编辑剧本版本

说明

仅支持对版本状态为“未提交”的剧本版本进行编辑。

步骤1 登录管理控制台。

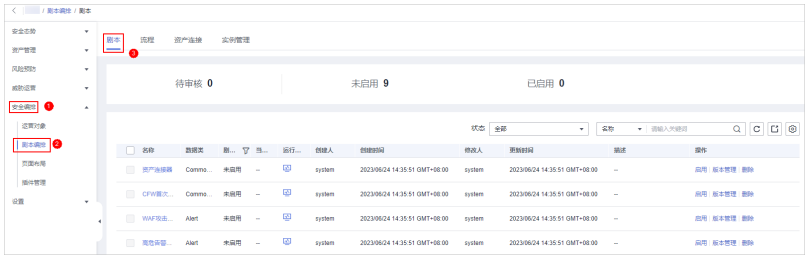
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-81 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-82 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-83 进入剧本版本管理页面

步骤6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“编辑”，弹出编辑版本页面。

步骤7 在剧本版本编辑页面，编辑版本信息。

步骤8 单击“确定”，完成剧本的编辑。

----结束

激活/失活剧本版本

说明

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

步骤1 登录管理控制台。

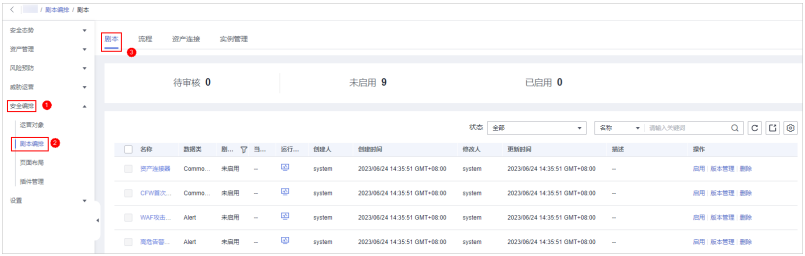
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-84 进入目标工作空间管理页面

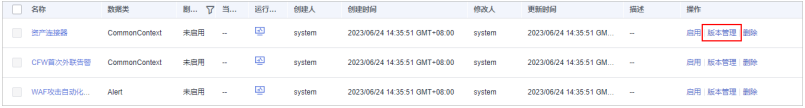
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-85 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-86 进入剧本版本管理页面



步骤6 在版本管理页面中，单击“版本信息”栏中目标剧本版本所在行“操作”列的“激活”（或“取消激活”），完成激活（或失活）操作。

----结束

复制剧本版本

说明

仅支持复制“已激活”、“未激活”的剧本版本。

步骤1 登录管理控制台。

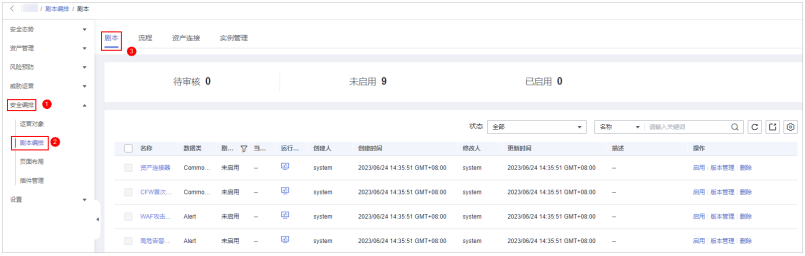
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-87 进入目标工作空间管理页面

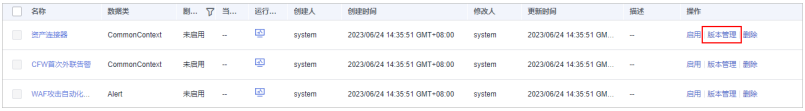
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-88 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-89 进入剧本版本管理页面



步骤6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“复制”，弹出复制版本页面。

步骤7 在弹出复制版本信息框中，单击“确认”，完成复制剧本版本。

----结束

删除剧本版本

说明

删除剧本版本需要**全部满足**以下条件：

- 剧本版本处于失活状态。
- 不存在正在运行的剧本版本实例。

步骤1 登录管理控制台。

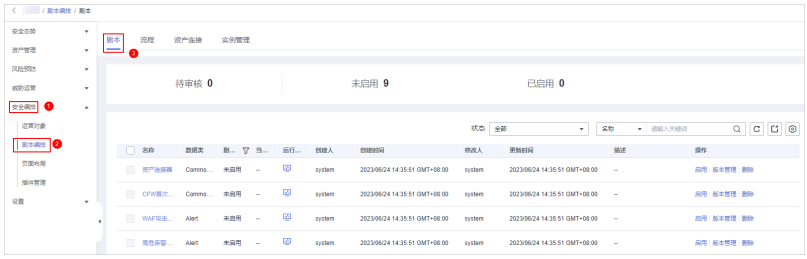
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-90 进入目标工作空间管理页面

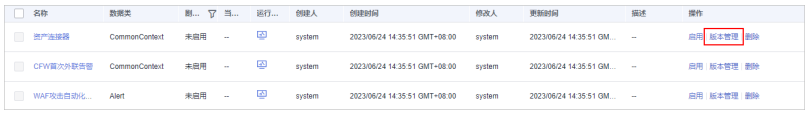
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 11-91 进入剧本管理页面



步骤5 在目标剧本“操作”列，单击“版本管理”，弹出剧本版本管理页面。

图 11-92 进入剧本版本管理页面



步骤6 在版本管理页面中，单击“版本信息”栏中目标版本所在行“操作”列的“删除”，完成删除剧本版本。

说明

剧本版本删除后，不可找回，请谨慎操作。

----结束

11.7.2 流程

11.7.2.1 审核流程版本

操作场景

本章节主要介绍如何审核流程版本。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

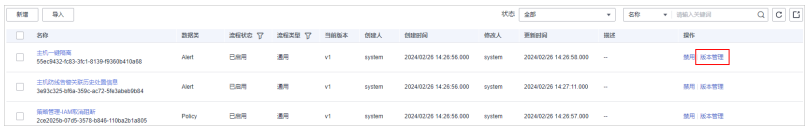
图 11-93 进入目标工作空间管理页面

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

图 11-94 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 11-95 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11-26**所示。

表 11-26 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**。

11.7.2.2 启用流程

操作场景

本章节主要介绍如何启用流程。

前提条件

已激活流程版本，具体操作请参见**管理流程版本**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

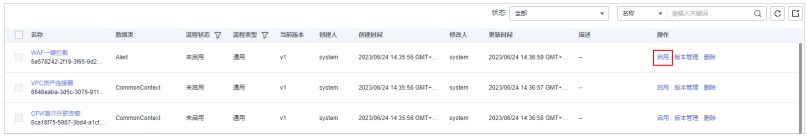
图 11-96 进入目标工作空间管理页面

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

图 11-97 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 11-98 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

11.7.2.3 管理流程

操作场景

本章节将介绍如何**查看流程**、**导出流程**、**删除流程**、**禁用流程**。

查看流程

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

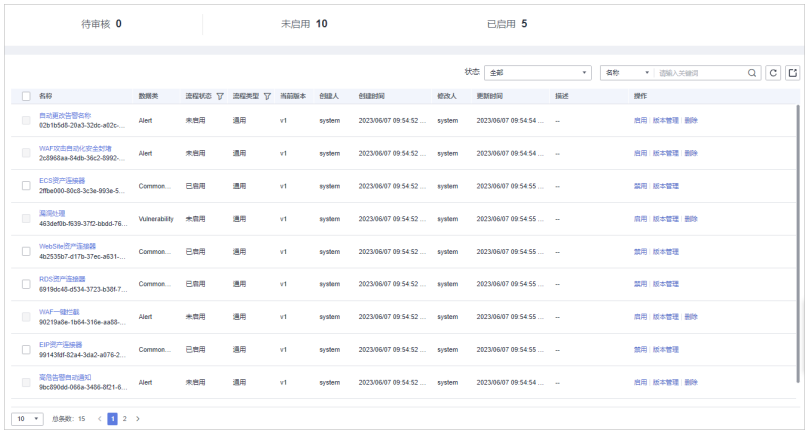
图 11-99 进入目标工作空间管理页面

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

图 11-100 流程管理页面

步骤5 在流程管理页面中，查看已创建流程的信息。

图 11-101 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。

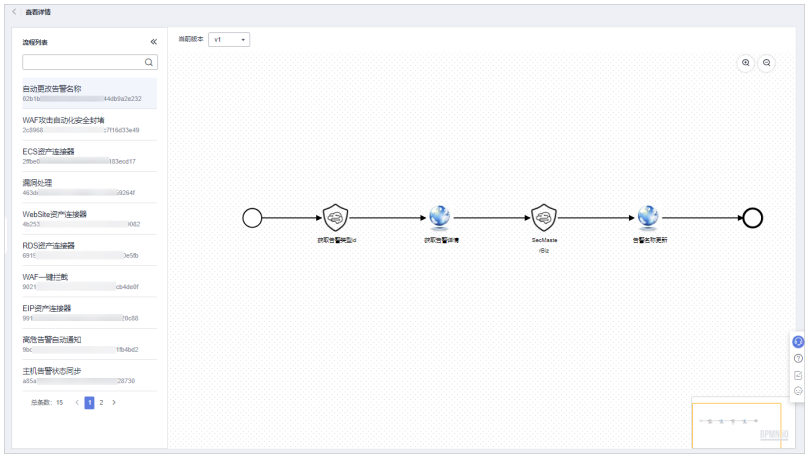
表 11-27 流程参数说明

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。
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。

参数名称	参数说明
描述	流程的描述信息。
操作	用户可以在操作栏中，执行启用、版本管理等操作。

步骤6 如需查看某个流程的详细信息，可单击待查看流程的名称，进入流程详情页面查看流程的详细信息。

图 11-102 流程详情示例



----结束

导出流程

说明

支持导出“流程状态”为“已启用”的流程。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-103 进入目标工作空间管理页面

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

图 11-104 流程管理页面

步骤5 在流程管理页面中，勾选需导出的流程，并单击列表右上角的，弹出导出流程确认框。

步骤6 在弹出的确认框中，单击“确认”，系统将导出流程信息到本地。

----结束

删除流程

说明

删除流程需要**全部满足**下列条件：

- “流程状态”为“未启用”。
- 当前流程中不存在激活的流程版本。

步骤1 登录管理控制台。

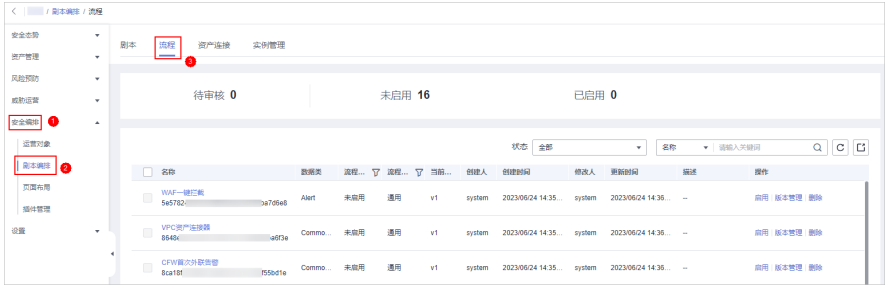
步骤2 在页面左上角单击，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-105 进入目标工作空间管理页面

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

图 11-106 流程管理页面



步骤5 在流程管理页面中，单击目标流程所在行“操作”列的“删除”，弹出删除流程确认框。

步骤6 单击“确认”，删除流程。

说明

删除时，默认删除当前流程中的所有历史版本，删除后不可恢复，请谨慎操作。

----结束

禁用流程

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-107 进入目标工作空间管理页面

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

图 11-108 流程管理页面

步骤5 在目标流程所在行的“操作”列，单击“禁用”，页面弹出禁用确认框。

步骤6 在弹出的确认框中，单击“确认”，完成流程禁用。

----结束

11.7.2.4 管理流程版本

操作场景

本章节将介绍如何**复制流程版本**、**编辑流程版本**、**提交流程版本**、**激活/失活流程版本**、**删除流程版本**。

复制流程版本

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

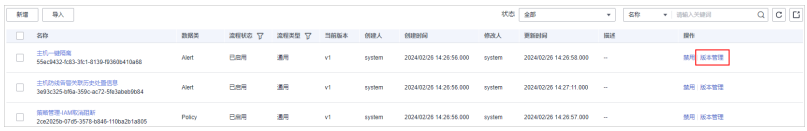
图 11-109 进入目标工作空间管理页面

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

图 11-110 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 11-111 进入流程版本管理页面



步骤6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“复制”，弹出确认框。

步骤7 在弹出的确认框中，单击“确认”，完成复制流程版本。

----结束

编辑流程版本

说明

支持对“版本状态”为“待提交”或“审核驳回”的流程版本进行编辑。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 11-112 进入目标工作空间管理页面

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

图 11-113 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 11-114 进入流程版本管理页面

步骤6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤7 在流程图绘制页面中，从左侧资源库（提供基础节点、流程节点、插件节点）拖拽节点到右边画布，进行设计。

表 11-28 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。

参数名称			参数说明
		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11-29**所示。
		子流程	另起一个流程，主要用于执行循环操作。相当于流程中的循环体。
	系统插件	排他网关	线路分流时，根据条件表达式选择多条线路中的一条执行。 线路汇聚时，多条线路只要有一条线路到达则继续后面的节点执行。
		并行网关	线路分流时，所有线路都会执行。 线路汇聚时，多条线路全部到达，才会继续后续节点的执行(如果有一条失败，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(如果有一条失败，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 11-29 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。

参数名称	参数说明
处理人	设置此流程的审核处理人为当前账号中的IAM用户。设置后如有流程需审批，仅设置的责任人可在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8 设计完成后，单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

如果流程校验失败，请根据失败提示进行检查。

----结束

提交流程版本

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

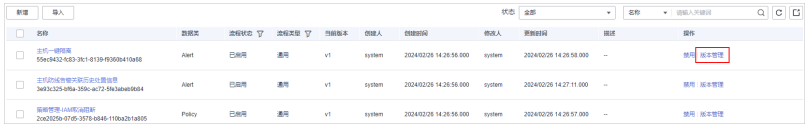
图 11-115 进入目标工作空间管理页面

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

图 11-116 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 11-117 进入流程版本管理页面



步骤6 在流程版本管理页面中，单击“版本信息”栏中目标流程所在行的“操作”列的“提交”，弹出提交确认框。

图 11-118 提交流程版本

步骤7 在确认框中，单击“确认”，提交流程版本。

说明

- 流程版本提交后“版本状态”更新为“待审核”。
- 流程版本提交后不可以再编辑，如果需要编辑可以新建版本，或者在审核中驳回提交。

----结束

激活/失活流程版本

说明

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

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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。

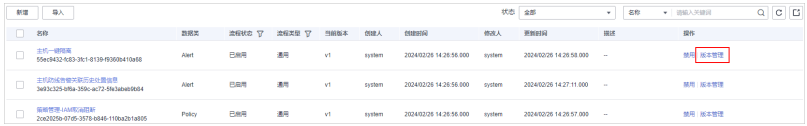
图 11-119 进入目标工作空间管理页面

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

图 11-120 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 11-121 进入流程版本管理页面



步骤6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“激活”或者“取消激活”。

图 11-122 取消激活示例

步骤7 在弹出确认框中，单击“确认”，完成激活/失活操作。

----结束

删除流程版本

步骤1 登录管理控制台。

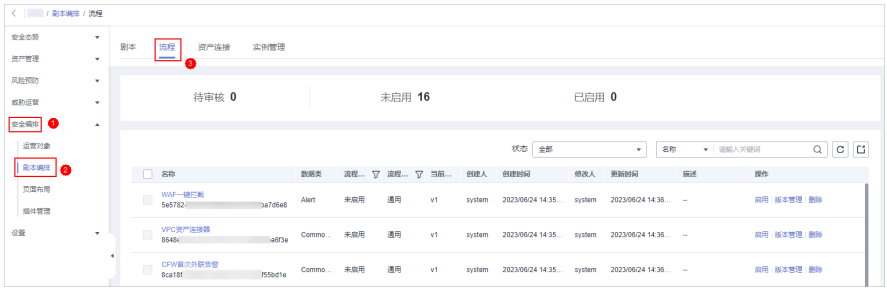
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-123 进入目标工作空间管理页面

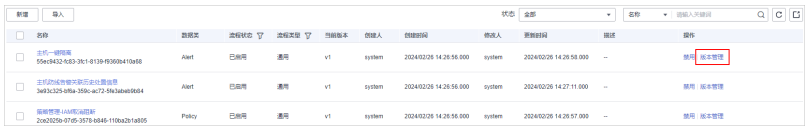
步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

图 11-124 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 11-125 进入流程版本管理页面



步骤6 在流程版本管理页面中，单击“版本信息”栏中目标流程版本所在行的“操作”列的“删除”，并在弹出的确认框中，单击“确认”，删除流程版本。

说明

流程版本删除后，不可找回，请谨慎操作。

----结束

11.7.3 资产连接

11.7.3.1 新增资产连接

操作场景

本章节主要介绍如何新建资产连接。

操作步骤

步骤1 登录管理控制台。

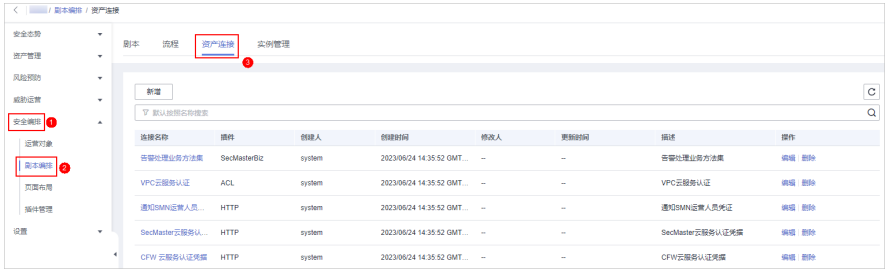
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 11-127 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11-30所示。

表 11-30 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。
连接类型	选择资产连接的类型。
凭证信息	根据选择的连接类型填写凭证信息，例如AK、SK等。

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

11.7.3.2 管理资产连接

操作场景

本章节主要介绍如何**查看资产连接**、**编辑资产连接**、**删除资产连接**。

查看资产连接

步骤1 登录管理控制台。

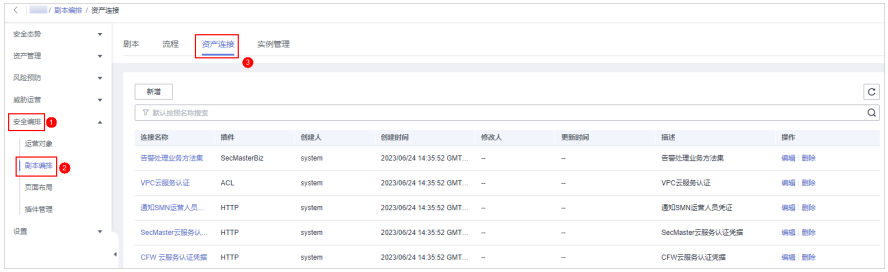
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 11-129 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 11-130 查看资产连接信息

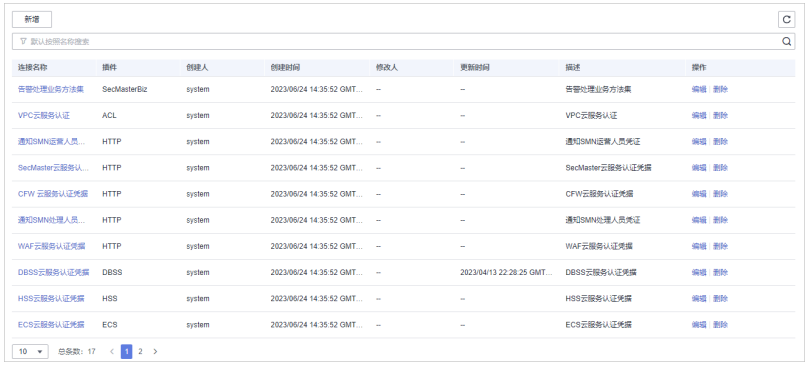


表 11-31 资产连接参数说明

参数名称	参数说明
连接名称	资产连接的名称。
插件	资产连接对应的插件。
创建人	创建资产连接的用户。
创建时间	资产连接的创建时间。
修改人	最近一次修改资产连接的用户。
更新时间	资产连接最近一次更新的时间。
描述	资产连接的描述信息。
操作	用户可以在操作栏中，执行编辑、删除操作。

步骤6 如需查看某个资产连接的详细信息，可单击待查看资产连接的名称，进入资产连接详情页面进行查看。

----结束

编辑资产连接

步骤1 登录管理控制台。

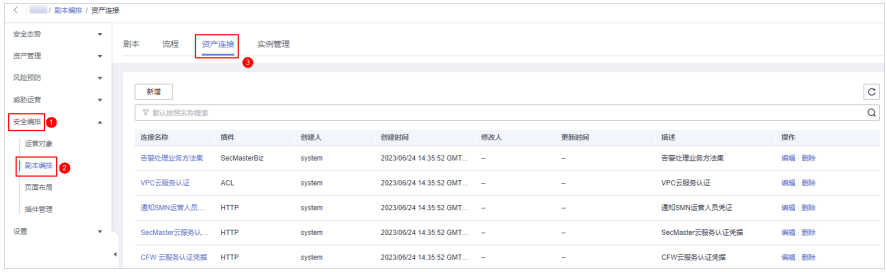
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 11-132 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11-32所示。

表 11-32 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**。
连接类型	选择资产连接的类型。
凭证信息	根据选择的连接类型填写凭证信息，例如AK、SK等。

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。

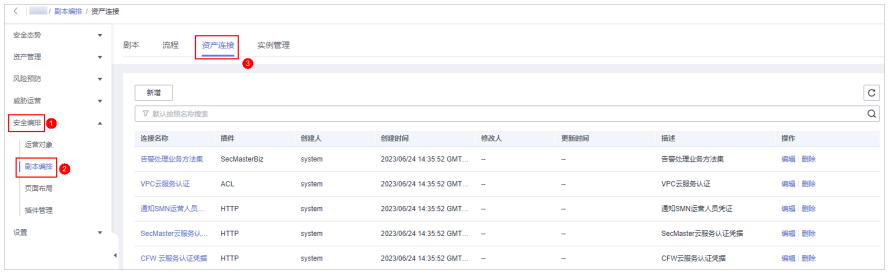
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 11-134 资产连接管理页面



步骤5 在目标连接所在行“操作”列，单击“删除”，弹出删除确认框。

步骤6 在弹出的确认框中，单击“确认”，完成资产连接删除。

说明

资产连接删除后，不可找回，请谨慎操作。

----结束

11.7.4 实例管理

11.7.4.1 查看剧本实例监控

操作场景

当剧本执行完成后，剧本实例管理列表中会生成剧本实例，即剧本实例监控。实例监控列表每条记录是一个实例，可呈现实例的历史实例任务列表，以及历史实例任务的运行情况。

本章节主要介绍如何查看实例监控信息。

约束与限制

单账号单workspace内一天内的重试次数限制如下：

- 手动重试：流程实例最大重试次数100次。重试之后，等剧本执行完毕之后才允许再次重试。
- API接口重试：流程实例最大重试次数100次。重试之后，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。

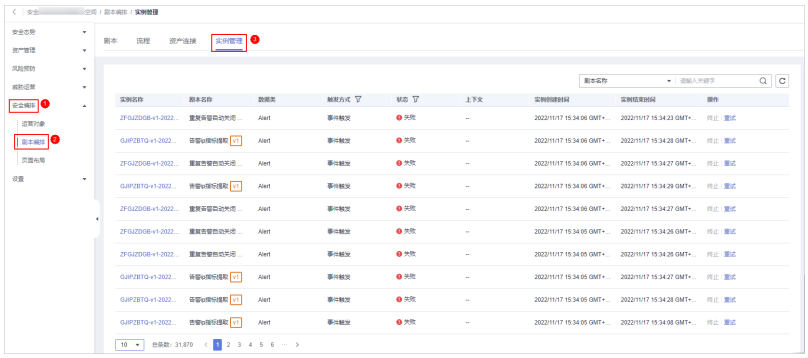
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

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

图 11-136 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11-33所示。

图 11-137 实例信息

表 11-33 实例列表参数

参数名称	参数说明
实例名称	实例的名称。

参数名称	参数说明
剧本名称	实例对应的剧本名称。
数据类	剧本的运营对象，即数据类。
触发方式	实例的触发方式。 ● 定时触发 ● 事件触发
状态	实例的状态。 ● 成功：剧本实例成功执行。 ● 失败：剧本实例执行失败，单击操作列的重试可重新执行剧本。 ● 运行中：剧本实例处于运行状态，单击操作列的终止可终止剧本。 ● 重试中：剧本实例正在重试中。 ● 终止中：剧本实例正在终止。 ● 已终止：剧本实例已经成功终止。
上下文	实例的上下文信息。
实例创建时间	实例创建的具体时间。
实例结束时间	实例结束的具体时间。
操作	用户可执行终止、重试等操作。

步骤6 如需查看某个实例的详细信息，可以单击任一实例名称，进入剧本实例图页面，可查看实例流程图和流程节点信息。

----结束

11.8 页面布局管理

11.8.1 查看已有布局模板

操作场景

布局中已有**告警管理**、**事件管理**、**漏洞管理**、**分析报告**、**情报管理**、**安全大屏**页面布局的管理页和详情页面模板。

本章节主要介绍如何查看已有布局模板。

操作步骤

步骤1 登录管理控制台。

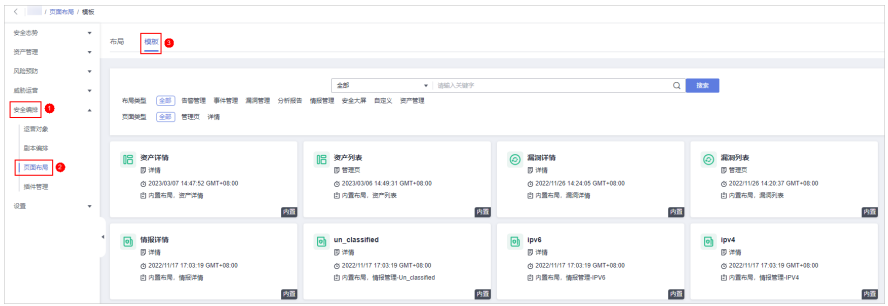
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-138 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 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 11-139 进入布局模板页面



步骤5 在布局模板页面，查看模板信息。

可以通过“布局类型”、“页面类型”，并输入关键字来搜索指定布局模板。

- 可以查看当前已有模板的名称、页面类型、创建时间等信息。
- 可以对已有模板的名称、模板内的布局进行编辑。
- 可以删除已有模板。

----结束

11.8.2 查看已有布局

操作场景

本章节将介绍如何**查看已有布局**。

查看已有布局

步骤1 登录管理控制台。

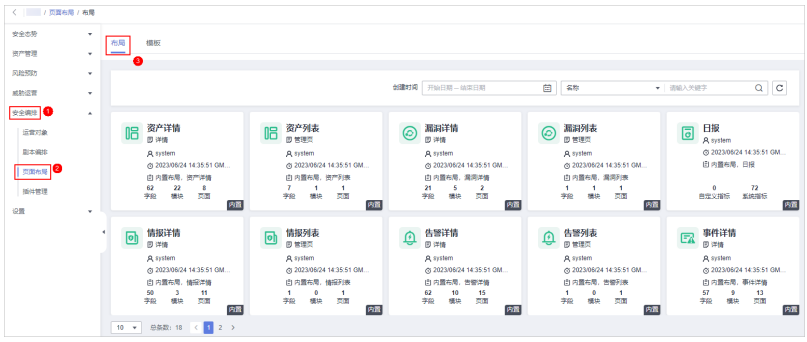
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-140 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 页面布局”，默认进入页面布局管理页面。

图 11-141 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

11.9 插件管理

11.9.1 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。
- **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。

11.9.2 查看插件详情

操作场景

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。

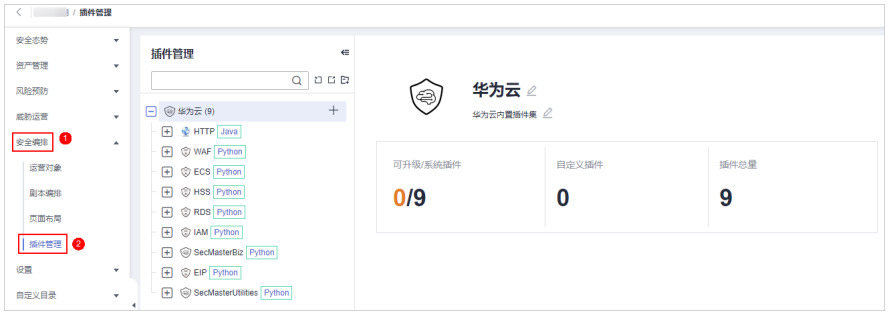
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 11-142 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 插件管理”，进入插件管理页面。

图 11-143 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

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Linux系统x86_64架构的ECS主机上。ECS主机支持以下操作系统类型：Huawei Cloud EulerOS 2.5、Huawei Cloud EulerOS 2.9、EulerOS 2.5、EulerOS 2.9、CentOS 7.9。
- 安装Agent时，在控制台中查看信息时，仅支持使用IAM账号登录。

采集器规格

采集管理中，采集器规格说明如下：

表 12-1 采集器规格

规格	参考处理能力
4U8G50G100G	2000 EPS @ 1KB
8U16G50G100G	5000 EPS @ 1KB
16U32G50G100G	10000 EPS @ 1KB

日志源的数量

采集器支持的日志源数量不受限制，可随云资源配置变化而动态扩展。

12.1.2 采集数据

操作场景

本章节介绍如何采集数据。

步骤一：购买 ECS

购买用于采集数据的弹性云服务器，详细操作请参见**购买ECS**。

⚠ 注意

- 数据采集的Agent目前仅支持运行在Linux系统x86_64架构的ECS主机上。ECS主机支持以下操作系统类型：Huawei Cloud EulerOS 2.5、Huawei Cloud EulerOS 2.9、EulerOS 2.5、EulerOS 2.9、CentOS 7.9。
  购买时，需注意操作系统和版本的选择。

  图 12-1 选择操作系统版本

- ECS购买后，系统将根据使用情况进行收费，具体收费情况请参见**ECS计费说明**。
  后续如果不再使用数据采集功能，需要手动释放用于采集数据的ECS资源，详细操作请参见**如何释放ECS和VPC终端节点资源？** 。

步骤二：安装 Agent

1. 安装Agent前预检查。
   a. 执行**ps -ef | grep salt**命令，检查主机之前的salt-minion进程是否残留。
      - 如果有，请先关闭。
      - 如果没有，请继续执行**1.b**。

      图 12-2 检查进程

      ```
      [root@host-192-168-  ~]# ps -ef | grep salt
      root      18749  18315  0 09:28 pts/0    00:00:00 grep --color=auto salt
      root      58881      1  0 Apr11 ?        00:00:00 /usr/bin/python3 /usr/bin/salt-minion
      isap-sa+  58888  58881  0 Apr11 ?        00:01:08 /usr/bin/python3 /usr/bin/salt-minion
      ```

   b. 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

      ```
      [root@ecs-  ~]# df -h
      Filesystem      Size  Used Avail Use% Mounted on
      /dev/vda1        40G  1.7G   36G   5% /
      devtmpfs        7.8G     0  7.8G   0% /dev
      tmpfs           7.8G     0  7.8G   0% /dev/shm
      tmpfs           7.8G  129M  7.7G   2% /run
      tmpfs           7.8G     0  7.8G   0% /sys/fs/cgroup
      /dev/vdb1        98G  8.9G   85G  10% /opt
      /dev/vdb2       108G   61M  103G   1% /var/lib/docker
      tmpfs           1.6G     0  1.6G   0% /run/user/0
      ```

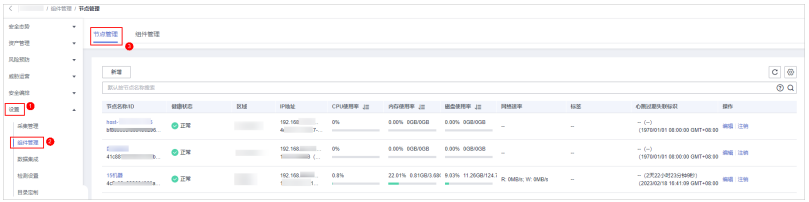
如果内存不足，请关闭一些高内存占用的应用程序或扩充内存容量后再进行安装。扩容操作详情请参见**变更服务器规格**。

2. 登录管理控制台。
3. 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。
4. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 12-4 进入目标工作空间管理页面

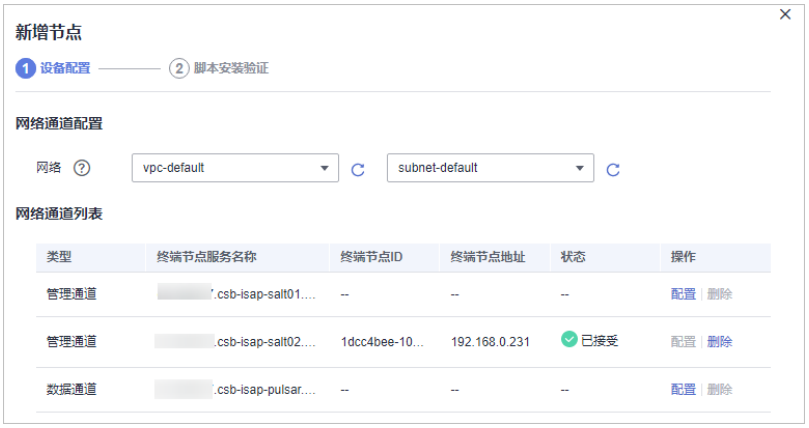
5. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 12-5 进入节点管理页面



6. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
7. 在新增节点页面中，配置设备。

图 12-6 新增节点



a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。
b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。

说明

VPC终端节点（用于连通和管理采集节点）配置后，系统将根据使用情况进行收费，具体收费情况请参见**VPC终端节点计费说明**。

后续如果不再使用数据采集功能，需要手动释放用于连通和管理采集节点的VPC终端节点，详细操作请参见**如何释放ECS和VPC终端节点资源?** 。

8. 单击页面右下角“下一步”，进入脚本安装验证页面后，单击 复制安装Agent的命令。
9. 远程登录待安装Agent的ECS。
   - **华为云主机**
     - 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，详细操作请参见**在云服务器控制台上登录主机**。
     - 如果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：PuTTY、Xshell等）登录主机，并使用root账号在主机中安装Agent。
   - **非华为云主机**

     请使用远程管理工具（例如：PuTTY、Xshell等）连接您服务器的弹性IP，远程登录到您的服务器。
10. 执行**cd /opt/cloud**命令，进入安装目录。

注意

安装路径建议为“/opt/cloud”，本章节也以此路径为例进行介绍。如需安装在其他自定义路径中，请根据路径修改。

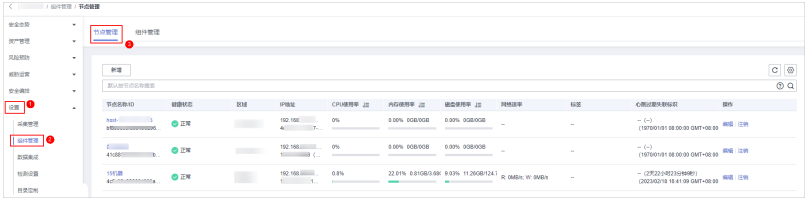
11. 粘贴复制的**8**复制的安装命令，以root权限执行，在ECS中安装Agent。
12. 根据界面提示，输入登录控制台的IAM账号和密码。
13. 如果界面回显类似如下信息时，则表示Agent安装成功。

```
install isap-agent successfully
```

步骤三：新增节点

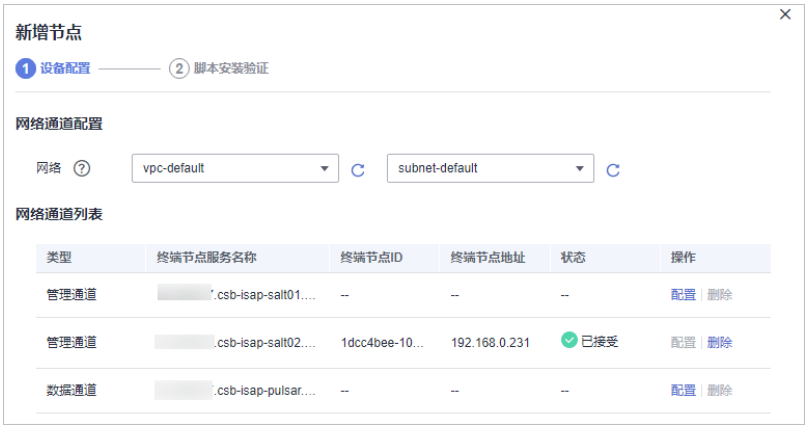
1. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 12-7 进入节点管理页面



2. 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。
3. 在新增节点页面中，配置设备。

图 12-8 新增节点



a. 在网络通道配置栏中，选择网络通道所属的虚拟私有云和子网。

b. 在网络通道列表中，单击通道“操作”列的“配置”，并在弹出的确认框中，单击“确认”。

4. 单击页面右下角“下一步”，进入“脚本安装验证”页面。
5. 确认已安装后，单击页面右下角“确认”。

步骤四：配置组件

1. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

图 12-9 进入组件管理页面

2. 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。
3. 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。
4. 单击页面右下角“保存并应用”。

步骤五：新增数据连接

1. 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 12-10 进入采集管理页面

2. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。
3. 新增数据连接来源。

   在“来源”页签中，选择数据源类型的来源，并根据选择的类型进行参数配置。

   数据源类型来源支持以下类型：传输控制协议 Tcp、文件 File、用户数据协议 Udp、对象存储 Obs、消息队列 Kafka、云脑管道 Pipe
4. 新增数据源连接目的。

   选择“目的”页签中，选择数据源类型的目的，并根据选择的类型进行参数配置。

   数据源类型目的支持以下类型：文件 File、传输控制协议 Tcp、用户数据协议 Udp、消息队列 Kafka、对象存储 Obs、云脑管道 Pipe
5. 设置完成后，单击页面右下角“确认”。

（可选）步骤六：配置解析器

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-11 进入解析器管理页面

2. 支持**•自定义新增**和**•由模板创建**，请根据您的需要进行选择。
   - **自定义新增**
     i. 在解析器列表管理页面中，单击“新增”，进入新增解析器页面。
     ii. 在新增解析器页面中，进行参数配置。

表 12-2 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。

参数名称	参数说明
规则列表	设置解析器解析规则。操作步骤如下： 1. 单击“添加”，并选择规则类型。 ● 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv解析”、“mutate解析”、“grok解析”、“date解析”、“drop解析”、“prune解析”、“csv解析”、“json解析”。 ● 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。 2. 根据选择的规则配置对应的参数信息。

iii. 设置完成后，单击页面右下角“确定”。

- **由模板创建**

i. 在解析器管理页面中，选择“模板列表”页签。

ii. 在目标模板页面中，单击目标模板所在行“操作”列的“由模板创建”。

iii. 在新增解析器页面中，进行参数配置。

表 12-3 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”。

iv. 设置完成后，单击页面右下角“确定”。

步骤七：新增采集通道

1. 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 12-12 进入采集通道管理页面

2. 新增分组。

   a. 在采集通道管理页面中，单击“分组列表”右侧的。

   b. 输入分组名称，并单击，完成新增。

   分组新增完成后，如需编辑/删除，可以将鼠标悬停在分组名称后，单击编辑/删除按钮，进行编辑/删除操作。

3. 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。
4. 在“基础配置”页面中，配置基础信息。

表 12-4 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
目的配置	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择来源的相关信息。

5. 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。
6. 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

   如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见**管理解析器**。

7. 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。
8. 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。

- 运行参数：节点添加后，如在已添加节点中运行参数，请参照以下步骤进行处理：
  i. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。
  ii. 单击“添加配置”，设置运行键和运行值。
- 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。

9. 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。
10. 在“通道详情预览”页面确认配置无误后，单击“确定”。

相关操作

Agent安装失败问题排查

12.1.3 采集管理

12.1.3.1 管理连接

操作场景

本章节主要介绍如何执行新增连接、查看连接管理信息、编辑数据连接、删除数据连接操作。

约束与限制

- 数据连接新增成功后，仅支持对已选择的数据源类型的参数信息进行修改，不支持变更数据源类型。

新增连接

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-13 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 12-14 进入采集管理页面

步骤5 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。

步骤6 新增数据连接来源。

在“来源”页签中，选择数据源类型的来源，并根据选择的类型进行参数配置。

数据源类型来源支持以下类型：传输控制协议 Tcp、文件 File、用户数据协议 Udp、对象存储 Obs、消息队列 Kafka、云脑管道 Pipe

步骤7 新增数据源连接目的。

选择“目的”页签中，选择数据源类型的目的，并根据选择的类型进行参数配置。

数据源类型目的支持以下类型：文件 File、传输控制协议 Tcp、用户数据协议 Udp、消息队列 Kafka、对象存储 Obs、云脑管道 Pipe

步骤8 设置完成后，单击页面右下角“确认”。

----结束

查看连接管理信息

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 12-16 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 12-5 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。
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 在页面左上角单击 ☰，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 12-17 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 12-18 进入采集管理页面

步骤5 在连接管理页面中，单击目标连接所在行“操作”列的“编辑”。

步骤6 在“数据源类型选择”页面中，编辑数据源类型信息参数信息。

步骤7 设置完成后，单击页面右下角“确认”。

----结束

删除数据连接

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-19 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 12-20 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

12.1.3.2 管理解析器

操作场景

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

创建解析器

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-21 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-22 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 12-6 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。

参数名称	参数说明
规则列表	设置解析器解析规则。操作步骤如下： 1. 单击“添加”，并选择规则类型。 ○ 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv解析”、“mutate解析”、“grok解析”、“date解析”、“drop解析”、“prune解析”、“csv解析”、“json解析”。 ○ 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。 2. 根据选择的规则配置对应的参数信息。

c. 设置完成后，单击页面右下角“确定”。

- **由模板创建**

a. 在解析器管理页面中，选择“模板列表”页签。

b. 在目标模板页面中，单击目标模板所在行“操作”列的“由模板创建”。

c. 在新增解析器页面中，进行参数配置。

表 12-7 新增解析器

参数名称		参数说明
基本信息	名称	解析器名称，系统已根据模板自动生成，可进行修改。
	描述	解析器描述信息，系统已根据模板自动生成，可进行修改。
规则列表		解析器解析规则，系统已根据模板自动生成，可进行修改。 如需添加规则，可以单击“添加”，选择规则类型，并根据选择的规则配置对应的参数信息。 ■ 解析规则：选择解析器的解析规则，支持选择“UUID”、“kv解析”、“mutate解析”、“grok解析”、“date解析”、“drop解析”、“prune解析”、“csv解析”、“json解析”。 ■ 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。

d. 设置完成后，单击页面右下角“确定”。

----结束

查看解析器管理信息

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ，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 12-23 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-24 进入解析器管理页面

步骤5 在解析器管理页面中，查看解析器的详细信息。

表 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6 在解析器管理页面中，选择“模板列表”页签，进入模板列表页面。

步骤7 在模板列表页面中，查看解析器模板信息。

表 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

导入解析器

说明

- 仅支持导入json格式的文件，且文件大小不超过1MB。
- 一次最多支持导入5个解析器文件，且每个解析器文件最多支持包含100个解析器。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-25 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-26 进入解析器管理页面

步骤5 在解析器列表管理页面中，单击解析器列表左上角的“导入”，弹出导入文件对话框。

步骤6 在弹出的导入文件对话框中，单击“添加文件”，选择你需要导入的json文件。

注意

- 仅支持导入json格式的文件，且文件大小不超过1MB。
- 一次最多支持导入5个解析器文件，且每个解析器文件最多支持包含100个解析器。

步骤7 选择完成后，单击“确定”，完成导入。

导入成功后，可以在解析器列表中查看导入的解析器信息。

----结束

编辑解析器

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-27 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-28 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。

参数名称	参数说明
规则列表	设置解析器解析规则。操作步骤如下： 单击“添加”，并选择规则类型。 ● 解析规则：选择解析器的解析规则。 ● 条件控制：选择解析器的条件控制原则。

步骤7 设置完成后，单击页面右下角“确定”。

----结束

导出解析器

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-29 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-30 进入解析器管理页面

步骤5 在解析器列表管理页面中，勾选需要导出的解析器，并单击列表上方的“导出”。

系统将自动下载.json格式的解析器文件到本地。

----结束

删除解析器

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-31 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

图 12-32 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

12.1.3.3 管理采集通道

操作场景

本章节主要介绍如何执行**新增采集通道**、**查看采集通道**、**编辑采集通道**、**删除采集通道**、**启用/停止/重启采集通道**操作。

新增采集通道

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-33 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 12-34 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 12-11 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择采集通道所属分组。
	（可选）描述	输入采集通道描述信息。
来源配置	源名称	选择采集通道来源名称。 选择后系统将自动生成已选择来源的相关信息。
目的配置	目的名称	选择采集通道目的名称。 选择后系统将自动生成已选择来源的相关信息。

步骤8 基础配置完成后，单击页面右下角“下一步”，进入“解析器配置”页面。

步骤9 在“解析器配置”页面中，选择解析器，选择后，系统将显示已选择解析器的相关信息。

如果无可选解析器或需新增解析器，可以单击“新建”，新建解析器。新增解析器详细操作请参见**管理解析器**。

步骤10 解析器配置完成后，单击页面右下角“下一步”，进入“运行节点选择”页面。

步骤11 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择节点后，单击“确认”。

- 运行参数：节点添加后，如在已添加节点中运行参数，请参照以下步骤进行处理：
  a. 在节点列表中，单击目标节点所在行“操作”列的“运行参数”按钮。
  b. 单击“添加配置”，设置运行键和运行值。
- 移除节点：节点添加后，如需移除，请在节点列表中，单击目标节点所在行“操作”列的“移除”按钮，已添加节点将被移除。

步骤12 运行节点选择完成后，单击页面右下角“下一步”，进入“通道详情预览”页面。

步骤13 在“通道详情预览”页面确认配置无误后，单击“确定”。

----结束

查看采集通道

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-35 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 12-36 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 12-12 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 在页面左上角单击 ☰，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 12-37 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 12-38 进入采集通道管理页面

步骤5 在采集通道管理列表中，单击目标通道所在行“操作”列的“更多 > 编辑”，进入编辑采集通道页面。

步骤6 在“基础配置”页面中，配置基础信息。

表 12-13 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**。

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 在页面左上角单击 ☰，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 12-39 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 12-40 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 在页面左上角单击 ☰，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 12-41 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集通道管理”页签，进入采集通道管理页面。

图 12-42 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

12.1.3.4 管理采集节点

操作场景

本章节主要介绍如何执行查看采集节点信息操作。

查看采集节点信息

步骤1 登录管理控制台。

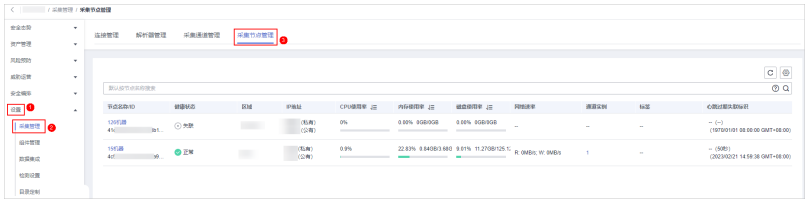
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 12-43 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“采集节点管理”页签，进入采集节点管理页面。

图 12-44 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 12-14 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

12.1.4 组件管理

12.1.4.1 管理节点

操作场景

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

新增节点

步骤1 登录管理控制台。

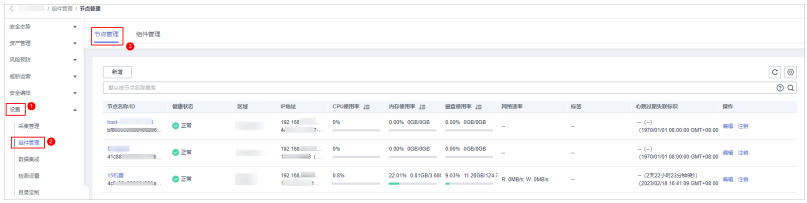
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 12-45 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 12-46 进入节点管理页面



步骤5 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。

步骤6 单击页面右下角“下一步”，进入“脚本安装验证”页面。

步骤7 确认已安装后，单击页面右下角“确认”。

如未安装请参照**步骤二：安装Agent**进行处理。

----结束

查看节点管理信息

步骤1 登录管理控制台。

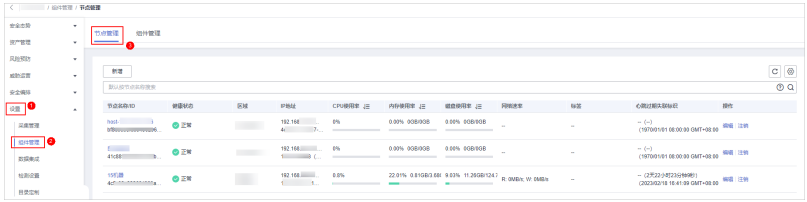
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 12-47 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 12-48 进入节点管理页面



步骤5 在节点管理页面中，查看节点的详细信息。

当节点较多时，可以通过搜索功能，选择节点的“节点名称”或“节点ID”，并在搜索框中输入关键词，单击🔍，即可快速查询指定节点。

表 12-15 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。

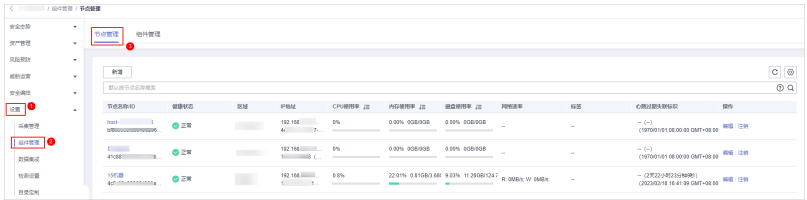
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 12-50 进入节点管理页面



步骤5 在节点管理页面中，单击目标节点所在行“操作”列的“编辑”，页面右侧弹出编辑节点页面。

步骤6 在编辑节点页面中，编辑节点补充信息。

表 12-16 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。

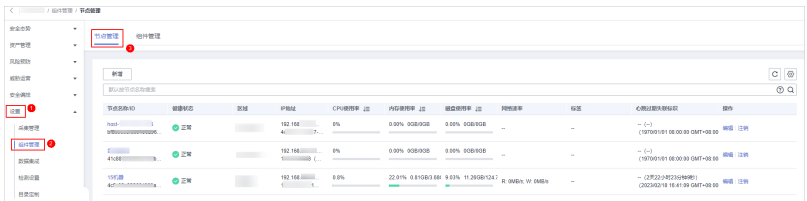
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 12-52 进入节点管理页面



步骤5 在节点管理页面中，单击目标节点所在行“操作”列的“注销”。

步骤6 在弹出的确认框中，单击“确认”。

说明

仅注销节点，不会删除ECS和endpointinterface资源。

----结束

12.1.4.2 管理组件

操作场景

本章节将介绍如何**配置组件**、查看组件相关信息。

配置组件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-53 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

图 12-54 进入组件管理页面

步骤5 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

步骤6 在节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择节点后，单击“确认”。

步骤7 单击页面右下角“保存并应用”。

----结束

查看组件详情

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-55 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 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。

图 12-56 进入组件管理页面

步骤5 在组件管理页面中，查看组件的详细信息。

- **运行节点**：
  单击待运行组件右上角“运行节点”，右侧将弹出该组件的运行节点信息。
- **查看配置**：
  单击待查看组件右上角“查看配置”，右侧将弹出该组件的详细配置信息。
- **编辑配置**：
  a. 单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。
  b. 在节点配置栏中，编辑节点配置信息。
     - 添加节点：单击节点列表左上角“添加”，并在弹出的“添加节点”框中，选择节点后，单击“确认”。
     - 编辑已添加节点参数信息：单击节点名称前的 ⌄，展开节点配置信息后，编辑节点参数信息。
     - 运行参数：单击目标节点所在行“操作”列的“运行参数”。
     - 移除节点：单击目标节点所在行“操作”列的“移除”。

- 批量删除：选中带移除节点后，单击列表左上角“批量移除”。
- 查看历史版本：单击页面右下角“历史版本”。

c. 单击页面右下角“应用”。

----结束

12.2 数据集成

12.2.1 支持接入的日志

安全云脑支持集成WAF、HSS、OBS等多种华为云云产品的日志数据。集成后，可以检索并分析所有收集到的日志，且默认存储7天。

表 12-17 支持接入的日志

云服务	日志描述	日志	日志生命周期范围
Web应用防火墙（Web Application Firewall，WAF）	攻击日志	waf-attack	7~10 天
	访问日志	waf-access	
安全云脑（SecMaster）	合规基线日志	secmaster-baseline	7~10 天
对象存储服务（Object Storage Service，OBS）	访问日志	obs-access	7~10 天
入侵防御系统（Intrusion Prevention System，IPS）	攻击日志	nip-attack	7~10 天
统一身份认证（Identity and Access Management，IAM）	审计日志	iam-audit	7~10 天
企业主机安全（Host Security Service，HSS）	主机安全告警	hss-alarm	7~10 天
	主机漏洞扫描结果	hss-vul	
	主机安全日志	hss-log	
Anti-DDoS流量清洗（Anti-DDoS）	攻击日志	ddos-attack	7~10 天
数据库安全服务（Database Security Service，DBSS）	告警日志	dbss-alarm	7~10 天
云审计服务（Cloud Trace Service，CTS）	云审计服务日志	cts-audit	7~10 天
云防火墙（Cloud Firewall，CFW）	访问控制日志	cfw-block	7~10 天
	流量日志	cfw-flow	

云服务	日志描述	日志	日志生命周期范围
	攻击事件日志	cfw-risk	
API网关（API Gateway）	访问日志	apig-access	7~30 天

12.2.2 接入数据

操作场景

安全云脑支持一键接入WAF、HSS、OBS等多种华为云云产品的日志数据。接入后，可以统一管理日志信息，以及检索并分析所有收集到的日志。

具体支持接入的云服务日志请参见**支持接入的日志**。

本章节介绍如何接入数据并查看日志存储位置。

接入服务日志

步骤1 登录管理控制台。

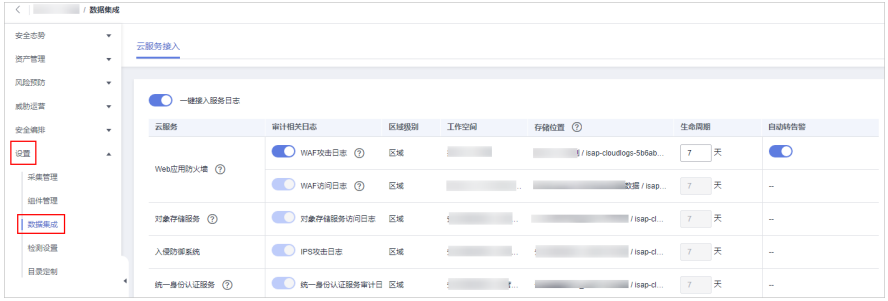
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 12-57 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 数据集成”，进入数据集成页面。

图 12-58 数据集成页面



步骤5 在待接入云产品的“审计相关日志”列，单击 ，开启接入的云服务日志。

如需接入当前region所有云产品日志，可直接单击“一键接入服务日志”前的按钮，一键接入当前region所有云服务日志。

步骤6 设置生命周期。

系统默认存储数据7天，您可以根据需要进行设置。

步骤7 设置是否自动转告警。

在待设置云产品的“自动转告警”列，单击，开启接入的云服务日志满足告警条件时，自动转为告警，并且在“告警管理”页面中进行展示。

说明

- 如果此处未开启自动转告警，在对应日志满足告警条件时，将不会转为告警，也不会在“告警管理”页面中进行展示。
- 在安全云脑的“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”，并在弹出的配置保存框中，单击“确定”。

接入完成后，将创建默认数据空间和管道。

----结束

查看日志数据的存储位置

步骤1 登录管理控制台。

步骤2 在页面左上角单击，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“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。

图 12-59 查看存储位置

----结束

相关操作

- 取消数据接入

a. 在待取消接入云产品的“审计相关日志”列，单击，关闭接入的云服务日志。
b. 单击“保存”。

- 编辑数据接入生命周期
  a. 在待编辑云产品的“生命周期”列，输入生命周期时间。
  b. 单击“保存”。
- 取消自动转告警
  a. 在待取消云产品的“自动转告警”列，单击，关闭告警映射。
  b. 单击“保存”。

12.3 检测设置

操作场景

使用云服务基线检查相关功能时，需要先参考本章节设置检查计划。

操作步骤

步骤1 登录管理控制台。

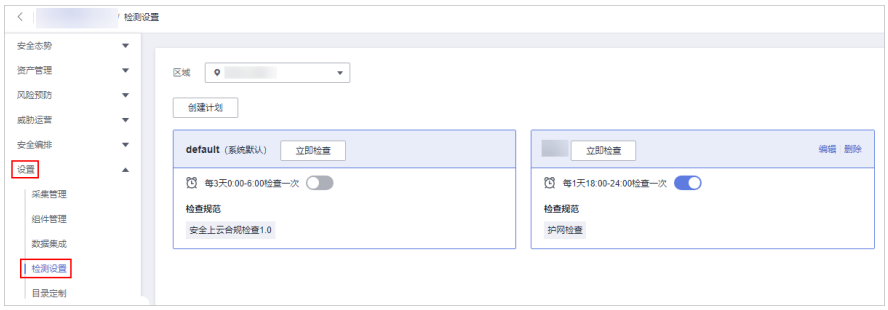
步骤2 在页面左上角单击，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 12-60 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

图 12-61 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12-18**所示。

表 12-18 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。更多关于基线检查项目详细描述请参见**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

操作场景

安全云脑支持自定义目录，您可以根据需要对目录进行定制。本章节将介绍以下操作：

- **查看已有目录**
- **更换布局**

约束与限制

- 系统内置的目录**不支持**编辑、删除操作。

查看已有目录

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 12-62 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 目录定制”，进入目录定制页面。

图 12-63 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 12-19 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。其中，系统内置目录默认发布者为“华为云”。
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 在页面左上角单击 ☰，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 12-64 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 目录定制”，进入目录定制页面。

图 12-65 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

13 剧本使用说明

13.1 概述

安全云脑通过启动剧本，自动执行相关代码，实现告警事件自动化响应处置。其中，有一部分剧本（例如，自动更新告警名称剧本、高危漏洞自动通知剧本、高危告警自动通知剧本等）需要进行自定义处理后，才能实现自定义的数据处理。

本文档将介绍如何自定义配置并启用需要自定义处理的剧本。

剧本、流程和插件的关系

其中，剧本、流程和插件的关系说明如下：

- 剧本是流程的组合，实现多维度、多层次的复杂数据业务处理。
- 流程是一系列插件节点的组合，实现复杂的数据业务处理。
- 插件是函数代码的封装，剧本的最小单元，实现特定的函数功能。

13.2 自动更新告警名称

13.2.1 概述

使用场景

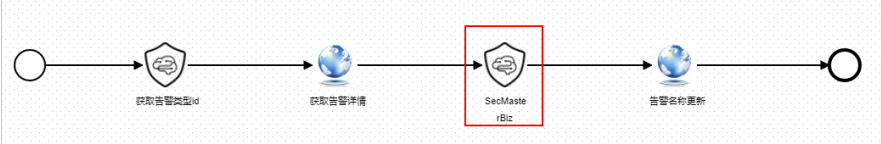
安全云脑提供的自动更改告警名称剧本，支持用户按照不同维度自定义告警名称。

剧本说明

“自动更改告警名称”剧本已匹配“自动更改告警名称”流程，配置该剧本，需要对流程及流程中的插件进行适配。

“自动更改告警名称”流程共四个插件节点：获取告警类型id、获取告警详情、SecMasterBiz、告警名称更新。本流程只需配置SecMasterBiz插件节点，该节点用来定制告警名称的。

图 13-1 自动更改告警名称流程



约束与限制

目前，仅支持对**webshell攻击类型**告警名称进行自定义修改。

功能实现效果

告警名称个性化处理前：

图 13-2 处理前

对原有webshell告警名称进行个性化处理后，效果如下所示：

图 13-3 处理后

13.2.2 配置并启用剧本

操作场景

本章节将介绍配置“SecMasterBiz”插件节点、启用“自动更改告警名称”流程、启用“自动更改告警名称”剧本。

步骤一：配置并启用流程

进入流程管理页面

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 13-4 进入目标工作空间管理页面

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

图 13-5 流程管理页面

复制流程版本

步骤5 在“自动更改告警名称”流程所在行的“操作”列，单击“版本管理”，弹出流程版本管理页面。

图 13-6 进入流程版本管理页面

步骤6 在“自动更改告警名称”的**流程版本管理**页面中，单击“版本信息”栏中初始版本（v1）所在行的“操作”列的“复制”，弹出确认框。

步骤7 在弹出的确认框中，单击“确认”。

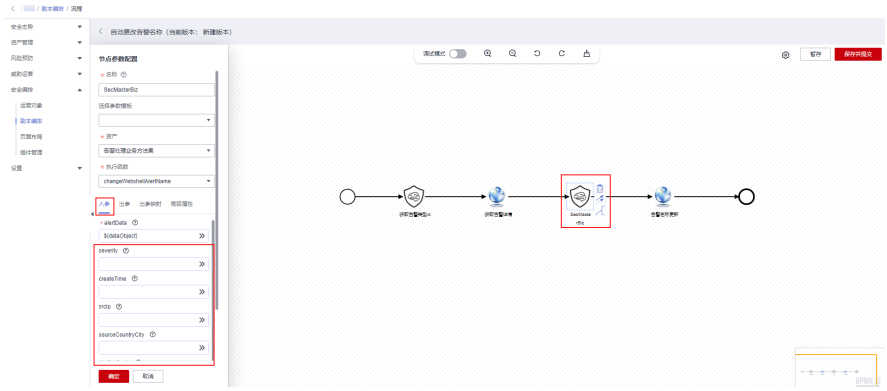
编辑并提交流程版本

步骤8 在“自动更改告警名称”的**流程版本管理**页面中，单击“版本信息”栏中已复制版本所在行的“操作”列的“编辑”，进入流程图绘制界面。

步骤9 在绘制页面中，单击**SecMasterBiz**插件，并在左侧展示的该插件信息中配置插件。

SecMasterBiz插件参数说明请参见**SecMasterBiz插件说明**。

图 13-7 SecMasterBiz 插件



步骤10 配置完成后，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”，页面返回流程管理页面。

审核流程版本

步骤11 在流程管理页面中，单击“自动更改告警名称”流程所在行的“操作”的“版本管理”。

步骤12 在**流程版本管理**页面中，单击已编辑的流程版本所在行的“操作”列的“审核”。

步骤13 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

激活流程版本

步骤14 在“自动更改告警名称”的**流程版本管理**页面中，单击已审核的流程版本所在行的“操作”列的“激活”。

步骤15 在弹出确认框中，单击“确认”。

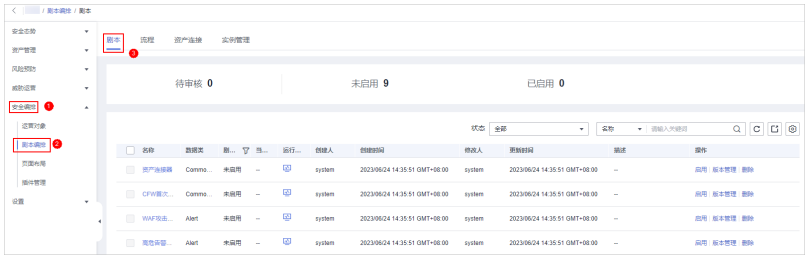
流程版本激活后，默认流程处于启用状态。

----结束

步骤二：配置并启用剧本

步骤1 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 13-8 进入剧本管理页面



步骤2 在**剧本管理**页面中，单击“自动更改告警名称”剧本所在行的“操作”列的“启用”。

步骤3 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

SecMasterBiz 插件说明

SecMasterBiz插件是自动更改告警名称流程中的一个插件，用于分析处理webshell类型告警的名称数据，可以按照用户自定义维度拼接告警名称，返回更新后的告警名称。

SecMasterBiz插件包含多个Action，其中，“changeWebshellAlertName” Action提供了几个入参供用户自定义选取，每个入参代表一个分析维度。

用户根据需要选择不同的维度参数对进行告警名称进行拼接，没有选中的参数，默认不返回该维度数据。填入y表示yes，即选择该参数；填入n表示no，或者保持为空，都表示不选择该参数。

表 13-1 参数配置说明

参数名称	参数含义	取值范围
severity	告警严重程度	y/n
createTime	告警创建时间	y/n
srcIp	告警攻击源IP	y/n
sourceCountryCity	告警攻击源国家和城市	y/n
destinationIp	告警攻击目标IP	y/n
destinationCountryCity	告警攻击目标国家和城市	y/n

13.2.3 验证剧本

操作场景

“自动更改告警名称”剧本启用成功后，可以对剧本运行情况进行验证。

本章节将介绍如何对已配置剧本进行验证。

操作步骤

步骤1 登录管理控制台。

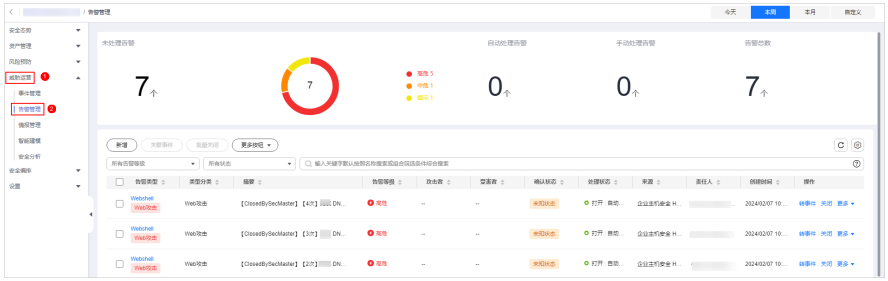
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-9 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警管理页面。

图 13-10 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。

- 告警名称：自定义告警名称。
- 告警类型：请选择“Web攻击/Webshell”。
- 调试模式：请勾选“是”。
- 描述：自定义告警描述信息。
- 其他参数保持缺省值即可。

步骤6 告警参数配置完成后，单击“确认”。

步骤7 刷新页面，查看告警名称是否更新。

在剧本已经启用情况下，剧本会自动对新增告警进行处理，处理后会显示更新后的告警名称。

图 13-11 默认不选择任何参数输出结果

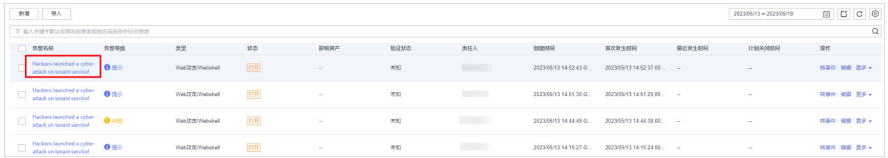


图 13-12 只选择 severity 参数输出结果

----结束

13.3 攻击链路分析告警通知

13.3.1 概述

使用场景

攻击者攻击域名成功之后会对后端服务器进行攻击，因此针对此链路攻击的路径，安全云脑提供了攻击链路分析告警通知剧本。当攻击者通过层层攻击到主机之后，进行告警，通知运营人员进行处置。

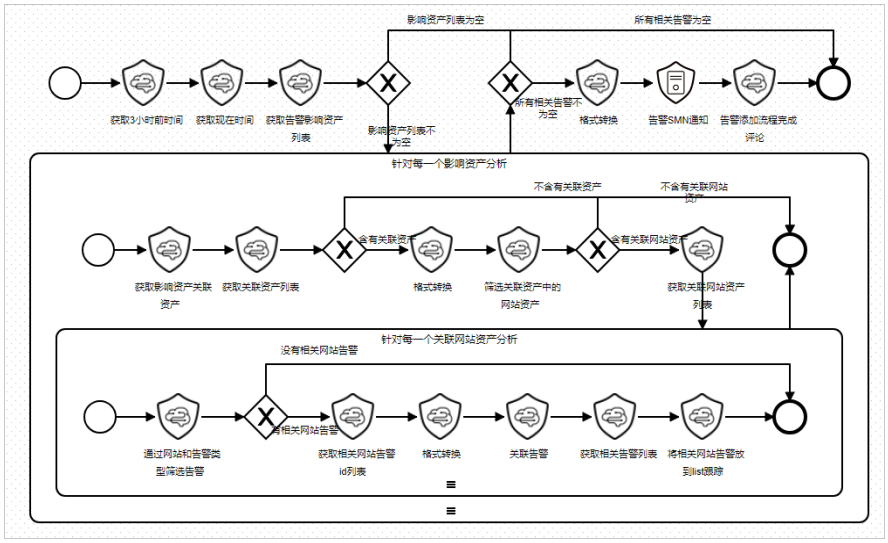
剧本说明

“攻击链路分析告警通知”剧本已匹配“攻击链路分析告警通知”流程，该流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

“攻击链路分析告警通知”流程是通过资产关联，查询对应HSS告警影响资产所关联的网站资产列表，流程预置默认查询最多3条网站资产。

- 如果有关联网站资产，则每条网站资产查询3小时前到现在这个时间段内对应的WAF告警数据（告警类型为XSS、SQL注入、命令注入、本地文件包含、远程文件包含、Webshell、漏洞攻击），同样的，最多查询3条告警数据。
- 如果有对应WAF告警，则将WAF告警数据与本条HSS告警数据进行关联，并通过消息通知服务（Simple Message Notification，SMN）通知到邮箱。

图 13-13 攻击链路分析告警通知流程

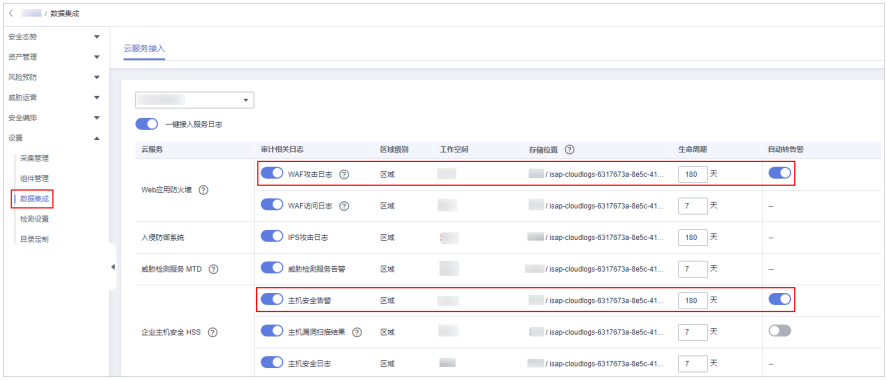


前提条件

- 已在安全云脑工作空间的“设置 > 数据集成”页面中接入来源为HSS和WAF的告警数据。

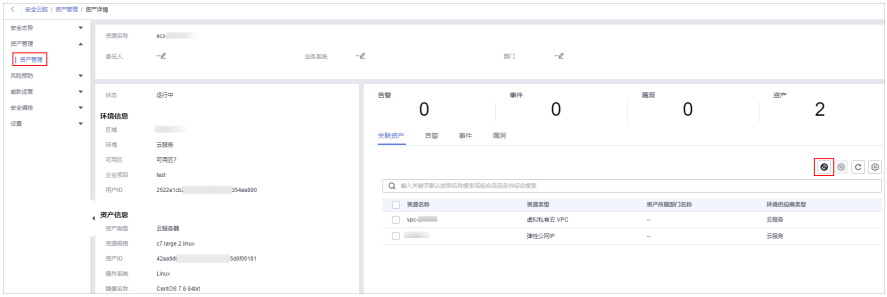
  接入HSS和WAF攻击数据，并开启自动转告警开关，详细操作请参见**数据集成**。

图 13-14 接入告警数据



- 已在安全云脑工作空间的“资产管理”页面中，单击资产名称，进入资产详情页面，将网站资产和主机资产进行关联。

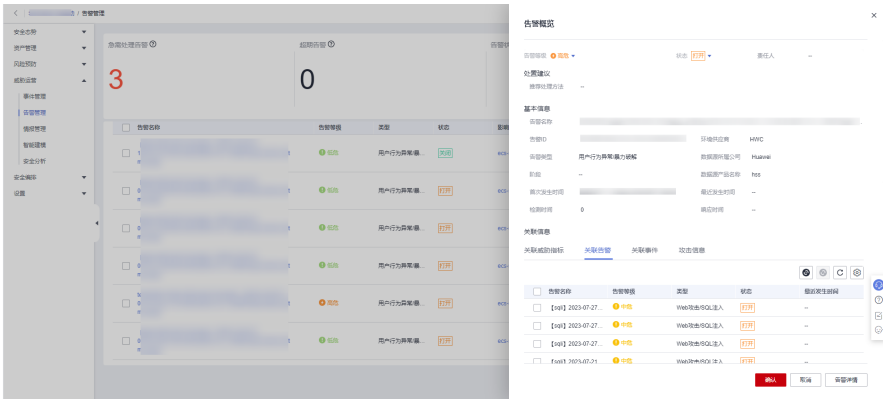
图 13-15 关联资产



功能实现效果

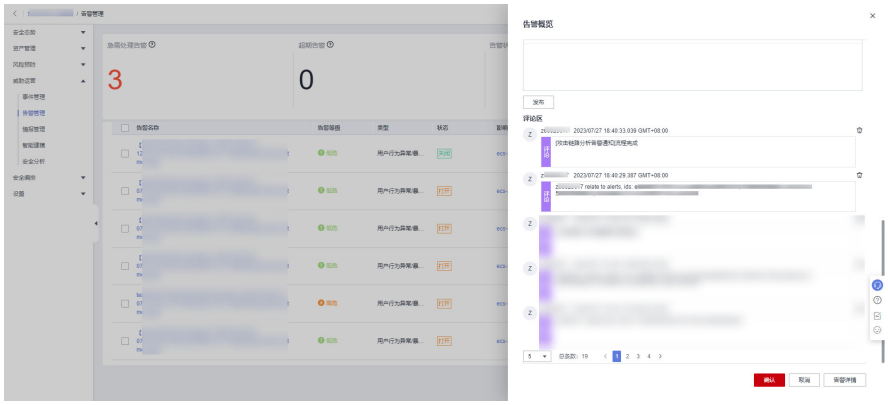
攻击链路分析告警通知剧本完成之后，对应HSS告警会将与之关联的网站资产影响的WAF来源的告警关联：

图 13-16 关联告警



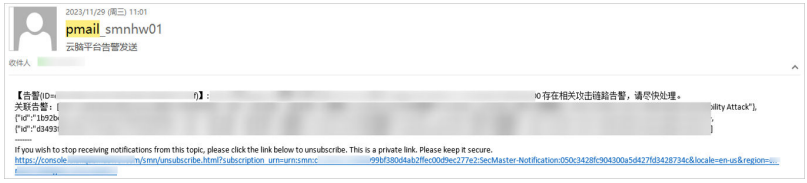
对应告警评论增加剧本评论：

图 13-17 增加评论



并邮件通知客户进行告警处置：

图 13-18 邮件通知



13.3.2 创建并订阅主题

操作场景

“攻击链路分析告警通知”流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

本章节将介绍如何创建并订阅主题。

操作步骤

步骤1 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 > 消息通知服务”，进入消息通知服务管理页面。

步骤3 创建主题。

1. 在左侧导航栏，选择“主题管理 > 主题”，进入主题管理页面后，单击右上角“创建主题”。

图 13-19 创建主题

2. 在弹出的创建主题页面中，配置主题信息后，单击“确定”。
   - 主题名称：建议设置为“SecMaster-Notification”。
   - 显示名：建议设置为“安全云脑通知主题”。
   - 其他参数保持缺省值即可。

图 13-20 配置主题

步骤4 添加订阅。

1. 在主题页面中，单击“SecMaster-Notification”主题所在行“操作”列的“添加订阅”。
2. 在弹出的添加订阅页面中，配置订阅信息后，单击“确定”。
   - 协议：请选择“邮件”。
   - 订阅终端：输入订阅终端邮箱地址，如username@example.com

图 13-21 添加订阅

----结束

13.3.3 配置并启用剧本

操作场景

在安全云脑中，默认“攻击链路分析告警通知”流程的初始版本（V1）也已启用，无需手动启用。默认“攻击链路分析告警通知”剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

本章节将介绍如何启用“攻击链路分析告警通知”剧本。

前提条件

已完成SMN主题订阅，详细操作请参见**创建并订阅主题**。

操作步骤

步骤1 登录管理控制台。

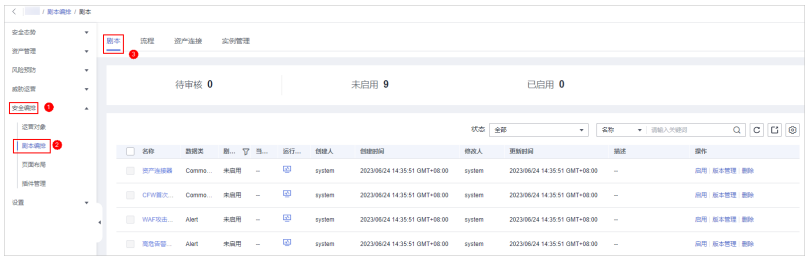
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-22 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 13-23 进入剧本管理页面



步骤5 在**剧本管理**页面中，单击“攻击链路分析告警通知”剧本所在行的“操作”列的“启用”。

步骤6 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

13.4 高危漏洞自动通知

13.4.1 概述

使用场景

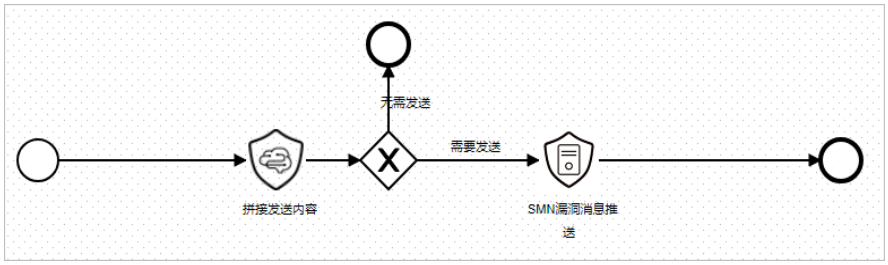
安全云脑提供的高危漏洞自动通知剧本，当新增主机漏洞，且等级为高危时，自动通知运营人员。

剧本说明

“高危漏洞自动通知”剧本已匹配“高危漏洞自动通知”流程，该流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

当新增HSS的高危漏洞时，会通过SMN服务对运营人员发送漏洞通知。

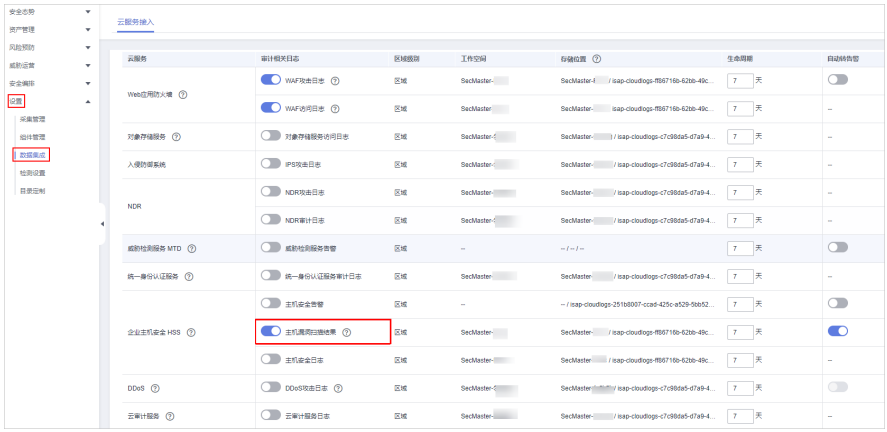
图 13-24 高危漏洞自动通知流程



前提条件

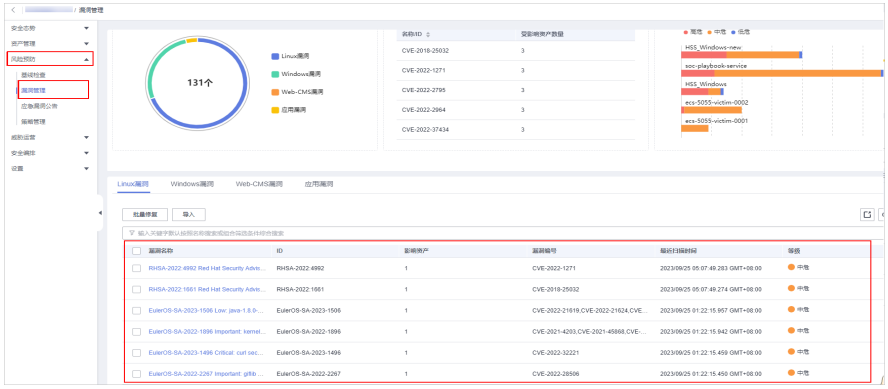
已在安全云脑工作空间的“设置 > 数据集成”页面中接入企业主机安全（Host Security Service，HSS）服务漏洞日志数据，详细操作请参见**数据集成**。

图 13-25 接入 HSS 告警



接入数据后，可以在“风险预防 > 漏洞管理”页面进行查看。

图 13-26 查看告警



13.4.2 创建并订阅主题

操作场景

“高危漏洞自动通知”流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

本章节将介绍如何创建并订阅主题。

操作步骤

步骤1 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 > 消息通知服务”，进入消息通知服务管理页面。

步骤3 创建主题。

1. 在左侧导航栏，选择“主题管理 > 主题”，进入主题管理页面后，单击右上角“创建主题”。

图 13-27 创建主题

2. 在弹出的创建主题页面中，配置主题信息后，单击“确定”。
   - 主题名称：建议设置为“SecMaster-Notification”。
   - 显示名：建议设置为“安全云脑通知主题”。
   - 其他参数保持缺省值即可。

图 13-28 配置主题

步骤4 添加订阅。

1. 在主题页面中，单击“SecMaster-Notification”主题所在行“操作”列的“添加订阅”。
2. 在弹出的添加订阅页面中，配置订阅信息后，单击“确定”。
   - 协议：请选择“邮件”。
   - 订阅终端：输入订阅终端邮箱地址，如username@example.com

图 13-29 添加订阅

----结束

13.4.3 配置资产连接

操作场景

使用“高危漏洞自动通知”流程前，需要将流程中使用到的凭证（“通知SMN运营人员凭证”资产连接）进行参数配置。

本章节将介绍配置资产连接。

前提条件

已完成SMN主题订阅，详细操作请参见**创建并订阅主题**。

操作步骤

步骤1 登录管理控制台。

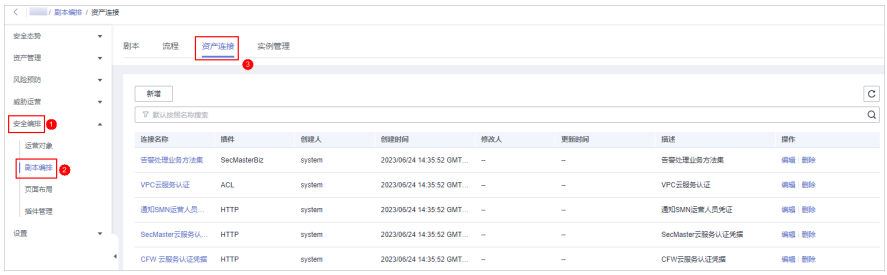
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-30 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“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。

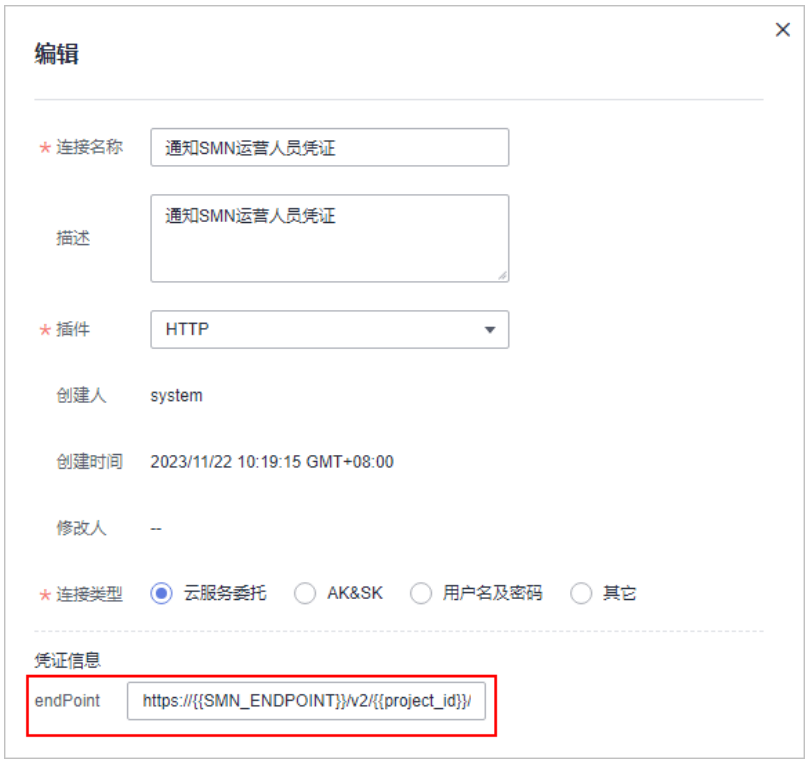
图 13-31 资产连接管理页面



步骤5 在资产连接管理页面中，单击“通知SMN运营人员凭证”所在行的“操作”列的“编辑”。

步骤6 在右侧弹出的编辑资产连接页面中，配置endpoint信息。

图 13-32 编辑资产连接



endPoint字段填写说明：**https://***{{SMN_ENDPOINT}}*/v2/*{{project_id}}*/**notifications/topics/***urn:smn:{{region_id}}:{{project_id}}:SecMaster-Notification*

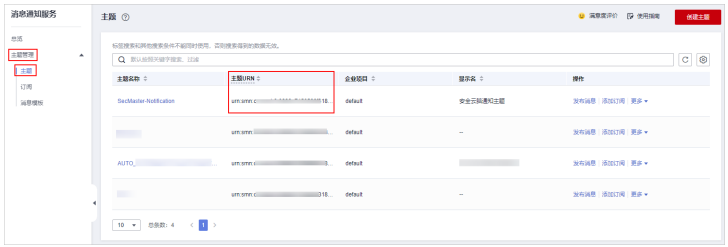
- *SMN_ENDPOINT*：为SMN服务调用域名，填写方式为“终端节点:443”，其中，终端节点信息请从**地区和终端节点**中获取。以华北-北京四为例：smn.cn-north-4.myhuaweicloud.com:443
- *project_id*：为当前工作空间所属的项目ID，查看方式如下：
  a. 已登录管理控制台，并将鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，默认进入API凭证页面。
  b. 在API凭证页面的“项目列表”中，查看项目ID。

图 13-33 项目 ID

- *urn:smn:{{region_id}}:{{project_id}}:SecMaster-Notification*：为发送邮件通知的SMN主题URN，查看方式如下：

  a. 在页面左上角单击 ☰，选择“管理与监管 > 消息通知服务”，进入消息通知服务管理页面。
  b. 在左侧导航栏，选择“主题管理 > 主题”，进入主题管理页面。
  c. 在主题列表中，查看**创建并订阅主题**创建的主题的主题URN信息。

图 13-34 主题 URN



步骤7 配置完成后，单击“确认”。

----结束

13.4.4 配置并启用剧本

操作场景

在安全云脑中，默认“高危漏洞自动通知”流程的初始版本（V1）也已启用，无需手动启用。默认“高危漏洞自动通知”剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

本章节将介绍如何启用“高危漏洞自动通知”剧本。

前提条件

- 已完成SMN主题订阅，详细操作请参见**创建并订阅主题**。
- 已完成资产连接配置，详细操作请参见**配置资产连接**。

操作步骤

步骤1 登录管理控制台。

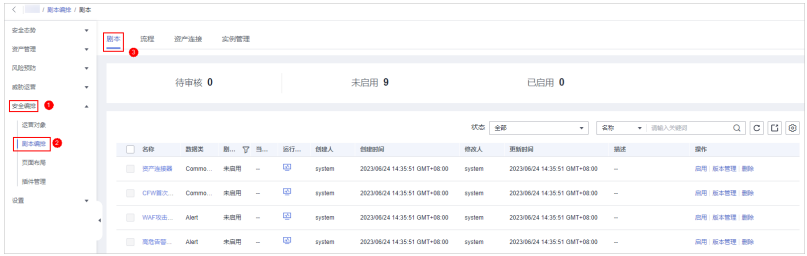
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-35 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 13-36 进入剧本管理页面



步骤5 在**剧本管理**页面中，单击“高危漏洞自动通知”剧本所在行的“操作”列的“启用”。

步骤6 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

13.5 高危告警自动通知

13.5.1 概述

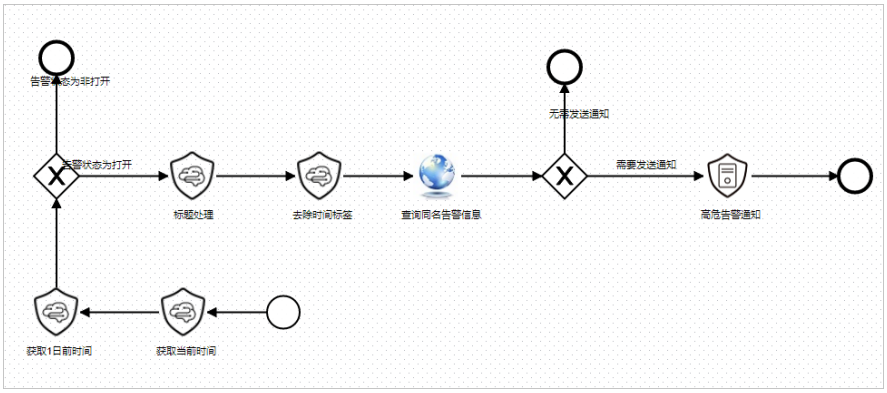
使用场景

安全云脑提供的高危告警自动通知剧本，当有告警新增时，对高危或者致命告警去重后，自动通知运营人员。

剧本说明

“高危告警自动通知”剧本已匹配“高危告警自动通知”流程，该流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

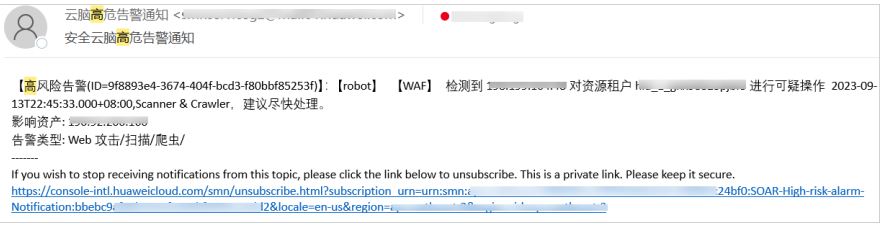
图 13-37 高危告警自动通知流程



功能实现效果

高危告警触发剧本，触发如下邮件通知：

图 13-38 告警通知邮件



13.5.2 创建并订阅主题

操作场景

“高危告警自动通知”流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

本章节将介绍如何创建并订阅主题。

操作步骤

步骤1 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 > 消息通知服务”，进入消息通知服务管理页面。

步骤3 创建主题。

1. 在左侧导航栏，选择“主题管理 > 主题”，进入主题管理页面后，单击右上角“创建主题”。

图 13-39 创建主题

2. 在弹出的创建主题页面中，配置主题信息后，单击“确定”。
   - 主题名称：建议设置为“SecMaster-Notification”。
   - 显示名：建议设置为“安全云脑通知主题”。
   - 其他参数保持缺省值即可。

图 13-40 配置主题

步骤4 添加订阅。

1. 在主题页面中，单击“SecMaster-Notification”主题所在行“操作”列的“添加订阅”。
2. 在弹出的添加订阅页面中，配置订阅信息后，单击“确定”。
   - 协议：请选择“邮件”。
   - 订阅终端：输入订阅终端邮箱地址，如username@example.com

图 13-41 添加订阅

----结束

13.5.3 配置并启用剧本

操作场景

在安全云脑中，默认“高危告警自动通知”流程的初始版本（V1）也已启用，无需手动启用。默认“高危告警自动通知”剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

本章节将介绍如何启用“高危告警自动通知”剧本。

前提条件

已完成SMN主题订阅，详细操作请参见**创建并订阅主题**。

操作步骤

步骤1 登录管理控制台。

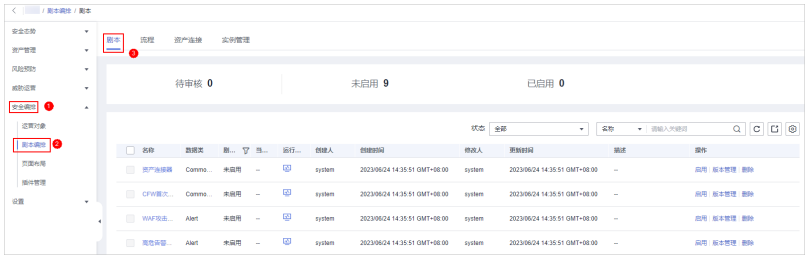
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-42 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 13-43 进入剧本管理页面



步骤5 在**剧本管理**页面中，单击“高危告警自动通知”剧本所在行的“操作”列的“启用”。

步骤6 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

13.6 WAF 攻击自动化安全封堵

13.6.1 概述

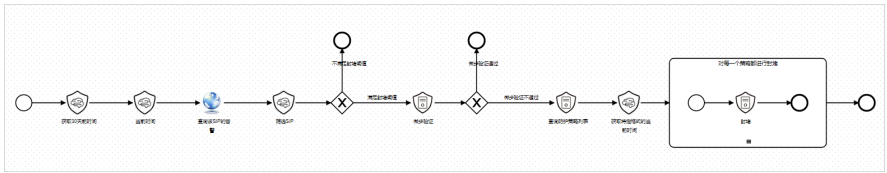
使用场景

安全云脑提供的WAF攻击自动化安全封堵剧本，可以自动将Web应用防火墙（Web Application Firewall，WAF）高危告警里的源IP封堵在WAF中。

剧本说明

“WAF攻击自动化安全封堵”剧本已匹配“WAF攻击自动化安全封堵”流程，配置该剧本，需要对流程及流程中的插件进行适配。

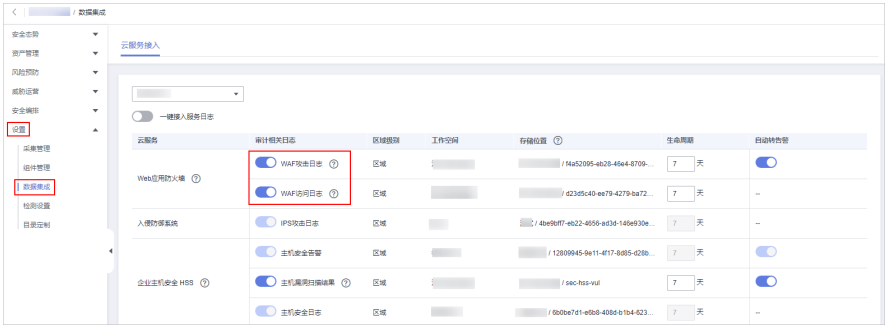
图 13-44 WAF 攻击自动化安全封堵



前提条件

- 已在安全云脑工作空间的“设置 > 数据集成”页面中接入WAF访问日志或WAF攻击日志，详细操作请参见**数据集成**。

图 13-45 接入 WAF 日志数据



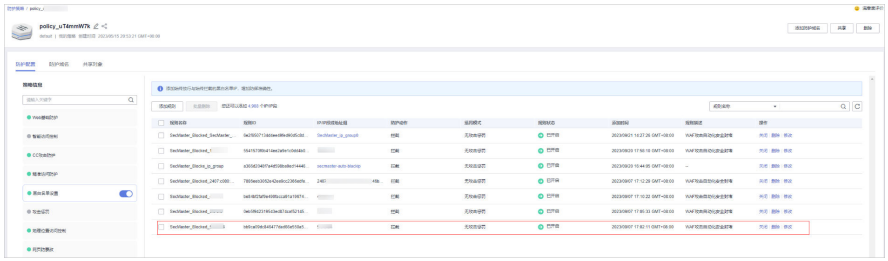
- 有可用的微步次数。

功能实现效果

封堵成功会在WAF黑名单里看到此IP已被封堵。查看方法如下：

1. 登录WAF控制台，进入“防护策略”页面后，单击目标防护策略名称。
2. 在防护策略详情页面，单击“防护配置”栏中的“黑白名单设置”，可以看到IP已被成功封堵在WAF黑名单中。

图 13-46 黑白名单



13.6.2 配置资产连接

操作场景

使用“WAF攻击自动化安全封堵”流程前，需要将流程中使用到的微步插件的APIkey（“微步认证凭据”资产连接）进行配置。

本章节将介绍配置资产连接。

前提条件

已完成SMN主题订阅，详细操作请参见**创建并订阅主题**。

操作步骤

步骤1 登录管理控制台。

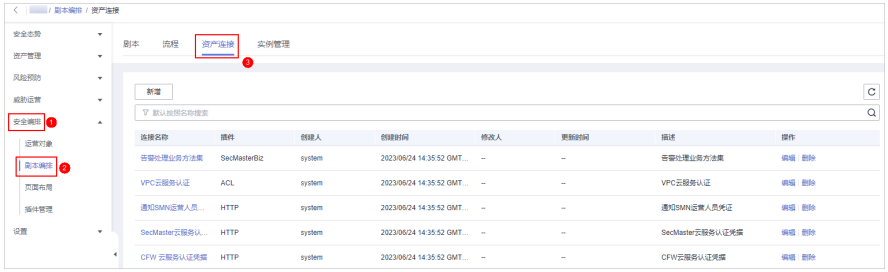
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-47 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

图 13-48 资产连接管理页面



步骤5 在资产连接管理页面中，单击“微步认证凭据”所在行的“操作”列的“编辑”。

步骤6 在右侧弹出的编辑资产连接页面中，配置凭证信息。

- freeApiKey，payApiKey：选择一填写即可，购买微步次数后可获得。
- redisHost：客户redis资源ip地址，如果没有，可不填。
- redisPort：客户redis资源端口号，如果没有，可不填。
- redisPassword：客户redis资源密码，如果没有，可不填。

图 13-49 编辑凭证信息

步骤7 配置完成后，单击“确认”。

----结束

13.6.3 配置并启用剧本

操作场景

在安全云脑中，默认“WAF攻击自动化安全封堵”流程的初始版本（V1）也已启用，无需手动启用。默认“WAF攻击自动化安全封堵”剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

本章节将介绍如何启用“WAF攻击自动化安全封堵”剧本。

前提条件

已完成资产连接配置，详细操作请参见**配置资产连接**。

操作步骤

步骤1 登录管理控制台。

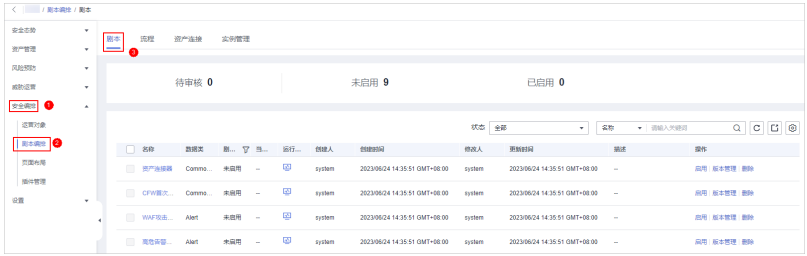
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-50 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 13-51 进入剧本管理页面



步骤5 在**剧本管理**页面中，单击“WAF攻击自动化安全封堵”剧本所在行的“操作”列的“启用”。

步骤6 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

13.7 HSS 文件隔离查杀

13.7.1 概述

使用场景

安全云脑提供的HSS文件隔离查杀剧本，自动隔离查杀恶意软件。

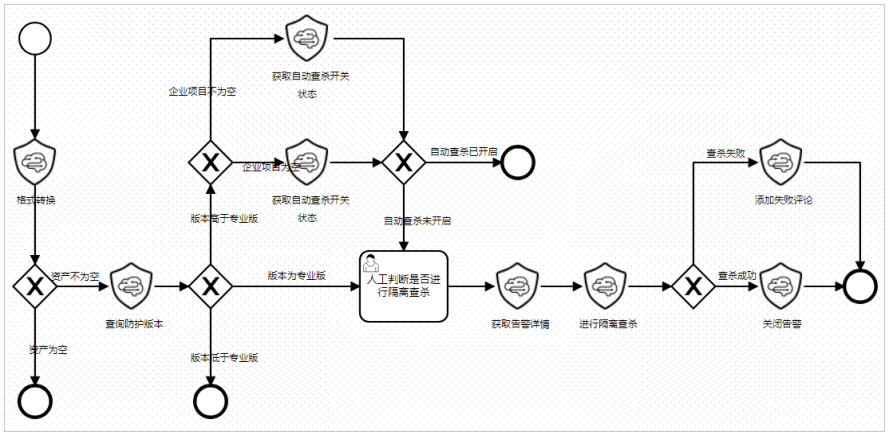
剧本说明

“HSS文件隔离查杀”剧本已匹配“HSS文件隔离查杀”流程，

“HSS文件隔离查杀”流程是通过HSS恶意文件隔离查杀进行恶意软件和勒索软件告警处置。

当资产HSS版本为专业版或者高于专业版但未开启自动隔离查杀，进行人工判断，人工审核需要进行隔离查杀，则通过HSS文件隔离查杀进行告警处置，隔离成功，关闭告警。隔离失败，添加需要手动处理的评论。

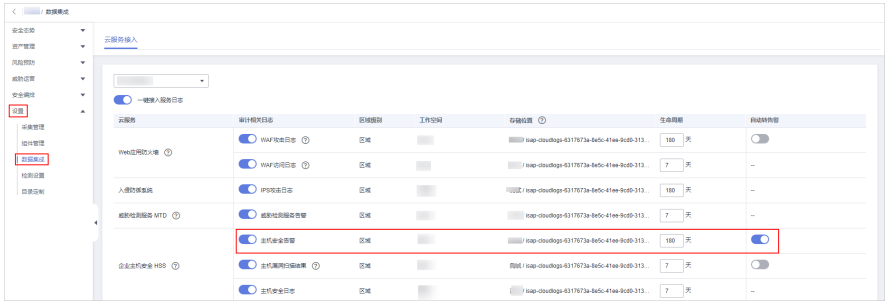
图 13-52 HSS 文件隔离查杀流程



前提条件

已在安全云脑工作空间的“设置 > 数据集成”页面中接入HSS告警数据，并开启自动转告警开关，详细操作请参见**数据集成**。

图 13-53 接入 HSS 告警



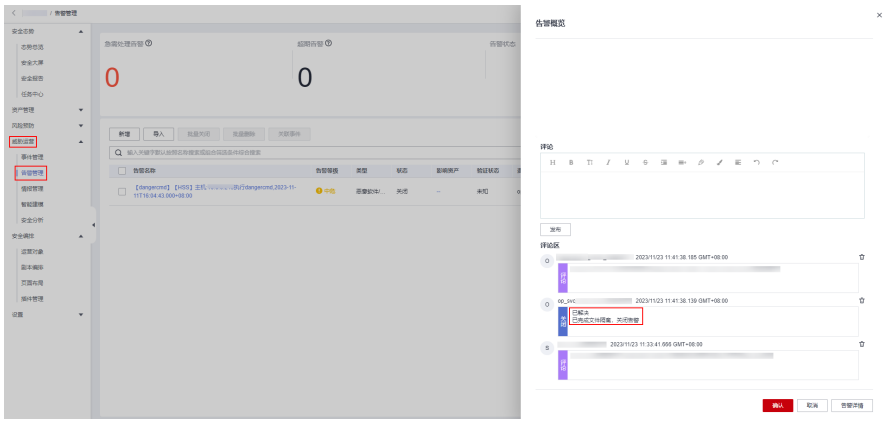
功能实现效果

- 隔离查杀成功告警自动关闭。

  图 13-54 自动关闭告警

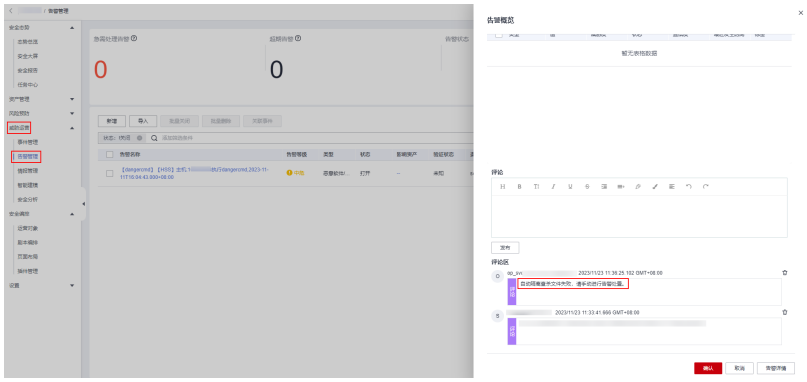
- 如果查杀成功，在评论可看到已完成文件隔离查杀。

图 13-55 查杀成功评论



- 如果隔离查杀失败，在评论可以看到需要手动进行告警处置。

图 13-56 查杀失败评论



13.7.2 配置并启用剧本

操作场景

在安全云脑中，默认“HSS文件隔离查杀”流程的初始版本（V1）也已启用，无需手动启用。默认“HSS文件隔离查杀”剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

本章节将介绍如何启用“HSS文件隔离查杀”剧本。

操作步骤

步骤1 登录管理控制台。

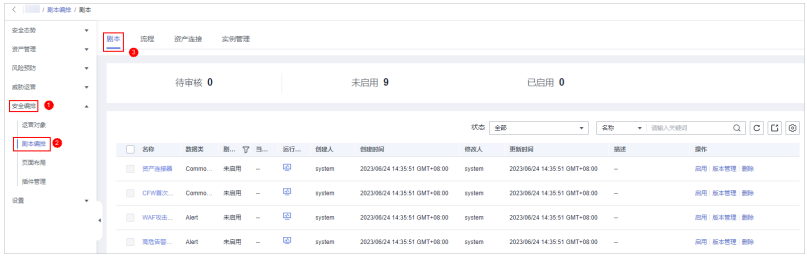
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-57 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 13-58 进入剧本管理页面



步骤5 在**剧本管理**页面中，单击“HSS文件隔离查杀”剧本所在行的“操作”列的“启用”。

步骤6 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

13.8 关键运维操作实时通知

13.8.1 概述

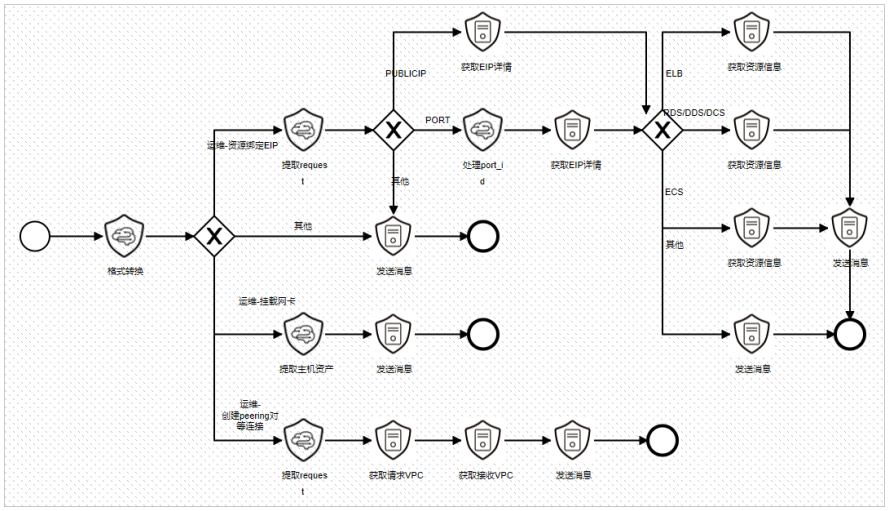
使用场景

安全云脑提供的关键运维操作实时通知剧本，基于运维操作，对关键运维操作进行邮件实时通知。

剧本说明

“关键运维操作实时通知”剧本已匹配“关键运维操作实时通知”流程，该流程是通过消息通知服务，当有关键运维操作时，发送通知给运营人员。

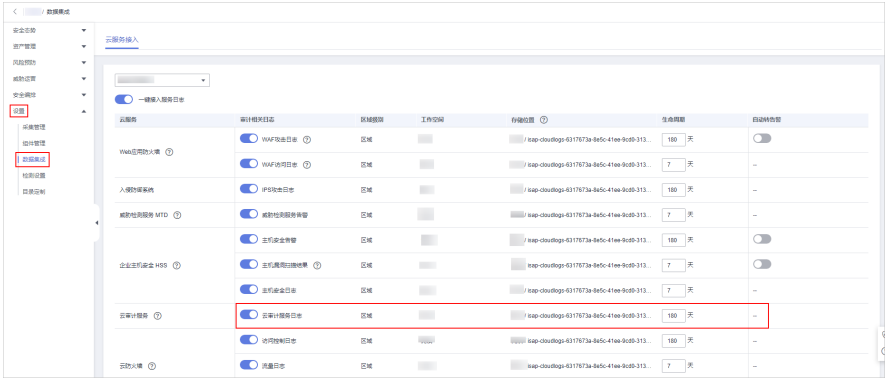
图 13-59 关键运维操作实时通知流程



前提条件

- 已在安全云脑工作空间的“设置 > 数据集成”页面中接入云审计服务日志数据，详细操作请参见**数据集成**。

  图 13-60 接入 CTS 日志

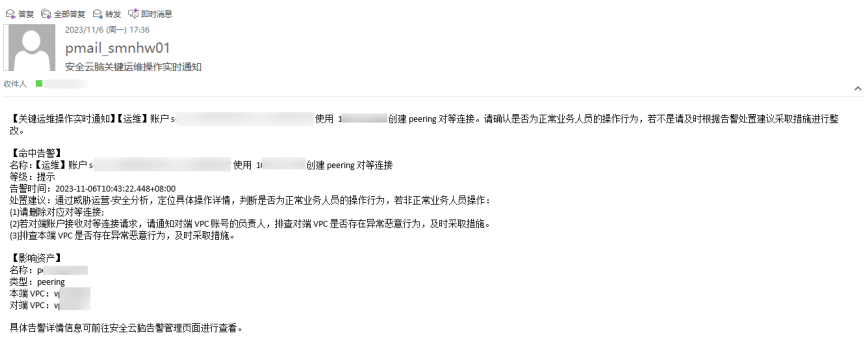
  

- 已启用对应的运维防线模型，详细操作请参见**启用告警模型**。

功能实现效果

当有关键运维操作时会触发剧本，触发如下邮件通知，以对等连接操作通知举例：

图 13-61 操作通知



13.8.2 启用告警模型

操作场景

使用“关键运维操作实时通知”剧本前，需要先启用运维防线模型（运维-挂载网卡、运维-创建peering对等连接、运维-资源绑定EIP）。

本章节将介绍如何启用告警模型。

操作步骤

创建告警模型

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，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 13-62 进入目标工作空间管理页面

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

图 13-63 模型模板页面

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

图 13-64 模板详情

步骤6 在模板详情页面，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。

- 管道名称：选择告警模型的执行管道。

  表 13-2 选择执行管道

告警模板	需要选择的执行管道
运维-挂载网卡	sec-cts-audit
运维-创建peering对等连接	
运维-资源绑定EIP	

- 其他参数建议保持默认值即可。

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，建议保持默认即可。

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”。

步骤12 重复步骤5-步骤11为其他模板创建告警模型。

启用告警模型

步骤13 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 13-65 可用模型页面

步骤14 在模型列表中，勾选所有需要启动的模型，然后单击列表左上角的“启用”。

步骤15 当模型状态更新为启用，则表示启动模型成功。

----结束

13.8.3 创建并订阅主题

操作场景

“关键运维操作实时通知”流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。

本章节将介绍如何创建并订阅主题。

操作步骤

步骤1 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 > 消息通知服务”，进入消息通知服务管理页面。

步骤3 创建主题。

1. 在左侧导航栏，选择“主题管理 > 主题”，进入主题管理页面后，单击右上角“创建主题”。

图 13-66 创建主题

2. 在弹出的创建主题页面中，配置主题信息后，单击“确定”。
   - 主题名称：建议设置为“SecMaster-Notification”。
   - 显示名：建议设置为“安全云脑通知主题”。
   - 其他参数保持缺省值即可。

图 13-67 配置主题

步骤4 添加订阅。

1. 在主题页面中，单击“SecMaster-Notification”主题所在行“操作”列的“添加订阅”。
2. 在弹出的添加订阅页面中，配置订阅信息后，单击“确定”。
   - 协议：请选择“邮件”。
   - 订阅终端：输入订阅终端邮箱地址，如username@example.com

图 13-68 添加订阅

----结束

13.8.4 配置并启用剧本

操作场景

在安全云脑中，默认“关键运维操作实时通知”流程的初始版本（V1）也已启用，无需手动启用。默认“关键运维操作实时通知”剧本的初始版本（V1）也已激活，只需要启用就可以进行使用。

本章节将介绍如何启用“关键运维操作实时通知”剧本。

前提条件

已完成SMN主题订阅，详细操作请参见**创建并订阅主题**。

操作步骤

步骤1 登录管理控制台。

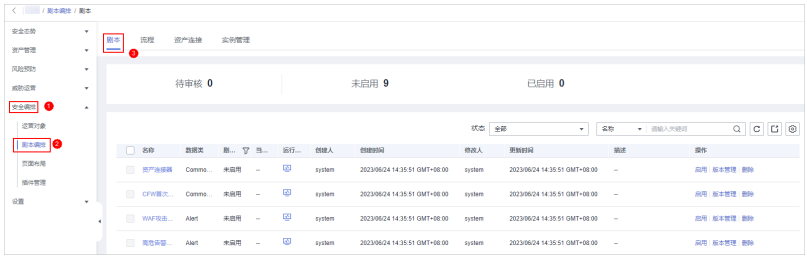
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

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 13-69 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

图 13-70 进入剧本管理页面



步骤5 在**剧本管理**页面中，单击“关键运维操作实时通知”剧本所在行的“操作”列的“启用”。

步骤6 在弹出的确认框中，选择初始剧本版本v1后，单击“确定”。

----结束

14 权限管理

14.1 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，IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，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、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账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14-1**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，SecMaster支持的系统权限，请参见**SecMaster系统权限**。如果您需要对除SecMaster之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

如**表14-1**所示，包括了SecMaster的所有系统权限。

表 14-1 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

示例流程

图 14-1 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. **用户登录**并验证权限

   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，如果提示权限不足，表示“SecMaster FullAccess”已生效。

14.2 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**。

目前华为云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

```
{
   "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"
         ]
      }
   ]
}
```

14.3 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），如果账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。

15 云审计服务支持的关键操作

15.1 云审计服务支持的 SecMaster 操作列表

云审计服务（Cloud Trace Service，CTS）记录了安全云脑相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

云审计服务支持的SecMaster操作列表如**表 云审计服务支持的SecMaster操作列表**所示。

表 15-1 云审计服务支持的 SecMaster 操作列表

操作名称	资源类型	事件名称
剧本审核	playbook	approvePlaybook
创建剧本动作	playbook	createPlaybookAction
修改剧本动作	playbook	updatePlaybookAction
删除剧本动作	playbook	deletePlaybookAction
创建剧本	playbook	createPlaybook
修改剧本	playbook	updatePlaybook
删除剧本	playbook	deletePlaybook
操作剧本实例	playbook	operatePlaybookInstance
导出剧本实例	playbook	exportPlaybookInstance
导出剧本	playbook	exportPlaybook
导入剧本	playbook	importPlaybook
新增剧本触发规则	playbook	createPlaybookRule
更新剧本触发规则	playbook	updatePlaybookRule
删除剧本触发规则	playbook	deletePlaybookRule

操作名称	资源类型	事件名称
创建剧本版本	playbook	createPlaybookVersion
更新剧本版本	playbook	updatePlaybookVersion
删除剧本版本	playbook	deletePlaybookVersion
克隆剧本版本	playbook	clonePlaybookVersion
创建流程	workflow	createWorkflow
修改流程	workflow	updateWorkflow
删除流程	workflow	deleteWorkflow
创建流程版本	workflow	createWorkflowVersion
修改流程版本	workflow	updateWorkflowVersion
审核流程版本	workflow	approveWorkflowVersion
删除流程版本	workflow	deleteWorkflowVersion
导出流程	workflow	exportWorkflow
导入流程	workflow	importWorkflow
创建资产连接	asset	createAsset
创建资产连接	asset	updateAsset
删除资产连接	asset	deleteAsset
上传附件	component	uploadAttachement
创建插件模板	component	createComponentTemplate
更新插件模板	component	updateComponentTemplate
删除插件模板	component	deleteComponentTemplate
添加评论	task	commentTask
提交待办	task	commitTask
创建工作空间	workspace	createWorkspace
删除工作空间	workspace	deleteWorkspace
更新工作空间	workspace	updateWorkspace
重新收集子服务统计数据	workspace	recollectServiceStatistics

15.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。

- warning：表示操作失败。
- incident：表示比操作失败更严重的情况，例如引起其他故障等。

– 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。

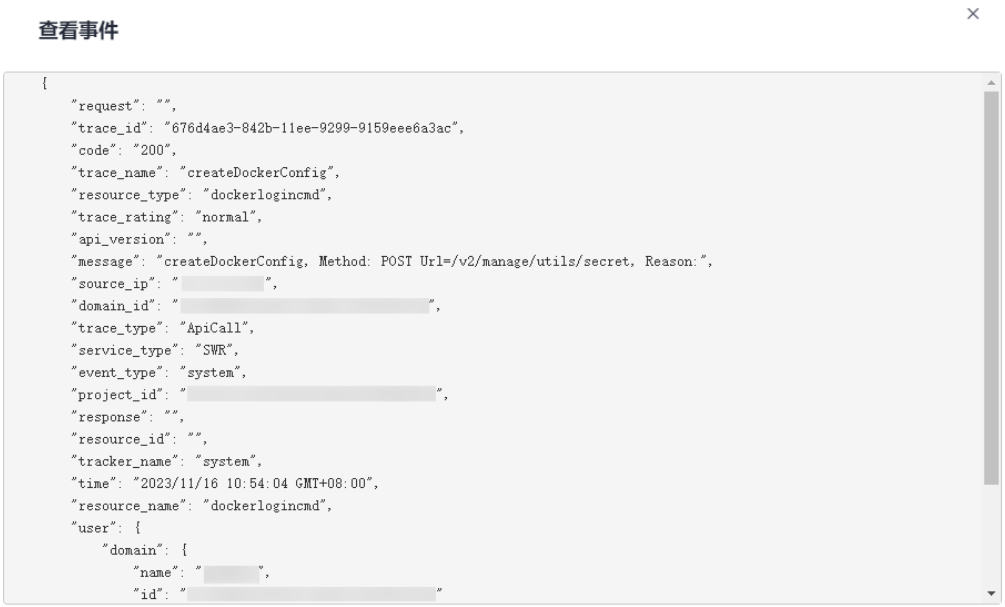
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   – 在搜索框中输入任意关键字，单击 按钮，可以在事件列表搜索符合条件的数据。
   – 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   – 单击按钮，可以获取到事件操作记录的最新信息。
   – 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   – 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   – 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   – 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   – 时间范围：可选择查询最近7天内任意时间段的操作事件。
   – 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**和**事件样例**。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

A 修订记录

发布日期	修改记录
2024-03-28	第十一次正式发布。 ● 更新**策略管理概述**、**新增/编辑应急策略**章节内容，更新约束限制并增加应急策略推荐配置说明。 ● 更新**采集数据**章节内容，增加ECS、VPC终端节点资源相关说明。 ● 更新**安全编排概述**、**查看剧本实例监控**章节内容，更新剧本、流程实例约束限制说明。 ● 更新**查看基线检查结果**章节内容，增加查看检查结果操作步骤。 ● 更新**查看资产信息**、**查看漏洞详情**、**查看事件信息**、**查看告警信息**、**查看情报指标**章节内容，更新查看数据描述信息。 ● 新增**一键阻断/解封**章节内容。

发布日期	修改记录
2024-02-29	第十次正式发布。 • 更新**编辑工作空间**章节内容，增加安全云脑对接标签服务资料描述。 • 更新**创建托管**章节内容，增加安全云脑对接Organizations资料描述信息。 • 更新**编辑/删除资产**章节内容，增加批量编辑资产操作步骤。 • 更新**查看告警信息**章节内容，告警详情页面优化，资料更新描述信息。 • 更新**查看基线检查结果**章节内容，新增检查结果页面描述。 • 更新**处理基线检查结果**章节内容，新增导入、导出检查结果操作指导。 • 更新**支持接入的日志**章节内容，新增支持接入安全云脑基线检查数据至安全分析管道中。 • 更新**工作空间概述**、**安全分析概述**章节内容，补充工作空间、安全分析的约束与限制。 • 更新**内置剧本和流程**章节内容，新增内置剧本、流程和资产连接。 • 更新**查看资产信息**、**查看漏洞详情**、**查看事件信息**、**查看告警信息**、**新增/编辑情报指标**章节内容，更新页面布局截图。 • 新增**舆情监测**功能资料说明。

发布日期	修改记录
2023-12-11	第九次正式发布。 • 更新**购买安全云脑**章节内容，安全云脑支持对接TMS服务，增加了相关描述内容。 • 更新**创建/复制安全报告**、**查看安全报告**章节内容，新增周报说明信息。 • 更新**总览**、**态势总览**、**综合态势感知大屏**、**值班响应大屏**、**资产大屏**、**威胁态势大屏**、**脆弱性大屏**章节内容，补充指标统计周期。 • 更新**查看已处理任务**章节内容，更新目录名称。 • 更新**服务委托授权**章节内容，补充安全云脑委托权限的说明。 • 更新**内置剧本和流程**章节内容，新增内置剧本、流程和资产连接。 • 新增**采集数据**章节内容。 • 删除“购买ECS”、“安装Agent”、“新增节点”、“配置组件”、“新增连接”、“配置解析器”、“新增采集通道”章节内容，优化合入**采集数据**章节。 • 删除“批量取消阻断”章节，合入**批量阻断/批量取消阻断**章节。 • 优化资料描述。
2023-10-30	第八次正式发布。 • 更新**创建/复制安全报告**章节内容，支持配置发送报告相关信息。 • 更新**查看安全报告**章节内容，新增月报展示内容说明信息。 • 新增**内置剧本和流程**章节内容，补充内置剧本、流程和资产连接信息。 • 新增**支持接入的日志**章节内容，补充可接入云服务日志信息。 • 新增**配置防线策略**章节内容。 • 删除“提交流程版本”章节内容，并更新**管理流程版本**章节内容，合入提交流程版本内容。 • 更新**购买标准版**、**购买专业版**章节内容，更新主机配额描述信息。 • 调整文档结构并优化资料描述。

发布日期	修改记录
2023-09-25	第七次正式发布。 ● 更新**资产管理概述**章节内容，新增资产来源以及对应的安全防护产品描述信息。 ● 更新**日志字段含义**章节内容，更新WAF攻击日志字段说明。 ● 更新**工作空间概述**章节内容，更新工作空间约束限制内容。 ● 新增**投递日志数据至LTS**章节内容。 ● 优化资料描述。
2023-08-10	第六次正式发布。 ● 更新**下载安全报告**章节内容，支持下载多种格式报告。 ● 更新**查看待办任务**章节内容，新增了备注信息。 ● 新增**查看已处理任务**章节，支持查看已处理任务信息。 ● 新增**设置资产订阅**章节内容，支持订阅其他region信息。 ● 新增**策略管理**章节，支持统一管理防线策略和应急策略。 ● 更新**查看事件信息**章节内容，可以查看受影响咨询信息。 ● 更新**关闭/删除事件**章节内容，支持批量关闭和删除事件。 ● 更新**查看告警信息**信息章节内容，可以查看受影响咨询信息。 ● 更新**告警转事件或关联事件**章节内容，新增告警关联事件操作。 ● 更新**关闭/删除告警**章节内容，支持批量关闭和删除告警。 ● 新增**告警处置建议**章节内容，针对TOP告警新增处理建议。 ● 更新**日志字段含义**章节内容，新增MTD告警字段说明。 ● 更新**安全编排使用流程**章节内容，系统内置剧本默认已激活，无需手动操作。 ● 新增**查看自定义类型**章节内容。 ● 更新**新增资产连接**、**管理资产连接**章节内容，更新描述信息。 ● 更新**数据采集概述**章节内容，增加了支持的安装系统。 ● 更新“购买ECS”章节内容，增加了支持的安装系统。 ● 更新**管理解析器**章节内容，支持自定义导入、导出解析器。 ● 删除“修改资产信息同步策略”章节，系统自动同步资产信息，无需再通过剧本进行同步。

发布日期	修改记录
2023-06-30	第五次正式发布。 • 新增**（可选）配置并启用流程**、**（可选）配置并启用剧本**章节内容。 • 更新**安全编排概述**、**安全编排使用流程**章节内容，优化描述信息。 • 删除“新增剧本”、“新增流程”、“新增布局”、“新增数据类”、“新增数据字段”章节内容。
2023-05-25	第四次正式发布。 • 新增**数据投递**、**服务委托授权**章节内容。 • 删除“资产管理访问授权”、“基线检查访问授权”章节内容，委托权限功能单独统一管理。 • 更新**综合态势感知大屏**、**值班响应大屏**、**资产大屏**、**威胁态势大屏**、**脆弱性大屏**章节数据详细说明。 • 优化文档描述。
2023-04-25	第三次正式发布。 • 新增**空间托管**章节内容。 • 新增**查看已购资源**章节内容，支持统一管理已购资源。 • 新增**脆弱性大屏**、**资产大屏**、**威胁态势大屏**章节内容。 • 新增**下载安全报告**章节内容。 • 新增**导入/导出资产**、“配置资产管理策略”章节内容，支持导入资产和管理资产同步策略。 • 新增**修复漏洞**、**导入/导出漏洞**、**忽略/取消忽略漏洞**章节内容。 • 新增**插件管理**章节内容。 • 新增**数据采集**章节内容，支持采集数据到安全云脑进行统一管理。 • 新增**导入/导出事件**、**导入/导出告警**、**导入/导出情报指标**章节内容。 • 更新**购买安全云脑**章节内容，新增智能分析增值包内容、版本升级内容。 • 更新**新增工作空间**章节内容，更新参数描述信息。 • 更新**创建/复制安全报告**章节内容，新增支持创建周报、月报描述。 • 更新**查看安全报告**章节内容，新增安全报告模板内容描述信息。 • 更新**查看资产信息**章节内容，更新各类资产分类展示描述信息。 • 更新**数据集成**章节内容，新增新接入数据源产品描述信息。

发布日期	修改记录
2023-02-20	第二次正式发布。 ● 刷新**总览**、**态势总览**章节内容，新增“合规检查”数据展示模块。 ● 刷新**购买增值包**章节内容，新增安排编排支持包周期购买说明。 ● 新增**删除工作空间**章节内容。 ● 新增**值班响应大屏**章节内容。 ● 刷新**漏洞管理**章节内容，新增“增漏洞统计”相关说明。 ● 刷新**事件管理**、**告警管理**、**情报管理**章节内容，新增事件/告警/情报统计情况描述。 ● 刷新“新增流程”章节内容，新增人工审核步骤，可以自定义审核人员。 ● 新增**目录定制**章节内容。
2022-12-10	第一次正式发布。