安全云脑

产品介绍

文档版本 08

发布日期 2025-02-17

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 什么是安全云脑 1
2 产品优势 2
3 应用场景 3
4 产品功能 4
5 个人数据保护机制 12
6 经验包 14
6.1 内置检查项 14
6.2 内置剧本 69
7 约束与限制 73
8 安全 77
8.1 责任共担 77
8.2 身份认证与访问控制 78
8.3 数据保护技术 78
8.4 审计与日志 79
8.5 服务韧性 79
8.6 监控安全风险 80
8.7 认证证书 81
8.8 安全编排 83
9 SecMaster 权限管理 84
10 与其他云服务的关系 89
11 基本概念 91
11.1 安全运营中心 91
11.2 总览和态势总览 96
11.3 工作空间 98
11.4 告警管理 98
11.5 安全编排 99
11.6 安全分析 100

1 什么是安全云脑

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

为什么选择安全云脑

- 一键安全合规：一键生成遵从报告，华为积累的全球安全合规经验服务化，帮助用户快速实现云上业务安全/隐私保护遵从。
- 一屏全面感知：采集各类安全服务的告警事件，并进行大数据关联、检索、排序，全面评估安全运营态势，支持大屏展示安全运营动态。
- 一云全局分析：结合华为云积累的每日数亿威胁情报定位威胁，多维关联分析，消除无效告警、识别潜在高级威胁。
- 一体全程处置：服务内置多种处理剧本，实现99%以上的安全事件分钟级自动化响应。

更多安全云脑产品优势请参见**产品优势**。

2 产品优势

见微知著的指标脉络与态势呈现

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

云原生的资产盘点与风险预防

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

智能高效的威胁检测与响应处置

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

灵活的环境集成与作战协同

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

3 应用场景

云安全的理念是“三分建设，七分运营”，安全云脑的应用场景即是占了七分的安全运营。主要有以下几个应用场景：

日常安全运营

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

重大保障

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

防护演练

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

安全评估

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

4 产品功能

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

同时，为满足不同场景下的安全需求，安全云脑提供了基础版、标准版和专业版供您选择，不同版本的功能存在差异，您可以根据业务需求选择合适的版本。

总览

总览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

表 4-1 总览功能介绍

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

工作空间管理

工作空间属于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。

表 4-2 工作空间功能说明

功能模块	功能描述	基础版	标准版	专业版
工作空间	• 空间管理： 安全云脑顶层工作台，单个工作空间可绑定项目和Region，可支撑不同场景下的工作空间运营模式。 • 空间托管：跨账号安全运营，可实现工作空间委托集中安全运营查看统一资产风险、告警和事件等。	√	√	√

安全治理

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

表 4-3 安全治理功能说明

功能模块	功能描述	基础版	标准版	专业版
安全治理	• 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。 **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。	×	×	√

已购资源

已购资源集中呈现当前账号已经购买的资源，方便统一管理已购资源。

表 4-4 已购资源功能说明

功能模块	功能描述	基础版	标准版	专业版
已购资源	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。	√	√	√

安全态势

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

表 4-5 安全态势功能介绍

功能模块	功能描述	基础版	标准版	专业版
态势总览	• 安全评分：根据安全云脑的分析检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。评估得分越低，即风险值越大，则整体资产安全隐患越大。 • 安全监控：集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。 • 安全趋势：呈现最近7天整体资产安全健康得分的趋势图。	√	√	√
安全大屏	利用AI技术将海量云安全数据的分析并分类，通过安全大屏将数据可视化展示，集中呈现云上实时动态，云上关键风险一目了然，掌握云上安全态势更简单，更直观，更高效。 **说明** 安全大屏功能需要在标准版/专业版基础上单独购买。 安全大屏还联动Astro大屏应用（Astro Canvas，简称AstroCanvas），支持指标自定义接入，页面零代码开发，数据分钟级接入。	×	√	√
安全报告	通过创建分析报告，定时以邮件形式向指定的收件人发送安全报告，及时掌握资产的安全状况数据。	×	×	√
任务中心	集中呈现当前需要进行处理的任务。	×	√	√

资产管理

资产管理支持对云上资产全面盘点，也可灵活纳管云外各种资产，点清所有资产，并呈现资产实时安全状态。

表 4-6 资产管理功能说明

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

风险预防

风险预防提供基线检查、漏洞管理、策略管理功能，帮助您的云安全配置达到等保、ISO、PCI等各类权威安全标准和华为云安全最佳实践标准；知晓全局的漏洞分布，并一键修复漏洞。

表 4-7 风险预防功能介绍

功能模块	功能描述	基础版	标准版	专业版
基线检查	通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。	√	√	√
漏洞管理	通过自动同步华为云主机安全服务（Host Security Service，HSS）的漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。	×	×	√
应急漏洞公告	针对业界披露的热点安全漏洞，支持每5分钟抓取一次安全漏洞讯息，获取最新应急漏洞公告详情。	√	√	√
策略管理	支持统一管理防线策略和应急策略。	×	√	√

威胁管理

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

表 4-8 威胁管理功能介绍

功能模块	功能描述	基础版	标准版	专业版
事件管理	集中呈现事件详情，支持人工转事件、自动化转事件。	×	√	√
告警管理	通过集成云服务告警，包含HSS、WAF、DDoS等，集中呈现并管理告警信息。	×	√	√
情报管理	支持基于告警和事件自定义规则提取指标。	×	×	√
智能建模	支持利用模型对管道中的日志数据进行扫描，如果检测到有满足模型中设置触发条件的内容时，系统将产生告警提示。	×	√	√
安全分析	• 查询与分析 – 检索分析：支持数据的快捷检索分析，支持安全调查场景安全数据的快速筛留、筛除等操作，快速定位关键数据。 – 筛选统计：支持数据字段快速分析统计，并基于分析结果进行数据的快速筛选；时序数据支持默认时间分区统计，快速识别数据量的变化趋势，支持基于时间分区的快速筛选；支持分析、统计、排序等丰富统计分析函数，支撑快速构建安全分析模型。 – 可视化：支持数据可视化分析，直观反映业务结构性和趋势性特征，并基于此构建自定义分析报告和分析指标。 • 数据投递：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。 • 数据监控：支持数据流量端到端的监控管理。 • 数据消费：提供数据消费和生产的流式通信接口，提供数据管道集成SDK，支持租户利用SDK进行系统集成，支持客户自定义数据的生产和消费。提供Logstash开源采集软件插件，支持利用开源生态进行数据消费和生产。 **说明** 需额外购买增值包中的安全分析功能。其中，安全分析、内置剧本、安全编排含有赠送配额，具体说明请参见**赠送规格说明**。	×	√	√

功能模块	功能描述	基础版	标准版	专业版
安全舆情	安全舆情监测可以持续挖掘和感知互联网安全态势变化，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，还可以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** 仅部分region支持使用安全舆情监测功能，具体开放region请参见**功能总览**。其他region如需使用该功能，需先**提交工单**申请开通使用权限。	√	√	√

安全编排

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

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

表 4-9 安全编排功能介绍

功能模块	功能描述	基础版	标准版	专业版
运营对象	集中对数据类、数据类类型、分类映射等运营对象进行管理。	×	√	√
剧本编排	支持对剧本、流程、资产连接、实例的全生命周期管理。 **说明** 需额外购买增值包中的安全编排功能。其中，安全分析、内置剧本、安全编排含有赠送配额，具体说明请参见**赠送规格说明**。	×	√	√
页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。	×	√	√
插件管理	支持将安全编排流程中使用的插件进行统一管理。	×	×	√

数据采集

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

表 4-10 数据采集功能说明

功能模块	功能描述	基础版	标准版	专业版
数据采集（采集管理和组件管理）	使用Logstash通过多种方式采集各类日志数据。采集后，可以快速实现历史数据分析比对、数据关联分析、以及未知威胁发现等相关分析。	×	√	√

数据集成

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

表 4-11 数据集成功能说明

功能模块	功能描述	基础版	标准版	专业版
数据集成	云内置采集系统，支持一键集成存储、管理与监管、安全等多种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。	×	√（仅支持集成云服务告警）	√

目录定制

支持自定义目录，可以根据需要对目录进行定制。

表 4-12 目录定制功能说明

功能模块	功能描述	基础版	标准版	专业版
目录定制	支持查看已有目录及更换布局等操作。	×	√	√

赠送规格说明

安全云脑增值包中的安全分析、安全编排功能在不同的版本有不同的赠送配额，具体说明如下：

表 4-13 赠送规格说明

功能		标准版	专业版
安全分析	安全数据采集	120 MB/天/配额	120 MB/天/配额

功能		标准版	专业版
	安全数据保留	120 MB/天/配额	120 MB/天/配额
	安全数据导出	120 MB/天/配额	120 MB/天/配额
	平台安全数据	40 MB/天/配额	40 MB/天/配额
	安全建模分析	×	120 MB/天/配额
威胁管理	预制威胁模型	×	计算模型数据120 MB/天/配额；预置模型200个
	预制响应剧本	×	预置剧本30个
安全编排	安全编排	×	操作7000次

5 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、邮箱等）不被未经过认证、授权的实体或者个人获取，安全云脑（SecMaster）通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

安全云脑收集及产生的个人数据如表5-1所示。

表 5-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
邮箱	采用邮箱方式启用通知类剧本时，安全云脑获取对应消息通知服务主题订阅的邮箱。 或者开启安全分析报告定时发送功能时，安全云脑获取用户在界面输入的接收邮箱地址（需要经过拥有接收邮箱地址的用户授权同意接收安全分析报告邮件）。	是	是
请求源IP	安全云脑上开启WAF防护场景，有攻击防护域名时，被WAF拦截或者记录的攻击者IP。	否	是
URL	安全云脑上开启WAF防护场景，有攻击的防护域名的URL，被WAF拦截或者记录的防护域名的URL。	否	是
HTTP/HTTPS Header信息（包括Cookie）	安全云脑上开启WAF防护场景，且有攻击命中用户配置的CC攻击、精准访问防护规则时，在攻击告警中可能携带用户在配置界面输入的Cookie值和Header值。	否	否 如果配置的Cookie和Header信息不含有用户的个人信息，则安全云脑也不会收集及产生用户的个人数据。

类型	收集方式	是否可以修改	是否必须
请求参数（Get、Post）	安全云脑上开启WAF防护场景，在WAF防护日志里，WAF记录的请求详情。	否	否 如果请求参数里不含有用户的个人信息，则WAF记录的相关请求中不会收集及产生用户的个人数据。
登录位置信息	安全云脑上开启HSS主机防护场景，服务器开启防护后，登录云服务器时，HSS记录的用户登录位置信息。	否	是

存储方式

安全云脑（SecMaster）通过加密算法对用户个人敏感数据加密后进行存储。

- 邮箱：加密存储。
- 登录位置信息：不属于敏感数据，明文存储。
- 请求源IP、URL、HTTP/HTTPS Header信息（包括Cookie）、请求参数（Get、Post）：对敏感字段提供了脱敏配置，其他字段在日志中明文保存。

访问权限控制

用户个人数据通过加密后存储在安全云脑数据库中，数据库的访问需要通过白名单的认证与授权。

用户只能查看自己业务的相关日志。

6 经验包

6.1 内置检查项

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 6-1 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
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

检查规范	检查类别		包含的检查项数量
		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
华为云安全配置基线	网络		6
	身份与访问管理		16
	安全		14
	日志与监控		17
	虚拟机与容器		16
	数据库		31
	存储		17
	企业智能		14

安全上云合规检查—身份与访问管理

表 6-2 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。

安全上云合规检查一检测

表 6-3 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 6-4 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（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（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 6-5 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 6-6 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 6-7 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（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（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，您的主机才能受到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（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 6-8 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 6-9 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 6-10 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 6-11 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 6-12 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 6-13 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 6-14 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 6-15 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连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连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 6-16 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 6-17 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 6-18 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 6-19 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 6-20 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 6-21 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 6-22 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 6-23 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 6-24 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 6-25 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 6-26 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 6-27 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 6-28 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 6-29 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 6-30 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 6-31 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。

华为云安全配置基线—网络

表 6-32 网络风险项检查项

检查子项目	检查项目
确保限制SSH的Internet公网访问	SSH协议多作用于远程连接并管理主机，默认端口为22，在网络攻击中经常作为资源扫描和暴力破解的入口。 配置VPC子网的网络ACL规则/安全组时，禁止配置源地址为 0.0.0.0/0 或者::/0 的SSH协议相关端口规则。如业务所必须，需要按照白名单的形式配置特定的源IP。
确保安全组不允许源地址0.0.0.0/0访问远程管理端口及高危端口	配置VPC安全组规则时，建议在安全组入方向规则中不应该对外远程管理端口、高危端口，如业务所必需，建议根据最小化开放原则开放此类端口。 源地址为 0.0.0.0/0 或::/0，公网地址掩码小于32以及内网地址掩码小于24即被视为不满足最小化访问控制原则。 高危端口至少包括：20、21、135、137、138、139、445、389、593、1025。 远程管理端口包括：23、177、513、4899、6000~6063、5900、5901。
确保子网ACL不允许源地址0.0.0.0/0访问远程管理端口及高危端口	配置VPC子网的网络ACL规则时，建议在网络ACL入方向规则中不应该对外远程管理端口、高危端口，如业务所必需，建议根据最小化开放原则开放此类端口。 源地址为 0.0.0.0/0 或::/0，公网地址掩码小于32以及内网地址掩码小于24即被视为不满足最小化访问控制原则。 高危端口至少包括：20、21、135、137、138、139、445、389、593、1025。 远程管理端口包括：23、177、513、4899、6000~6063、5900、5901。
确保限制RDP的Internet公网访问	RDP协议作用于远程桌面连接并管理主机，默认端口为3389，在网络攻击中经常作为资源扫描和暴力破解的入口。配置VPC子网的网络ACL规则/安全组时，禁止配置源地址为 0.0.0.0/0 或者::/0 的RDP协议相关端口规则。如业务所必须，需要按照白名单的形式配置特定的源IP。

检查子项目	检查项目
启用ELB监听器的访问控制	ELB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。 访问流量的IP先通过白名单或黑名单访问控制，然后负载均衡转发流量，通过安全组安全规则限制，所以安全组的规则设置是不会影响负载均衡的白名单或黑名单设置访问控制。 访问控制只限制实际业务的流量转发，不限制ping命令操作，被限制的IP仍可以ping通后端服务器。 对于共享型负载均衡实例来说，需要创建监听器并添加后端云服务器，才可以ping通。 对于独享型负载均衡实例来说，创建完监听器，不需要添加后端云服务器，即可以ping通。
确保VPC对等连接满足最小化访问控制	对等连接是指两个VPC之间的网络连接，对于对等连接的路由应该满足最小访问权限原则。 建议本端路由的目的地址最好限定在最小子网网段内，对端路由的目的地址最好限定在最小子网网段内。

华为云安全配置基线—身份与访问管理

表 6-33 身份与访问管理风险项检查项

检查子项目	检查项目
设置初始IAM用户时，避免对具有控制台密码的用户设置访问密钥	为了提高账号资源的安全性，建议在设置初始IAM用户时，对具有控制台密码的IAM用户，不要设置访问密钥。
启用访问密钥保护	为了提高账号资源的安全性，需开启访问密钥保护功能。“访问密钥保护”功能默认为关闭状态。开启该功能后，仅管理员才可以创建、启用/停用或删除 IAM 用户的访问密钥。
启用用户登录保护	为了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，用户可在 IAM 的安全设置中开启登录保护。开启后用户登录时除了需要口令认证还需要通过虚拟 MFA 或短信或邮件验证，以再次确认登录者身份。
确保IAM密码每180天或更短时间轮换一次	IAM 用户的密码有效期策略必须设置，建议满足以下要求： 设置密码过期后，系统强制要求修改密码（密码有效期设置为 180 天或更短时间）。

检查子项目	检查项目
确保设置密码最短使用时间	IAM 用户密码最短使用时间策略必须设置，建议满足以下要求： 设置密码最短使用时间，必须超过设置的时间，才能进行修改（最短使用时间设置为 5 分钟）。
确保IAM密码策略要求最小长度为8或更大	密码策略 IAM 用户的密码策略应设置强密码策略，建议满足以下要求： 密码长度不小于 8 位。
启用用户操作保护	为了进一步提高账号安全性，有效确保用户安全地使用云产品，用户可在 IAM 中开启操作保护。开启后，主账号及子用户在控制台进行敏感操作时（例如：删除弹性云服务器、弹性 IP 解绑等），将通过虚拟 MFA 或手机短信或邮件再次确认操作者的身份。
确保任何单个IAM用户仅有一个可用的活动访问密钥	为了提高账号资源的安全性，建议单个 IAM 用户仅有一个可用的活动访问密钥。
确保IAM密码策略要求符合密码复杂度	IAM 用户的密码策略应设置强密码策略，建议满足以下要求： ● 包含以下字符中的 3-4 种：大写字母、小写字母、数字和特殊字符。 ● 密码中允许同一字符连续出现次数（最大次数设置为 1）。
确保管理员账号已启用MFA	虚拟Multi-Factor Authentication（MFA）是多因素认证方式的一种，用户需要先在智能设备上安装一个MFA应用程序（例如：“华为云”手机应用程序），才能绑定虚拟MFA设备。绑定MFA后，用户在登录时或进行敏感操作前需输入MFA随机产生的6位数字认证码。MFA设备可以基于硬件也可以基于软件，目前华为云仅支持基于软件的虚拟MFA。用户登录Console控制台必须启用MFA，保证安全登录。
确保IAM密码策略防止密码重复使用	IAM 用户的密码策略应设置强密码策略，建议满足以下要求： 新密码不能与最近的历史密码相同（重复次数设置为 3）。

检查子项目	检查项目
配置IAM的网络访问控制策略	管理员可以设置访问控制策略，限制用户只能从特定 IP 地址区间、网段及 VPC Endpoint 访问华为云： 1. 允许访问的 IP 地址区间：限制用户只能从设定范围内的 IP 地址访问华为云，可以在 0.0.0.0~255.255.255.255 之间设置。默认值为 0.0.0.0~255.255.255.255。如不设置或设置为默认值，意味着用户的 IAM 用户可以从任意地方访问华为云。 2. 允许访问的 IP 地址或网段：限制用户只能从设定的 IP 地址或网段访问华为云，例如：10.10.10.10/32。 3. 允许访问的 VPC Endpoint：仅在“API 访问”页签中可进行配置。限制用户只能从具有设定ID的VPC Endpoint访问华为云API，例如：0ccad098-b8f4-495a-9b10-613e2a5exxxx 访问控制生效条件： a. 控制台访问：仅对账号下的IAM用户登录控制台生效，对账号本身不生效。 b. API 访问：仅对账号下的IAM用户通过API网关访问API接口生效，修改后2小时内生效。
确保管理员账号禁用AK/SK	为了进一步提高账号安全性，有效确保用户安全地使用云产品，用户可在 IAM 中开启操作保护。开启后，主账号及子用户在控制台进行敏感操作时（例如：删除弹性云服务器、弹性 IP 解绑等），将通过虚拟 MFA 或手机短信或邮件再次确认操作者的身份。
确保不创建允许“*:*”管理权限的IAM策略	为了提高账号资源的安全性，不创建允许“*:*”管理权限的 IAM 策略。

检查子项目	检查项目
配置登录验证策略	管理员可以设置登录验证策略，包括“会话超时策略”、“账号锁定策略”、“账号停用策略”、“最近登录提示”、“登录验证提示”。 1. 会话超时策略：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。管理员可以设置会话超时的时长，会话超时时长默认为1个小时，可以在15分钟~24小时之间进行设置。 2. 账号锁定策略：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。管理员可以设置账号锁定时长、锁定前允许的最大登录失败次数、重置账号锁定计数器的时间： ● 账号锁定时长（分钟）：默认为 15 分钟，可以在 15~30 分钟之间进行设置。 ● 锁定前允许的最大登录失败次数：默认为 5 次，可以在 3~10 次之间进行设置。 ● 重置账号锁定计数器的时间：默认为 15 分钟，可以在 15~60 分钟之间进行设置。 3. 账号停用策略：如果 IAM 用户在设置的有效期内没有通过界面控制台或者API访问华为云，将会被停用。账号停用策略默认关闭，管理员可以选择开启，并在 1~240 天之间进行设置。该策略仅对账号下的 IAM 用户生效，对账号本身不生效。IAM用户被停用后，可以联系管理员重新启用。 4. 最近登录提示：如果开启最近登录提示，用户登录成功后，将在“登录验证”页面中看到上次登录成功时间，最近登录提示可以帮助用户查看是否存在异常登录信息，如果存在不是本人的登录信息，建议立即修改密码。最近登录提示默认关闭，管理员可以选择开启。 5. 登录验证提示：管理员可以在最近登录提示中进行公告，例如欢迎语，或者提示用户谨慎删除资源等。登录验证提示默认关闭，管理员可以选择开启。开启后，用户将在“登录验证”页面中看到公告信息。
确保不创建非管理员权限的IAM用户	“admin”为缺省用户，具有所有云服务资源的操作权限，当所有用户全部属于admin用户组或共用一个企业管理员账号是不安全的。为了更好的管控人员或应用程序对云资源的使用，可以使用统一身份认证服务（IAM）的用户管理功能，给员工或应用程序创建IAM用户。

华为云安全配置基线—安全

表 6-34 安全风险项检查项

检查子项目	检查项目
启用勒索病毒防护（旗舰版/容器版/网页防篡改版）	勒索病毒入侵主机后，会对主机数据进行加密勒索，导致主机业务中断、数据泄露或丢失，主机所有者即使支付赎金也可能难以挽回所有损失，因此勒索病毒是当今网络安全面临的最大挑战之一。企业主机安全支持静态、动态勒索病毒防护，定期备份主机数据，可以帮助您抵御勒索病毒，降低业务损失风险。
启用CBH并开启多因子认证	启用云堡垒机（Cloud Bastion Host，CBH）可以实时收集和监控网络环境中每个组成部分的系统状态、安全事件和网络活动，保障网络和数据不受来自外部或内部用户的入侵和破坏，便于集中报警、及时处理及审计定责。为了进一步提高堡垒机账号安全性，用户可启用云堡垒机服务（CBH）的多因子认证功能。启用后，用户通过Web浏览器或SSH客户端登录CBH实例时需进行多因子认证。多因子认证方式包括：手机短信、手机令牌、USBKey、动态令牌。
启用企业主机安全 HSS（基础版/专业版/企业版/旗舰版）	主机实例（例如：ECS、BMS）应安装企业主机安全防护（HSS）且开启防护，全面识别并管理主机资产，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。
启用WAF防护事件告警通知	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。
配置WAF回源IP（源站服务器部署在ECS）	回源 IP是WAF用来代理客户端请求服务器时用的源 IP，在服务器看来，接入WAF后所有源 IP都会变更为WAF的回源 IP，真实的客户端 IP会被加载HTTP头部的字段中。当WAF后未配置ELB，应配置只允许WAF的回源 IP访问ECS。
启用SecMaster高危告警自动通知	启用安全云脑（SecMaster）的高危告警自动通知，当检测到高危告警时，用户可以及时收到邮件/短信通知，从而快速处置和响应。
启用WAF对Web基础防护的拦截模式	Web基础防护支持“拦截”和“仅记录”模式。“仅记录”模式仅会记录攻击行为，并不会对攻击行为进行阻断，建议开启Web基础防护的“拦截”模式，以在发现攻击后立即阻断并记录。
启用云防火墙 CFW功能	对于有弹性公网 IP（EIP）对外暴露业务的用户，建议启用云防火墙（CFW）。启用后，所有经过EIP的公网出入流量都会先经过CFW，恶意攻击流量会被CFW检测并阻断，而正常流量返回给业务服务器，从而确保业务服务器安全、稳定、可用。

检查子项目	检查项目
启用Web应用防火墙功能	对于有Web业务的用户，要求启用Web应用防火墙服务（ WAF ）。启用后，网站所有的公网流量都会先经过WAF，恶意攻击流量会被WAF检测并过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。
启用CFW告警通知	通过创建告警规则完成对日志的实时监控，当日志中的出现满足设定规则时产生告警，并通过短信或邮件的方式通知用户，可以用来实时监控日志中出现的异常信息。
启用DEW凭据托管功能	启用数据加密服务（ Data Encryption Workshop，DEW ）凭据托管功能，实现对数据库账号口令、服务器口令、SSH Key、访问密钥等各类型凭据的统一管理、检索与安全存储。
配置WAF地理位置访问策略	用户可以通过WAF配置地理位置访问控制规则，以实现对指定国家、地区的来源IP的自定义访问控制。
配置WAF回源IP（源站服务器部署在ELB ）	回源IP是WAF用来代理客户端请求服务器时用的源IP，在服务器看来，接入WAF后所有源IP都会变更WAF的回源IP，真实的客户端IP会被加载HTTP头部的字段中。当WAF后配置了ELB，应配置只允许WAF的回源IP访问ELB。
启用HSS网页防篡改功能	应开启HSS中的网络防篡改防护，以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。

华为云安全配置基线—日志与监控

表 6-35 日志与监控风险项检查项

检查子项目	检查项目
启用RDS数据库审计功能	当用户开通SQL审计功能，系统会将所有的SQL操作记录下来存入日志文件，方便用户下载并查询。SQL审计功能默认关闭，启用该功能可能会有一定的性能影响。
启用DBSS数据库安全审计告警通知功能	通过设置告警通知，当数据库发生设置的告警事件时，用户可以收到DBSS发送的告警通知，及时了解数据库的安全风险。否则，无论是否有危险，用户都只能登录管理控制台自行查看，无法收到告警信息。
启用DBSS数据库安全审计功能	数据库应开通数据库审计功能，数据库安全服务（ DBSS ）的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。
确保存储日志的OBS桶为非公开可读	确保存储审计日志的桶，非公开可读，防止审计日志被非法访问。

检查子项目	检查项目
启用CTS	用户开通云审计服务（CTS）后，系统会自动创建一个追踪器，该追踪器会自动识别并关联当前租户所使用的所有云服务，并将当前租户的所有操作记录在该追踪器中。CTS服务具备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。
启用CTS的关键操作通知功能	关键操作包含高危操作（重启虚拟机、变更安全配置等）、成本敏感操作（创建、删除高价资源等）、业务敏感操作（网络配置变更等）。下面列出部分云服务的关键操作项： ● IAM：createUser、deleteUser、createAgency、DeleteAgency 等 ● ECS：rebootServer、updateSecurityGroup、removeSecurityGroup 等 ● VPC：modifySecurityGroup 等 ● CTS：updateTracker、deleteTracker 等 ● OBS：setBucketAcl、setBucketPolicy 等 启用CTS的关键操作通知功能后，CTS会对这些关键操作通过消息通知服务（SMN）实时向相关订阅者发送通知，该功能由CTS触发，SMN完成通知发送。 CTS中需要开启关键操作通知，配置操作类型建议设置为自定义（包括删除、创建、登录）。在录入某些关键操作时，CTS可以通过SMN实时向订阅者发送通知。该功能由CTS触发，SMN发送通知。如Root Login，即企业管理员有登录事件时发送通知；或CTS更改意味着当CTS跟踪器发生更改时发送通知。
启用OBS桶日志功能	出于分析或审计等目的，用户可以开启 OBS 桶日志记录功能。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。当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中。
开启日志文件加密存储	将审计日志转储到OBS，可以配置加密存储，防止文件被非法访问。
启用WAF全量日志功能	启用WAF全量日志功能后，可以将攻击日志、访问日志记录到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。开启全量日志功能是将WAF日志记录到LTS，不影响WAF性能。

检查子项目	检查项目
启用LTS日志转储	主机和云服务的日志数据上报至云日志服务（LTS）后，在默认存储事件过期后会被自动删除。因此，对于需要长期存储的日志数据，应在LTS中配置日志转储。LTS支持将日志转储至以下云服务： ● OBS：提供日志存储功能，长期保存日志。 ● 数据接入服务（DIS）：提供日志长期存储能力和丰富的大数据分析能力。
启用VPC流量日志功能	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助用户优化安全组和防火墙控制规则、监控网络流量、进行网络攻击分析等。当用户想要了解虚拟私有云网卡的流量详情时，用户可以通过LTS实时查看虚拟私有云的网卡日志数据。
启用LTS主机全量日志功能	当用户选择了主机接入方式时，LTS可以将主机待采集日志的路径配置到日志流中，ICAgent将按照日志采集规则采集日志，并将多条日志进行打包，以日志流为单位发往LTS，用户可以在LTS控制台实时查看日志。
确保LTS存储时长满足需求	主机和云服务的日志数据上报至云日志服务（LTS）后，在默认存储事件过期后会被自动删除。因此，需要用户根据业务需求配置存储时长。
启用ELB访问日志记录功能	ELB在外部流量分发时，会记录HTTP(S)详细的访问日志记录，如URI请求、客户端 IP和端口、状态码。ELB日志可用于审计，也可用于通过时间和日志中的关键词信息搜索日志，同时，也可以通过各种SQL聚合函数来分析某段时间内的外部请求统计数据，以掌握真实用户的网站使用频率等。
启用FuctionGraph函数日志功能	出于分析或审计等目的，用户可以开启FunctionGraph日志功能。通过访问日志记录，函数拥的拥有者可以分析函数执行过程，快速定位问题。
启用CFW日志管理能力	将攻击事件日志、访问控制日志、流量日志记录到云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的CFW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。
开启日志文件完整性校验	将审计日志转储到OBS，可以同步开启文件校验，保障审计文件的完整性，防止文件被篡改。

华为云安全配置基线—虚拟机与容器

表 6-36 虚拟机与容器风险项检查项

检查子项目		检查项目
云容器引擎 CCE	启用HSS的容器安全版	企业主机安全（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。推荐启用HSS服务保护CCE集群中的Node节点及之上的容器。
	禁止容器获取宿主机元数据	租户使用CCE集群作为共享资源池来构建高阶服务，且允许高阶服务的最终用户在集群中创建不可控的容器负载时，应限制容器访问所在宿主机的元数据。
	启用LTS服务并采集容器日志	云日志服务（Log Tank Service，简称LTS）用于收集来自主机和云服务的日志数据，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为您提供实时、高效、安全的日志处理能力，帮助您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。 建议统一采集容器日志(包括容器标准输出、容器内的日志文件、节点日志文件和Kubernetes事件)并上报到LTS。
	禁止使用CCE已经EOS的K8S集群版本	集群版本EOS后，CCE将不再支持对该版本的集群创建，同时不提供相应的技术支持，包含新特性更新、漏洞/问题修复、补丁升级以及工单指导、在线排查等客户支持，不再适用于CCE服务SLA保障。 请留意CCE Console公告栏或CCE官方资料中的Kubernetes版本策略，在集群生命周期截止前参考集群升级等资料及时完成升级。
	集群apiserver不要暴露到公网	Kubernetes API具备访问控制能力，但偶尔存在一些无访问控制的CVE漏洞，同时为减少攻击者刺探Kubernetes API版本，建议非必须不要为集群绑定EIP，以减少攻击面。在必须绑定EIP的情况下，应通过合理配置防火墙或者安全组规则，限制非必须的端口和IP访问。
	限制业务容器访问管理面	在节点上的业务容器无需访问kube-apiserver时，建议禁止节点上的容器网络流量访问到kube-apiserver。

检查子项目		检查项目
	及时处置CCE在官网发布的漏洞	CCE服务会不定期发布涉及的漏洞，用户需及时关注和处理。对于高危漏洞，当Kubernetes社区发现漏洞并发布修复方案后，CCE一般在1个月内进行修复，修复策略与社区保持一致。在CCE官方未彻底修复漏洞前，请租户参考CCE官方提供的消减措施为最大化降低漏洞带来的影响。
	集群节点不要暴露到公网	节点对公网暴露后，攻击者可通过互联网发起攻击，攻破节点后可能会进一步控制集群。 如非必需，集群节点不建议绑定EIP，以减少攻击面。在必须绑定EIP的情况下，应通过合理配置防火墙或者安全组规则，限制非必须的端口和IP访问。 在使用CCE集群过程中，由于业务场景需要，在节点上配置了kubeconfig.json文件，kubectl使用该文件中的证书和私钥信息可以控制整个集群。在不需要时，请清理节点上的/root/.kube目录下的目录文件，防止被恶意用户利用： rm -rf /root/.kube
	加固K8S集群所在VPC的安全组规则	CCE作为通用的容器平台，安全组规则的设置适用于通用场景。用户可根据安全需求，通过网络控制台的安全组找到CCE集群对应的安全组规则进行安全加固。
弹性云服务器 ECS	确保ECS内的重置密码插件更新到最新版本	弹性云服务器提供一键式重置密码功能。当弹性云服务器的密码丢失或过期时，如果提前安装了一键式重置密码插件，则可以应用一键式重置密码功能，给弹性云服务器设置新密码。及时更新重置密码插件可确保漏洞及时得到修复。
	在ECS内设置防火墙策略限制对元数据的访问	弹性云服务器元数据包含了弹性云服务器在云平台的基本信息，例如云服务ID、主机名、网络信息等，亦可能包含敏感信息，GuestOS的多用户设计会导致元数据访问范围开放过大，租户APP的SSRF漏洞也可能导致元数据泄露。 在ECS内设置防火墙策略限制对元数据的访问，可以限制元数据访问范围，消减元数据泄露风险。

检查子项目		检查项目
	确保私有镜像开启了加密	镜像加密支持私有镜像的加密。在创建弹性云服务器时，用户如果选择加密镜像，弹性云服务器的系统盘会自动开启加密功能，从而实现弹性云服务器系统盘的加密。
	使用密钥对安全登录ECS	密钥对，即SSH密钥对，是为用户提供远程登录云服务器的认证方式，是一种区别于传统的用户名和密码登录的认证方式。 密钥对包含一个公钥和一个私钥，公钥自动保存在KPS（Key Pair Service）中，私钥由用户保存在本地。若用户将公钥配置在Linux云服务器中，则可以使用私钥登录Linux云服务器，而不需要输入密码。 由于密钥对可以让用户无需输入密码登录到Linux云服务器，因此，可以防止由于密码被拦截、破解造成的账户密码泄露，从而提高Linux云服务器的安全性。
裸金属服务器 BMS	使用密钥对安全登录BMS	密钥对，即SSH密钥对，是为用户提供远程登录云服务器的认证方式，是一种区别于传统的用户名和密码登录的认证方式。 密钥对包含一个公钥和一个私钥，公钥自动保存在KPS（Key Pair Service）中，私钥由用户保存在本地。若用户将公钥配置在Linux云服务器中，则可以使用私钥登录Linux云服务器，而不需要输入密码。 由于密钥对可以让用户无需输入密码登录到Linux云服务器，因此，可以防止由于密码被拦截、破解，造成的账户密码泄露，从而提高Linux云服务器的安全性。
	确保BMS内的重置密码插件更新到最新版本	裸金属服务器提供一键式重置密码功能。当裸金属服务器的密码丢失或过期时，如果提前安装了一键式重置密码插件，则可以应用一键式重置密码功能，给裸金属服务器设置新密码。 及时更新重置密码插件可确保漏洞及时得到修复。

检查子项目		检查项目
	在BMS内设置防火墙策略限制对元数据的访问	裸金属服务器元数据包含了裸金属服务器在云平台的基本信息，例如云服务ID、主机名、网络信息等，亦可能包含敏感信息，GuestOS的多用户设计会导致元数据访问范围开放过大，租户APP的SSRF漏洞也可能导致元数据泄露。 在BMS内设置防火墙策略限制对元数据的访问，可以限制元数据访问范围，消减元数据泄露风险。

华为云安全配置基线—数据库

表 6-37 数据库风险项检查项

检查子项目		检查项目
RDS for MySQL	配置合理的安全组规则	安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求，保障数据库的安全性和稳定性。
	避免绑定EIP直接通过互联网访问	避免RDS for MySQL部署在互联网或者DMZ里，应该将RDS for MySQL部署在公司内部网络，使用路由器或者防火墙技术把RDS for MySQL保护起来，避免直接绑定EIP方式从互联网访问RDS for MySQL。通过这种方式防止未授权的访问及DDoS攻击等。
	开启加密通信	如果未启用TLS加密连接，那么在MySQL客户端和服务器之间以明文形式传输数据，容易受到窃听、篡改和“中间人”攻击。如果您是通过像Internet这样的非安全网络连接到MySQL服务器，那么启用TLS加密连接就显得非常重要。
	禁止使用默认端口	MySQL的默认端口是3306，使用默认端口容易被监听，存在安全隐患，推荐使用非默认端口。
	开启透明数据加密功能	对数据文件执行实时 I/O 加密和解密，数据在写入磁盘之前进行加密，从磁盘读入内存时进行解密，能有效保护数据库及数据文件的安全。
	数据库版本更新到最新版本	MySQL社区有新发CVE漏洞时，会及时分析漏洞的影响，依据漏洞实际风险的影响大小决定补丁发布计划。建议及时升级修复，避免漏洞影响数据的安全。

检查子项目		检查项目
	开启数据库审计日志	审计功能可以记录用户对数据库的所有相关操作。通过查看审计日志，您可以对数据库进行安全审计、故障根因分析等操作，提高系统运维效率。
RDS for PostgreSQL 数据库	开启备份功能设置合理的备份策略	定期对数据库进行备份，当数据库故障或数据损坏时，可以通过备份文件恢复数据库，从而保证数据可靠性。
	开启用户登录时日志记录功能	为了保证数据库的安全性和可追溯性，登录者所有的操作都会记录，以达到安全审计的目的。log_connections可以记录每次尝试连接到服务器的连接认证日志，log_disconnections记录用户注销时的日志，当受到攻击或者内部员工误操作而造成重要的数据丢失时，能够及时定位登录的IP地址。
	禁止使用默认端口	PostgreSQL的默认端口是5432，使用默认端口容易被监听，存在安全隐患，推荐使用非默认端口。
	配置合理的安全组规则	安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求，保障数据库的安全性和稳定性。
	配置客户端认证超时时间	authentication_timeout控制完成客户端认证的时间上限，单位是秒。该参数可以防止客户端长时间占用连接通道，默认是60s。
	限制连接数据库的IP地址	如果对连接数据库的IP地址不设置限制，全网都可访问，直接会增大攻击面。
	开启数据库审计日志	通过将PostgreSQL审计扩展（pgAudit）与RDS for PostgreSQL数据库实例一起使用，可以记录用户对数据库的所有相关操作，通过查看审计日志，您可以对数据库进行安全审计、故障根因分析等操作，提高系统运维效率。
	数据库版本更新到最新版本	PostgreSQL社区当前 9.5/9.6/10 版本已经EOL，社区已不再维护，云上 9.5/9.6 版本已经发布EOS公告。使用较老的版本可能存在漏洞，运行最新版本的软件可以避免受到某些攻击。

检查子项目		检查项目
GaussDB 数据库	数据库连接的最大并发连接数配置	如果GaussDB连接数过高，会消耗服务器大量资源，导致操作响应变慢，同时要根据操作系统环境来设置最大连接数，如果高于操作系统接收的最大线程数，设置无效。 通过设置最大连接数，可以避免出现DDoS攻击，同时可以用最合理的方式利用系统的资源，达到最佳的OPS响应能力。
	权限管理	防止PUBLIC拥有CREATE权限，导致数据库任何账户都可以在PUBLIC模式下创建表或者其他数据库对象，需要对PUBLIC的权限进行限制
	开启数据库审计日志	审计功能可以记录用户对数据库的所有相关操作。通过查看审计日志，您可以对数据库进行安全审计、故障根因分析等操作，提高系统运维效率。
	安全认证配置	为了保证用户体验，同时为了防止账户被人通过暴力破解，GaussDB设置了账户登录重试次数及失败后自动解锁时间的保护措施。
	用户密码的安全策略	用户密码存储在系统表pg_authid中，为防止用户密码泄露，GaussDB对用户密码进行加密存储，所采用的加密算法由配置参数password_encryption_type决定； GaussDB数据库用户的密码都有密码有效期，可以通过参数password_notify_time提醒客户修改密码，如果需要修改密码有效期，可以通过修改password_effect_time来更改。
	WAL归档配置	WAL（Write Ahead Log）即预写式日志，也称为Xlog。
	开启备份功能设置合理的备份策略	当数据库或表被恶意或误删除，虽然GaussDB支持高可用，但备机数据库会被同步删除且无法还原。因此，数据被删除后只能依赖于实例的备份保障数据安全。
DDS 文档数据库	开启加密通信	如果未启用TLS加密连接，那么在MongoDB客户端和服务器之间以明文形式传输数据，容易受到窃听、篡改和“中间人”攻击。 如果您是通过像Internet这样的非安全网络连接到MongoDB服务器，那么启用TLS加密连接就显得非常重要。

检查子项目		检查项目
	开启备份功能设置合理的备份策略	DDS实例支持自动备份和手动备份，您可以定期对数据库进行备份，当数据库故障或数据损坏时，可以通过备份文件恢复数据库，从而保证数据可靠性。
	禁止使用默认端口	MongoDB的默认端口是27017，使用默认端口容易被监听，存在安全隐患，推荐使用非默认端口。
	补丁升级	DDS支持补丁升级，版本升级涉及新功能添加、问题修复，同时可以提升安全能力、性能水平。
	关闭脚本运行功能	启用javascriptEnabled选项security.javascriptEnabled，可以在mongod服务端运行javascript脚本，存在安全风险,，禁用javascriptEnabled选项，mapreduce、group命令等将无法使用。 如果您的应用中没有mapreduce等操作的需求，为了安全起见，建议关闭javascriptEnabled选项。
	设置秒级监控和告警规则	DDS默认支持对实例进行监控，当监控指标的值超出设置的阈值时就会触发告警，系统会通过SMN自动发送报警通知给云账号联系人，帮助您及时了解DDS实例的运行状况。
	限制最大连接数	如果MongoDB的连接数过高，首先会消耗服务器过多的资源，导致ops（query、insert、update、delete）等反应变慢，同时要根据操作系统环境来设置最大连接数，如果高于操作系统接收的最大线程数，设置无效。通过设置最大连接数，可以避免出现DOS攻击，同时可以用最合理的方式利用系统的资源，达到最佳的OPS响应能力。
	开启数据库审计日志	审计功能可以记录用户对数据库的所有相关操作。通过查看审计日志，您可以对数据库进行安全审计、故障根因分析等操作，提高系统运维效率。
	开启磁盘加密	通过启用磁盘加密，可以提高数据安全性，但对数据库读写性能有少量影响。

华为云安全配置基线—存储

表 6-38 存储风险项检查项

检查子项目		检查项目
对象存储服务 OBS	使用OBS的服务端加密存储对象	启用OBS桶的服务端加密后，用户在上传对象时，数据会在服务端加密成密文后存储。
	合规场景开启WORM功能	OBS提供了合规模式的WORM（Write Once Read Many）功能，即一次写入多次读取，可以确保指定时间内不能覆盖或删除指定对象版本的数据。
	在需要在线预览OBS对象的场景使用自定义域名	基于安全合规要求，华为云对象存储服务 OBS禁止通过OBS的默认域名在线预览桶内对象，即使用上述域名从浏览器访问桶内对象（如视频、图片、网页等）时，不会显示对象内容，而是以附件形式下载；在用户需要在线预览OBS对象的场景，建议使用自定义域名实现。
	禁用匿名访问	OBS桶对于匿名用户禁用对外公开访问的权限，可以防止桶中数据被开放给所有人，保护私有数据不泄露（静态网站等需要对外开放的场景例外）。
	使用OBS的数据临时分享功能来快速分享指定数据	当需要将存放在OBS中对象（文件或文件夹）分享给其他用户时，可以使用OBS的数据临时分享功能，分享的URL可指定有效期，过期自动失效。
	使用双端固定对OBS的资源进行权限控制	设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源，设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问，实现访问控制的双向限定。
	启用多版本控制功能	利用OBS多版本控制功能，可以在一个桶中保留一个对象的多个版本，提升数据异常场景快速恢复能力。
	启用防盗链功能	建议启动OBS提供的防盗链能力，可以防止用户在OBS的数据被其他人盗链。
	使用桶策略限制对OBS桶的访问必须使用HTTPS协议	通过桶策略中的SecureTransport条件限制必须使用HTTPS协议对该桶进行操作，可确保数据上传下载的传输安全。
	避免在私有桶创建公开对象	避免在OBS桶中对匿名用户提供对象的公共读权限，可以防止对象被对外开放给所有人员，防止对象数据泄漏。

检查子项目		检查项目
	启用跨区域复制功能	启用跨区域复制功能，可为用户提供的跨区域数据容灾能力。
弹性文件服务 SFS	确保SFS Turbo文件系统是加密的	SFS Turbo文件系统加密保护您的静态数据。SFS Turbo文件系统加密特性在数据从您的应用写入到SFS Turbo文件系统时自动加密，从SFS Turbo文件系统读取数据时自动解密。
云硬盘 EVS	确保云硬盘是加密的	云硬盘加密保护您的静态数据。云硬盘加密特性在数据从云服务器写入到云硬盘时自动加密，从云硬盘读取数据时自动解密。
云备份 CBR	开启跨区域复制备份功能	开启跨区域复制功能，更安全可靠。
	开启强制备份	开启强制备份，最大限度保障用户数据的安全性和正确性，确保业务安全。
	备份数据删除建议开启二次确认	为防止备份数据误删，建议开启二次确认机制。
	承载备份数据的云硬盘选择加密盘	CBR备份磁盘可选为加密磁盘，成为加密备份。此特性无法手动加密和取消加密备份。

华为云安全配置基线—企业智能

表 6-39 企业智能风险项检查项

检查子项目		检查项目
云数据仓库 DWS	开启集群数据加密功能	DWS可以为集群启用数据库加密，以保护静态数据，避免拖库等安全问题。
	开启DWS数据库审计日志	DWS支持数据库操作审计日志，与管控面的审计互相独立，可以记录数据库内部各个用户的操作记录。 建议按需开启需要记录的操作日志，方便追溯历史数据的操作，保证数据安全。

检查子项目		检查项目
	开启DWS管理控制台审计日志	GaussDB(DWS)通过云审计服务（Cloud Trace Service，CTS）记录GaussDB(DWS)管理控制台的关键操作事件，比如创建集群、创建快照、扩容集群、重启集群等。 记录的日志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。开启后方便进行控制台操作审计及问题定位。
	开启DWS数据库审计日志转储	DWS的数据库审计日志可以记录数据库中的连接和用户活动相关信息。这些审计日志信息有助于监控数据库以确保安全或进行故障排除或定位历史操作记录，默认存储在数据库中。可以将审计日志转储到OBS中，确保审计日志有备份，且更方便用户操作查看审计日志。
	开启DWS三权分立模式	默认情况下，创建GaussDB(DWS)集群时指定的管理员用户属于数据库的系统管理员，能够创建其他用户和查看数据库的审计日志，即权限不分立，三权分立模式为关闭。 为了保护集群数据的安全，GaussDB(DWS)支持对集群设置三权分立，使用不同类型的用户分别控制不同权限的模式。
	开启SSL加密传输功能	SSL协议是安全性更高的协议标准，它们加入了数字签名和数字证书来实现客户端和服务器的双向身份验证，保证了通信双方更加安全的数据传输，建议配置开启。
AI 开发平台 ModelArts	使用IP白名单的方式接入notebook	Notebook实例支持通过SSH方式直接连接，通过keypair方式进行认证。除此之外，对于安全性要求更强的用户，建议配置IP白名单的方式，进一步限制能接入该实例的终端节点。
	对不同的子用户，使用独立的委托	要使用ModelArts的资源，需要得到用户的委托授权。 为了控制各子用户之间权限，建议租户在ModelArts全局配置功能中给各子用户分配委托权限时，分开授权，不要多个子用户共用一个委托凭证。
	使用专属资源池	在使用训练、推理、开发环境时，建议生产环境下使用专属资源池，它在提供独享的计算资源情况下，还可以提供更强更安全的资源隔离能力。

检查子项目		检查项目
	自定义镜像使用非root用户运行	自定义镜像支持自行开发Dockerfile，并推送到SWR。 出于权限控制范围的考虑，建议用户在自定义镜像时，显式定义默认运行的用户为root用户，以降低容器运行时的安全风险。
	开启“严格模式”	使用ModelArts的资源时，需要对不同的子用户分配不同的委托授权，达到最小化授权。
MapReduce 服务 MRS	集群EIP安全组管控	MRS集群支持绑定EIP，绑定EIP后，并开通安全组后，可以使用EIP访问MRS集群Manager管理界面，也可以使用SSH登录到MRS集群节点。因此，需要做好安全组管控，不要将不可信的IP加入到安全组的规则中，允许其访问。此外，需要放通的IP，也要控制端口范围，按需放开，不建议直接放开所有端口。
	管控数分设	MRS集群的常用部署模板“管控合设”、“管控分设”、“数据分设”，为了数据节点和管控节点的隔离，建议使用“管控分设”、“数据分设”方式。
	开启Kerberos认证	MRS集群组件使用Kerberos认证。 Kerberos认证开启时，用户需要通过认证后才可以访问组件对应资源，若不开启Kerberos认证，访问组件将不需要认证和鉴权，会给集群带来风险。

6.2 内置剧本

安全编排根据需求内置了剧本，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 6-40 内置剧本

安全防线	剧本名	描述	数据类
主机安全	主机告警状态同步	自动同步主机告警状态	Alert
	高危漏洞自动通知	对威胁等级为High的漏洞进行邮件或者短信通知	Vulnerability
	攻击链路分析告警通知	针对攻击链路进行分析，如果主机产生告警，就会查看关联主机所属的网站，如果有对应网站信息且有告警，就进行告警通知	Alert
	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
	新增主机资产防护状态通知	新增主机资产为未防护状态，通知客户及时防护	Resource
	HSS高危告警拦截通知	主机高危告警，如果源IP未加入安全组阻断，则通知客户并生成代办，如果人工审核通过则加入安全云脑VPC策略阻断	Alert
	主机Rootkit事件攻击自动化处置	当主机告警类型为Rootkit，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，同时关闭告警	Alert
	主机反弹Shell攻击自动化处置	当主机告警类型为反弹shell，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，同时关闭告警	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

安全防线	剧本名	描述	数据类
	Web登录爆破拦截	对登录爆破成功的IP进行情报验证，如果不在白名单，则进行拦截通知，生成拦截代办，代办人工审核通过后会将该IP加入安全云脑WAF阻断策略中	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
	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
	低危告警自动关闭	对于低危和提示的告警，进行自动化关闭	Alert
	同步CFW黑IP到情报	将CFW的黑IP同步到云脑的情报管理中	CommonContext

安全防线	剧本名	描述	数据类
	同步WAF黑IP到情报	将WAF的黑IP同步到云脑的情报管理中	CommonContext

7 约束与限制

本文介绍安全云脑 SecMaster在使用过程中的约束和限制。

购买

表 7-1 购买

模块	约束与限制
配额数	• 当前账户下所有ECS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。 • 配额数最大限制为10000台。
增值包	• 基础版不支持购买增值包，如需使用增值包功能，请升级为标准版或专业版。 • 增值包不支持单独使用。 – 如果需要购买增值包，请先购买标准版或专业版。 – 如果退订了按需计费的专业版，系统将自动一并退订增值包。 – 如果退订了包周期计费的标准版或专业版，需手动一并退订增值包。
标签	最多支持为安全云脑添加10个标签。

工作空间

表 7-2 工作空间

模块	约束与限制
工作空间（Workspace）	• 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。 • 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。
纳管环境	• 不支持纳管边缘环境：IEC、DEC、IES等边缘站点。 • 仅支持纳管Default项目，不支持纳管子项目。 • 不支持按EPS粒度纳管资源。
空间托管	• 单账号单Region内最多创建1个空间托管视图。 • 一个托管视图可以跨Region管理不同账号下的最多150个工作空间。 • 单账号最多创建10个账号委托。

安全报告

表 7-3 安全报告

模块	约束与限制
安全报告	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）。

告警模型

表 7-4 告警模型

模块	约束与限制
告警模型	• 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。

安全分析

表 7-5 安全分析

模块	约束与限制
查询与分析	● 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。 ● 查询与分析结果保存为指标卡片时，单账号单Workspace最多保存100个。
数据空间	单账号单Region单Workspace最多创建5个数据空间。
数据管道	单账号单Region单数据空间最多创建20个数据管道。

事件、告警、情报、漏洞

表 7-6 安全报告

模块	约束与限制
漏洞	单账号单Workspace内，每天最多新增100个漏洞。
告警	● 单账号单Workspace内，每天最多新增100个告警。 ● 单账号单Workspace内，每天最多可以告警转事件100个。
事件	单账号单Workspace内，每天最多新增100个事件。
情报	单账号单Workspace内，每天最多新增100个情报。

安全编排

表 7-7 安全编排

模块	约束与限制
剧本	单账号单workspace内，单剧本调度频率时间 ≥ 5分钟。

模块	约束与限制
剧本和流程实例	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	● 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。

8 安全

8.1 责任共担

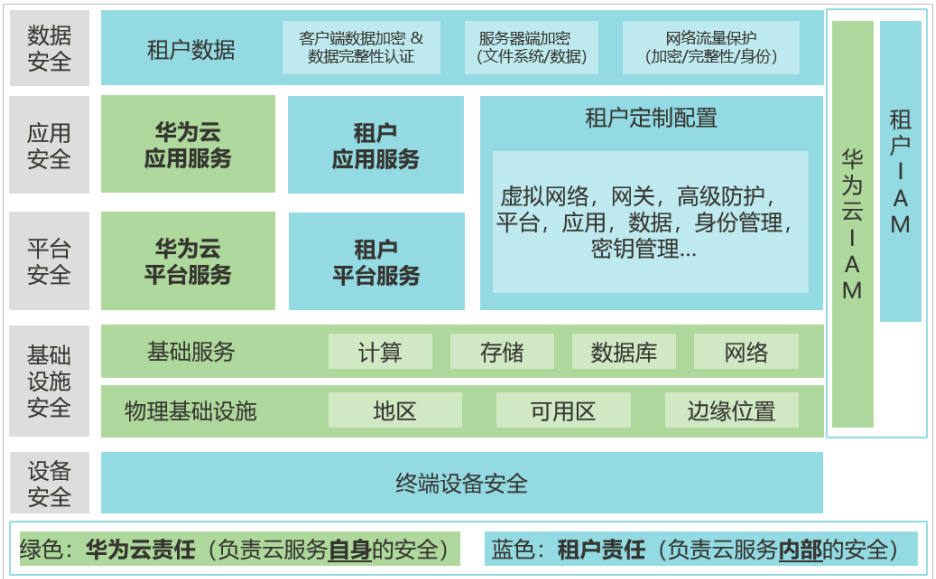
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



8.2 身份认证与访问控制

SecMaster对接了统一身份认证服务（Identity and Access Management，IAM）服务。SecMaster租户身份认证与访问控制通过IAM权限控制。

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助SecMaster服务安全地控制访问权限。

通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对SecMasterr资源的访问范围。SecMaster权限可以通过细粒度定义允许和拒绝的访问操作，以此实现SecMaster资源的权限访问控制。

8.3 数据保护技术

SecMaster通过多种数据保护手段和特性，保证通过SecMaster的数据安全可靠。

表 8-1 SecMaster 的数据保护手段和特性

数据保护手段	简要说明
静态数据保护	SecMaster通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间数据传输进行加密，防止数据在传输过程中泄露或被篡改。用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	1. SecMaster接入云服务告警、漏洞和基线等时，有数据完整性校验。 2. SecMaster核心数据面进程启动时，配置数据执行可靠事件模式确保数据完整性（网络抖动、延迟、配置数据重发&重试等场景）。

数据保护手段	简要说明
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。SecMaster对云服务自动感知并在保留期到期后释放资源。

同时，SecMaster服务充分尊重用户隐私，遵循法律法规，不会采集和存储任何用户隐私数据。更多隐私数据使用和保护问题，请参考**隐私政策声明**。

8.4 审计与日志

- 审计

  云审计服务（Cloud Trace Service，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。

  用户开通云审计服务并创建和配置追踪器后，CTS可记录SecMaster的管理事件和数据事件用于审计。

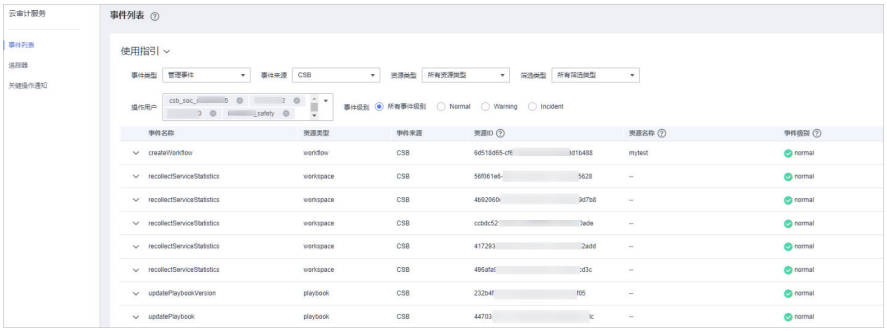
  CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

- 日志
  - 查询

    出于分析或审计等目的，用户开启了云审计服务后，系统开始记录SecMaster资源的操作。云审计服务管理控制台保存最近7天的操作记录。

    关于SecMaster云审计日志的查看，如**图8-2**所示。

    图 8-2 查询日志

8.5 服务韧性

华为云SecMaster当前主要部署在国内，已部署数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其他灾难带来的服务中断，华为云SecMaster提供灾难恢复计划。

当发生故障时，SecMaster的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云SecMaster当前主要部署在国内，并在多个分区部署，同时SecMaster的所有管理面、引擎等组件均采用主备或集群方式部署。

8.6 监控安全风险

SecMaster已对接云监控服务（Cloud Eye，CES），可以通过管理控制台，查看SecMaster的相关运行指标，及时了解SecMaster运行状况。CES服务是华为云为用户提供一个针对各种云上资源的立体化监控平台，用户通过云监控服务可以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。

SecMaster自身作为云上安全运营作战平台，可以接入其他云服务的安全告警，按照告警类型和等级统一维度呈现，可以准确实时监控云上威胁攻击、检测您资产中的安全告警事件；定义威胁告警通知，设置每日定时告警通知和实时告警通知，通过接收消息通知及时了解威胁风险。定义监控的威胁名单、告警类型、告警级别等，选择性呈现关注的威胁告警。帮助用户及时了解安全状况，从而起到预警作用。

CES的详细介绍和开通配置方法，请参见**CES快速入门**。

表 8-2 监控

事件来源	事件名称	事件级别	事件说明	处理建议	事件影响
SYS.SecMaster	独享引擎创建失败	重要	一般是由于底层资源不足等原因导致。	提交工单让运维在后台协调资源再重试。	无法创建独享引擎
SYS.SecMaster	独享引擎运行异常	紧急	一般是由于流量过大或者恶意流程，插件导致。	1. 排查流程，插件执行是否占用资源过多。 2. 查看实例监控，短期内是否实例数量暴增。	无法执行实例
SYS.SecMaster	剧本实例执行失败	一般	一般是由于剧本，流程配置出错导致。	通过实例监控查看失败原因，修改剧本，流程配置。	无
SYS.SecMaster	剧本实例突增	一般	一般是由于剧本，流程配置出错导致。	通过实例监控查看突增原因，修改剧本，流程配置。	无
SYS.SecMaster	日志消息突增	重要	上游服务产生大量日志，导致消息快速增加。	需要排查上游服务业务是否正常。	无
SYS.SecMaster	日志消息突减	重要	上游服务产生日志突然变小。	需要排查上游业务是否正常	无

告警监控相关内容详细操作请参见：

- **漏洞管理**
- **基线检查**
- **安全报告**

8.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 8-3 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看资源中心。

图 8-4 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 8-5 销售许可证&软件著作权证书

8.8 安全编排

SecMaster的安全编排功能可以针对云上安全事件提供安全编排剧本，实现安全事件的高效、自动化响应处置。其主要功能如下：

- 剧本管理：内置自动响应的剧本，支持按需定义扩展。
  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。
- 流程管理：绘制流程图响应剧本触发。
- 资产管理：支持对关键资产、安全资产等进行统一管理呈现。
- 实例管理：支持对运行的实例进行监控管理及记录查看。
- 安全事件自动化响应：对需要处理的安全事件（incidence）以及可疑事件，通过安全编排实现自动化处置及事件调查。

安全编排设置方法请参见**安全编排**。

9 SecMaster 权限管理

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

通过IAM，您可以在账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有安全云脑（SecMaster）的使用权限，但是不希望他们拥有删除SecMaster等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用SecMaster，但是不允许删除SecMaster的权限策略，控制他们对SecMaster资源的使用范围。

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

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账户中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

SecMaster 权限

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

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

权限根据授权精细程度分为角色和策略。

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

如表9-1所示，包括了SecMaster的所有系统权限。

表 9-1 SecMaster 系统权限

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

SecMaster 控制台功能依赖的角色或策略

IAM主账号给IAM子账号授予**区域级**SecMaster FullAccess权限后，在安全云脑控制台使用服务委托授权操作时，还需要给子账号授予IAM创建委托权限、委托授权策略权限，具体说明如下：

表 9-2 SecMaster 控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
服务委托授权	统一身份认证服务 IAM	IAM子账号设置了**区域级**SecMaster FullAccess权限后，需要增加IAM创建委托权限、委托授权策略权限，具体操作请参见**IAM子账号补充授权操作**。

相关介绍

- **IAM产品介绍**
- **创建用户组、用户并授予SecMaster权限**
- **SecMaster自定义策略**
- **SecMaster权限及授权项**

SecMaster FullAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "secmaster:*:*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get",
                "vpcep:endpoints:*"
            ],
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "obs:bucket:ListBucketVersions"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:permissions:checkRoleForAgencyOnDomain",
                "iam:permissions:checkRoleForAgencyOnProject",
                "iam:permissions:checkRoleForAgency",
                "iam:permissions:grantRoleToAgency",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:permissions:grantRoleToAgencyOnProject",
                "iam:policies:*",
                "iam:agencies:*",
                "iam:roles:*",
                "iam:users:listUsers",
                "iam:tokens:assume"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:organizations:get",
                "organizations:delegatedAdministrators:list",
                "organizations:roots:list",
                "organizations:ous:list",
                "organizations:accounts:list"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:cloudServers:list"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "sts:agencies:assume"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "lts:log*:list*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

SecMaster ReadOnlyAccess 策略内容

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "secmaster:*:get*",
                "secmaster:*:list*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get",
                "vpcep:endpoints:get",
```

```
            "vpcep:endpoints:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "obs:bucket:ListBucketVersions"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:checkRoleForAgency",
            "iam:policies:get*",
            "iam:policies:list*",
            "iam:agencies:get*",
            "iam:agencies:list*",
            "iam:roles:get*",
            "iam:roles:list*",
            "iam:users:listUsers"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "organizations:organizations:get",
            "organizations:delegatedAdministrators:list",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:accounts:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "ecs:cloudServers:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "lts:log*:list*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

IAM 子账号补充授权操作

SecMaster部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效。

当给IAM子账号进行区域级项目授权SecMaster FullAccess授权后，由于安全云脑对其他云服务资源有依赖，因此，还需要给IAM子账号进行全局级Action操作授权。具体添加权限如下：

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "iam:roles:listRoles",
```



```
            "iam:agencies:listAgencies",
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:checkRoleForAgency",
            "iam:agencies:createAgency",
            "iam:permissions:grantRoleToAgencyOnDomain",
            "iam:permissions:grantRoleToAgencyOnProject",
            "iam:permissions:grantRoleToAgency"
        ]
    }
  ]
}
```

其中，“iam:permissions:grantRoleToAgencyOnDomain”、“iam:permissions:grantRoleToAgency”、“iam:permissions:grantRoleToAgencyOnProject”、“iam:agencies:createAgency”为使用安全云脑时的**服务委托授权**操作权限，非IAM子账号必选权限，请根据需要进行配置，授权情况说明如下：

- 未授权：仅IAM主账号可进行服务委托授权操作，且IAM子账号进行服务委托授权操作时会出现报错提示。
- 授权：IAM主账号及已授权的IAM子账号均可以进行服务委托授权操作。

10 与其他云服务的关系

本章节主要介绍安全云脑与其他云服务之间的关系。

与安全服务的关系

安全云脑从**主机安全**（Host Security Service，HSS）、**Web应用防火墙**（Web Application Firewall，WAF）、**Anti-DDoS流量清洗**（Anti-DDoS）等安全防护服务中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能AI分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。更多说明请参见**安全云脑与其他安全服务之间的关系与区别**。

与弹性云服务器的关系

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

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS），为SecMaster提供云服务资源的操作记录，记录内容包括从访问管理控制台发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。

CTS记录SecMaster相关操作事件，方便用户日后的查询、审计和回溯。

与云监控服务的关系

云监控（Cloud Eye）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。用户可以通过事件及时了解安全云脑的状况，并及时收到异常报警做出反应，保证业务顺畅运行。具体请参见《云监控服务用户指南》。

与标签管理服务的关系

标签管理服务（Tag Management Service，简称TMS）是一种快速便捷将标签集中管理的可视化服务，方便用户通过标签标识管理工作空间实例。

表 10-1 标签管理服务支持的 SecMaster 操作列表

操作名称	资源类型	事件名称
查询资源实例列表	Workspace	listResourceInstance
查询资源实例数量	Workspace	countResourceInstance
批量查询资源标签	Tag	batchTagResources
批量删除资源标签	Tag	batchUntagResources
查询项目标签	Tag	listProjectTag
更新标签值	Tag	updateTagValue
查询资源标签	Tag	listResourceTag

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

安全云脑支持企业管理，您可以将安全云脑上的资源按照企业项目进行管理，并设置每个企业项目的用户权限。

11 基本概念

11.1 安全运营中心

安全运营中心（Security Operations Center，SOC）一个集中式功能或团队，负责全天候检测端点、服务器、数据库、网络应用程序、网站和其他系统的所有活动，以实时发现潜在的威胁；对网络安全事件进行预防、分析和响应，以改进企业的网络安全态势。SOC还使用最新的威胁情报来掌握威胁组和基础结构的最新信息，并在攻击者利用系统或流程漏洞之前识别和处理这些漏洞，从而主动开展安全工作。大多数SOC每周7天全天候运行，跨多个国家/地区的大型企业/组织可能还依赖于全球安全运营中心（GSOC）来掌控全球安全威胁，并协调多个本地SOC之间的检测和响应。

SOC 的功能

SOC团队承担以下职能来帮助防止、响应攻击并在遭到攻击后恢复。

- **资产和工具清单**

  为了消除覆盖范围中的盲点和缺口，SOC需要了解它保护的资产，并深入了解它用于保护企业/组织的工具。这意味着考虑到本地和多个云中的所有数据库、云服务、标识、应用程序和客户端。该团队还跟踪企业/组织中使用的所有安全解决方案，例如防火墙、反恶意软件、反勒索软件和监视软件。

- **减少攻击面**

  SOC的主要责任是减少企业/组织的攻击面。为此，SOC会维护包含所有工作负载和资产的清单、将安全修补程序应用于软件和防火墙、识别错误配置，并新资产联机时添加这些资产。团队成员还负责研究新出现的威胁并分析风险，这有助于他们领先于最新威胁。

- **持续监视**

  SOC团队使用安全分析解决方案全天候监视整个环境 - 本地、云、应用程序、网络和设备，来发现异常或可疑行为；其中这些解决方案包括安全信息企业管理（SIEM）解决方案、安全编排、自动化和响应（SOAR）解决方案和扩展检测和响应（XDR）解决方案。这些工具会收集遥测数据、聚合数据，并在某些情况下自动进行事件响应。

- **威胁情报**

  SOC还使用数据分析、外部源和产品威胁报告来深入了解攻击者行为、基础结构和动机。这种情报提供了有关Internet上正在发生的情况的全局视图，并帮助团队

了解威胁组是如何运作的。借助此信息，SOC可快速发现威胁，并加强企业/组织对新出现的风险的应对。

- **威胁检测**

  SOC团队使用SIEM和XDR解决方案生成的数据来识别威胁。这首先会从实际问题中筛选掉误报。然后，他们按严重性和对业务的潜在影响确定威胁的优先级。

- **日志管理**

  SOC还负责收集、维护和分析每个客户端、操作系统、虚拟机、本地应用和网络事件生成的日志数据。分析有助于建立正常活动的基线，并揭示可能指示恶意软件、勒索软件或病毒的异常。

- **事件响应**

  识别到网络攻击后，SOC会快速采取措施，在尽可能减少业务中断的情况下限制对企业/组织的损害。措施可能包括关闭或隔离受影响的客户端和应用程序、暂停被入侵的账户、移除遭到感染的文件，以及运行防病毒和反恶意软件。

- **发现和修正**

  在攻击之后，SOC负责将公司恢复到其原始状态。团队将擦除并重新连接磁盘、标识、电子邮件和客户端，重启应用程序，直接转换到备份系统，并恢复数据。

- **根本原因调查**

  为了防止类似的攻击再次发生，SOC进行了彻底的调查，来确定漏洞、效果不佳的安全流程和其他导致事件的教训。

- **安全性优化**

  SOC使用事件期间收集的任何情报来解决漏洞、改进流程和策略，并更新安全路线图。

- **合规性管理**

  SOC职责的一个关键部分是确保应用程序、安全工具和流程符合隐私法规，例如，《PCI DSS安全遵从包》、《ISO 27701安全遵从包》和《ISO 27001安全遵从包》等。团队定期审核系统来确保合规性，并确保在数据泄露后通知监管机构、执法人员和客户。

SOC 中的关键角色

根据企业/组织的规模，典型的SOC包括以下角色：

- **事件响应总监**

  此角色通常只出现在非常大型的企业/组织中，负责协调安全事件期间的检测、分析、遏制和恢复。他们还管理与相应利益干系人的沟通。

- **SOC管理者**

  SOC监督员是管理者，通常向首席信息安全官（CISO）报告。职责包括监督人员、运行业务、培训新员工和管理财务。

- **安全工程师**

  安全工程师负责企业/组织安全系统的启动和运行。这包括设计安全体系结构以及研究、实施和维护安全解决方案。

- **安全分析师**

  安全分析师是安全事件中的第一响应人，负责识别威胁、确定威胁的优先级，然后采取行动来遏制损害。在遭到网络攻击期间，他们可能需要隔离已遭到感染的主机、客户端或用户。在一些企业/组织中，会根据安全分析师负责解决的威胁的安全程度来对这些分析师进行分级。

- **威胁搜寻者**

  在一些企业/组织中，经验最丰富的安全分析师被称为威胁搜寻者。他们识别和响应自动工具未检测到的高级威胁。该角色主动行动，旨在加深企业/组织对已知威胁的了解，并在攻击发生之前揭示未知的威胁。

- **取证分析师**

  大型企业/组织可能还会聘用取证分析师，他们负责在出现违规后收集情报来确定其根本原因。他们会搜寻系统漏洞、违反安全策略的行为和网络攻击模式，这些有可能帮助防止将来发生类似的入侵。

SOC 的类型

企业/组织有几种不同的方式来设置其SOC。一些企业/组织选择构建具有全职员工的专用SOC。这种类型的SOC可以是内部的，具有物理的本地位置，也可以是虚拟的，员工使用数字工具远程协调工作。许多虚拟SOC既有合同工，也有全职员工。外包SOC也可称为“托管SOC”或“安全运营中心即服务”，它由托管安全服务提供商运行，该提供商负责防止、检测、调查和响应威胁。此外，它可以既有内部员工，也有托管安全服务提供商。这种版本被称为托管或混合SOC。企业/组织使用这种方法来增加自身员工的影响力。例如，如果他们没有威胁调查员，那么聘用第三方可能与在内部配备这些人员更加容易。

SOC 团队的重要性

强大的SOC可帮助企业、政府和其他组织领先于不断变化的网络威胁环境。这不是一件容易的事。攻击者和防御社区都经常开发新的技术和战略，而管理所有的变化需要时间和精力。SOC利用其对更广泛的网络安全环境的了解以及对内部薄弱点和业务优先级的理解，帮助企业/组织制定符合业务长期需求的安全路线图。SOC还可限制发生攻击时对业务的影响。他们会持续监视网络并分析警报数据，因此与分散在其他几个优先事项的团队相比，他们更有可能更早地发现威胁。通过定期培训和记录良好的流程，SOC可以快速处理当前事件，即使在压力极大的情况下也能做到。对于没有全天候关注安全运营的团队来说，这可能很困难。

SOC 的优势

通过将用于保护企业/组织免受威胁影响的人员、工具和流程进行统一，SOC可帮助企业/组织更有效、更高效地防御攻击和泄露。

- **强大的安全状况**

  提高企业/组织的安全性是一项永无止境的工作。它需要持续监视、分析和规划，以发现漏洞并掌握不断变化的技术。当有待处理事项的优先级不相上下时，很容易会忽视安全性，而关注感觉更紧迫的任务。

  集中式SOC有助于确保持续改进流程和技术，从而减低成功攻击带来的风险。

- **遵守隐私法规**

  行业、国家和地区在治理数据收集、存储和使用方面的法规各有不同。许多法规要求企业/组织在使用者请求时报告数据泄露并检测个人数据。制定适当的流程和程序与拥有适当的技术同样重要。SOC的成员帮助企业/组织承担保持技术和数据流程最新的责任来遵守这些法规。

- **快速响应事件**

  发现和阻止网络攻击的速度有多快至关重要。借助适当的工具、人员和情报，可以在漏洞造成任何损害之前遏止这些漏洞。但是，恶意操作者也很聪明，他们会隐藏起来、窃取大量数据，并在任何人注意到之前提升他们的权限。安全事件也是一个让人非常有压力的事情，尤其是对于在事件响应方面缺乏经验的人来说。

借助统一的威胁情报和记录良好的程序，SOC团队能够快速检测、响应攻击，并在遭到攻击后快速恢复。

- **降低入侵成本**

  对于企业/组织来说，一次成功的入侵可能会付出非常昂贵的代价。恢复通常需要停机很长时间，很多企业在事件发生后不久会失去客户或难以赢得新客户。通过先于攻击者行动并快速响应，SOC可帮助企业/组织在重回正常运营时节省时间和金钱。

SOC 团队的最佳做法

要负责的事情太多，SOC必须有效地企业/组织和管理才能取得结果。拥有强大SOC的企业/组织会实施以下安全做法：

- **策略与业务看齐**

  即使资金最充裕的SOC也必须决定将时间和金钱集中在哪些方面。企业/组织通常会先进行风险评估，来识别最容易出现风险的方面和最大的业务机会。这有助于确定需要保护哪些内容。SOC还需要了解资产所在的环境。很多企业的环境很复杂，一些数据和应用程序在本地，一些跨多个云分布。策略有助于确定安全专业人员是否需要每天任何时间都可联系，以及是在内部配置SOC还是使用专业服务更好。

- **员工具备能力、经过良好培训**

  有效SOC的关键在于高技能且不断进步的员工。首先是要找到最优秀的人才，但由于安全人员市场竞争非常激烈，因此这可能很棘手。为了避免技能差距，许多企业/组织试着寻找拥有各种专业知识的人员，这些知识包括系统和情报监视、警报管理、事件检测和分析、威胁搜寻、道德黑客、网络取证和逆向工程。他们还会部署可自动执行任务的技术，让较小型的团队更加高效，并提高初级分析员的产出。在定期培训方面投入有助于企业/组织留住关键员工、弥补技能差距和发展员工的职业生涯。

- **端到端可见性**

  攻击可能从单个客户端开始，因此SOC了解企业/组织的整个环境至关重要，这包括由第三方管理的任何内容。

- **适当的工具**

  安全事件是如此的多，团队很容易不知所措。有效SOC会在卓越安全工具上投入，这些工具可很好地协同工作，并使用 AI 和自动化来上报重大风险。互操作性是避免覆盖范围出现缺口的关键。

SOC 工具与技术

- **安全信息和事件管理（SIEM）**

  SOC中最重要的工具之一是基于云的SIEM解决方案，它将来自多个安全解决方案和日志文件的数据聚合在一起。借助威胁情报和AI，这些工具帮助SOC检测不断演化的威胁、加快事件响应速度并先于攻击者行动。

- **安全编排、自动化和响应（Security Orchestration, Automation and Response，SOAR）**

  SOAR可自动执行定期和可预测的扩充、响应和修正任务，从而空出时间和资源来进行更深入的调查和搜寻。

- **扩展检测和响应（Extended Detection and Response，XDR）**

  XDR是一种服务型软件工具，它通过将安全产品和数据集成到简化的解决方案中来提供全面、更优的安全性。企业/组织使用这些解决方案在多云混合环境中主动

有效地应对不断演化的威胁环境和复杂的安全挑战。与终结点检测和响应（EDR）等系统相比，XDR扩大了安全范围，从而跨更广泛的产品集成了保护，包括企业/组织的终结点、服务器、云应用程序和电子邮件等。在此基础中，XDR将预防、检测、调查和响应相结合，提供可见性、分析、相关事件警报和自动化响应来增强数据安全并对抗威胁。

- **防火墙**

  防火墙会监视进出网络的流量，根据SOC定义的安全规则允许或阻止流量。

- **日志管理**

  日志管理解决方案通常是SIEM的一部分，它会记录来自企业/组织中运行的每个软件、硬件和客户端的所有警报。这些日志提供了网络活动的相关信息。

- **漏洞管理**

  漏洞管理工具会扫描网络来帮助识别攻击者可能利用的任何薄弱点。

- **用户和实体行为分析（User and Entity Behavior Analytics，UEBA）**

  用户和实体行为分析构建在许多新式安全工具之中，它使用AI来分析从各种设备收集的数据，来为每个用户和实体建立正常活动的基线。当事件偏离基线时，会标记该事件供进一步分析。

SOC 和 SIEM

如果没有SIEM，SOC将很难完成其任务。新式SIEM提供：

- 日志聚合：SIEM会收集日志数据并关联警报，分析人员可使用这些信息来检测和搜寻威胁。
- 上下文：SIEM跨组织中的所有技术收集数据，所以它帮助将单个事件之间的点连接起来，识别复杂的攻击。
- 减少警报数：SIEM使用分析和AI来关联警报并识别最严重的事件，从而减少用户需要审查和分析的事件数。
- 自动响应：内置规则使SIEM能够识别和阻止可能的威胁，无需人员交互。

说明

另请务必注意，单靠SIEM不足以保护组织。用户需要将SIEM与其他系统集成，为基于规则的检测定义参数，并评估警报。正因为如此，定义SOC策略和聘用适当的员工至关重要。

SOC 解决方案

有多种解决方案可用来帮助SOC保护组织。最佳解决方案协同工作，跨本地和多个云提供完整覆盖范围。华为云安全提供全面的解决方案，来帮助SOC消除覆盖范围方面的差距，并获得其环境的360度视图。安全云脑检测和响应解决方案集成，为分析师和威胁搜寻者提供查找和遏止网络攻击所需的数据。

常见问题

1. 安全运营中心团队要做什么？

   SOC团队监视服务器、设备、数据库、网络应用程序、网站和其他系统，以实时发现潜在威胁。他们还及时了解最新威胁并在攻击者利用系统或进程漏洞之前发现和解决这些漏洞，以执行主动安全工作。如果企业/组织已然遭受到攻击，SOC团队负责根据需要去除威胁以及还原系统和备份。

2. 安全运营中心的关键组件是什么？

SOC由有助于保护组织免受网络攻击的人员、工具和流程组成。为了实现其目标，它执行以下功能：清点所有资产和技术、日常维护和准备、持续监视、威胁检测、威胁情报、日志管理、事件响应、恢复和修正、根本原因调查、安全优化和合规性管理。

3. 为什么企业/组织需要强大的SOC?

   强大的SOC通过统一防御、威胁检测工具和安全流程来帮助企业/组织更高效和有效地管理安全性。与没有SOC的公司相比，具有SOC的企业/组织能够改进其安全流程、更快地应对威胁以及更好地管理合规性。

4. SIEM和SOC有什么区别?

   SOC是负责保护企业/组织免受网络攻击的人员、流程和工具。SIEM是SOC用于保持可见性和响应攻击的众多工具之一。SIEM汇总日志文件，并使用分析和自动化向决定响应方式的SOC成员揭示可信威胁。

11.2 总览和态势总览

安全风险

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

安全评分

安全云脑实时呈现您云上资产的整体安全评估状况，并根据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。

如下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 11-1 安全分值表

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

- 安全评分扣分项

  安全评分扣分项及其分值情况如下所示：

表 11-2 安全评分扣分项

分类	扣分项	单项扣分值	处理建议	最高扣分上限
安全服务启用	未开启安全相关服务	不扣分	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		

分类	扣分项	单项扣分值	处理建议	最高扣分上限
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		

11.3 工作空间

工作空间

工作空间（Workspace）属于安全云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和Region，可支撑不同场景下的工作空间运营模式。

数据空间

数据空间是进行数据分组、负载、流控单元。同一数据空间的数据共享同一负载均衡策略。

数据管道

数据传输消息主题和存储索引组合为数据管道。

11.4 告警管理

威胁告警

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

事件

事件是一个广泛的概念，可以包括告警，但不限于此，它可以是系统正常操作的一部分，也可以是异常或错误。在运维和安全领域，事件通常指的是已经发生并需要被关注、调查和处理的问题或故障。事件可能由一条或多条告警触发，也可能由其他因素（如用户操作、系统日志等）引发。

事件的目的是为了记录、分析、报告或审计，通常用于记录和报告系统的历史行为，以便于分析和审计。

告警

告警是运维中的一种异常信号的通知，通常是由监控系统或安全设备在检测到系统或网络中的异常情况时自动生成的。例如，当服务器的CPU使用率超过90%时，系统可能会发出告警。这些异常情况可能包括系统故障、安全威胁或性能瓶颈等。

告警通常有明确的指示性，能够明确指出异常发生的位置、类型和影响。同时，告警可以按照严重程度来进行分类，如紧急、重要、一般等，以便运维人员根据告警的严重程度来决定哪些需要优先处理。

告警的目的是及时通知相关人员，以便他们能够迅速响应并采取措施解决问题。

当安全云脑检测到的云资源中存在的异常情况（例如，某个恶意IP对资产攻击、资产已被入侵等）时，将以告警的形式将威胁信息展示在安全云脑告警管理界面中。

11.5 安全编排

分类和映射

分类和映射是指对云服务告警进行类型匹配和字段映射。

安全编排

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

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

剧本

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。

流程

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。

剧本和流程的关系

- 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。

插件管理

- 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。

资产连接

资产连接是安全编排流程中，每个插件节点需要使用到的连接域名和鉴权参数。用于在安全编排的流程执行过程中，每个插件节点运行时，传入需要连接的域名信息，以及在访问该域名时，需要使用到的用户鉴权信息，如用户名/密码、账号AK/SK等。

资产连接与插件的关系

每个插件在运行过程中，需要通过域名调用的方式访问其他云服务或者三方服务，调用过程中需要鉴权，因此，在插件的登录凭证参数中会定义需要的域名参数（Endpoint）和认证参数（用户名/密码、账号AK/SK等）。资产连接则是配置插件登录凭证的参数值，流程中每个插件节点绑定不同的资产连接，支持相同插件的不同节点访问不同的服务。

实例监控

当剧本/流程执行完成后，实例管理列表中会生成剧本/流程实例，即实例监控。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。

11.6 安全分析

生产者

是用来构建并传输数据到服务端的逻辑概念，负责把数据放入消息队列。

订阅器

用于订阅安全云脑管道消息，一个管道可由多个订阅器进行订阅，安全云脑通过订阅器进行消息分发。

消费者

是用来接收并处理数据的运行实体，负责通过订阅器把安全云脑管道中的消息进行消费并处理。

消息队列

是数据存储和传输的实际容器。

威胁检测模型

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