

安全云脑

# 产品介绍

文档版本 11  
发布日期 2026-05-15



版权所有 © 华为云计算技术有限公司 2026。保留一切权利。

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

## 商标声明



HUAWEI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

<b>1 什么是安全云脑</b>	<b>1</b>
<b>2 产品优势</b>	<b>2</b>
<b>3 应用场景</b>	<b>3</b>
<b>4 服务版本差异</b>	<b>5</b>
<b>5 产品功能</b>	<b>10</b>
<b>6 个人数据保护机制</b>	<b>20</b>
<b>7 经验包</b>	<b>22</b>
7.1 内置检查项	22
7.2 内置剧本	159
7.3 内置类型	162
<b>8 约束与限制</b>	<b>208</b>
<b>9 安全</b>	<b>212</b>
9.1 身份认证与访问控制	212
9.2 数据保护技术	212
9.3 审计与日志	213
9.4 服务韧性	213
9.5 监控安全风险	214
9.6 认证证书	214
9.7 安全编排	216
<b>10 权限管理</b>	<b>217</b>
<b>11 与其他云服务的关系</b>	<b>224</b>
<b>12 基本概念</b>	<b>226</b>
12.1 安全运营中心	226
12.2 总览和态势总览	231
12.3 工作空间	233
12.4 告警管理	234
12.5 安全编排	238
12.6 安全分析	239

# 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。

## 介绍视频

## 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

您可以通过态势感知即时查看大屏、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

## 日志审计场景

### 场景说明

安全监管趋严，合规要求越来越高，各地隐私保护遵从要求、数据安全、网络安全法等法规条例多且解读难。通过安全云脑基线检查、日志审计等功能，确保企业在满足国家行业监管要求的同时，能帮助企业明确安全目标，系统化进行信息系统安全建设，降低安全隐患及被攻击的风险。

### 解决方案

安全云脑提供的基线检查、日志审计等功能，可以帮助客户有效检查是否满足等级保护合规要求，同时接入安全云脑的数据支持存储180天满足等保审计对保留时长的要求。

### 推荐版本

标准版

## 威胁检测与响应场景

### 场景说明

云上威胁可能通过多种手段进入企业云上资产如网络入侵、主机入侵等，为防御和检测威胁，主机安全、云防火墙、Web 应用防火墙往往是企业上云的必然选择，但也带来诸多问题：如告警众多并且管理分散、处置和封禁入口多样、无法有效进行处置等。以上问题导致系统安全薄弱点多，运维难度大，威胁管理效率低，安全风险高。

### 解决方案

安全云脑提供威胁管理和安全编排功能可有效帮助用户解决以上问题。威胁管理将以安全云脑为核心平台，采集并整合分析企业主机安全 HSS、云防火墙 CFW、Web应用防火墙 WAF各类告警与日志，对告警进行集中分析。同时依靠云原生能力，安全云脑整合了主机安全、云防火墙、Web 应用防火墙、安全组等各类产品的处置与封禁能力，可以为 enterprise 客户提供集中处置、一键处置、自动处置，极大的提升威胁响应效率。

- 百万告警降噪99%，降低合法事件的干扰，同时不漏报。
- 开箱即用，预置200+模型、30+安全剧本，实时流分析，秒级检测，秒级响应。
- 支持自定义告警模型、研判/处置剧本，以适配客户的安全需求。

### 推荐版本

专业版

## 云上云下统一管理

### 场景说明

针对多账号、多云的用户，安全数据、处置平台分散，缺乏统一安全运营标准；海量安全日志，事件依赖人工研判，威胁事件以及告警处置效率低；多平台数据难以关联，经验沉淀难。

### 解决方案

- 安全云脑的资产管理功能，支持管理云上和云外资产，可以查看资源的安全状态统计信息，帮助您快速定位安全风险问题。
- 安全云脑支持一键接入WAF、HSS、CFW等多种云产品的日志数据。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。
- 安全云脑空间托管，支持跨账号、跨Region统一安全运营。
- 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。
- 安全云脑提供威胁管理、安全编排功能，帮助企业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。

### 推荐版本

专业版

# 4 服务版本差异

安全云脑提供基础版、标准版、专业版供您使用。

表 4-1 版本说明

版本	计费模式	版本说明
基础版	<ul style="list-style-type: none"><li>包周期</li></ul>	<ul style="list-style-type: none"><li>了解安全云脑。提供安全总览及原始告警汇聚，了解基本态势感知信息。</li></ul> 不同服务版本支持的功能请参见 <a href="#">不同服务版本支持的功能特性</a> ，详细的功能说明请参见 <a href="#">产品功能</a> 。
标准版	<ul style="list-style-type: none"><li>包周期</li></ul>	提供态势感知信息、对原始告警汇聚及智能分析等能力，满足日志审计等安全合规要求。 <ul style="list-style-type: none"><li>提供基线检查、日志审计等功能，可以帮助客户有效检查是否满足等级保护合规要求。</li><li>接入安全云脑的数据支持存储180天满足等保审计对保留时长的要求。</li></ul> 不同服务版本支持的功能请参见 <a href="#">不同服务版本支持的功能特性</a> ，详细的功能说明请参见 <a href="#">产品功能</a> 。
专业版	<ul style="list-style-type: none"><li>按需</li><li>包周期</li><li>按需转包周期</li></ul>	提供态势感知信息，专业运营报告、预置安全模型及剧本，威胁检测模型告警，智能分析、安全编排及全量日志审计，满足企业日常安全运营、合规检查要求。 <ul style="list-style-type: none"><li>支持云上云下统一管理，支持跨账号、跨Region统一安全运营。</li><li>安全云脑提供威胁管理和安全编排功能，威胁运营将以安全云脑为核心平台，采集并整合分析企业主机安全 HSS、云防火墙 CFW、Web应用防火墙 WAF各类告警与日志，对告警进行集中分析。同时整合各类产品的处置与封禁能力，可以为企业客户提供集中处置、一键处置、自动处置，极大的提升威胁响应效率。</li></ul> 不同服务版本支持的功能请参见 <a href="#">不同服务版本支持的功能特性</a> ，详细的功能说明请参见 <a href="#">产品功能</a> 。

## 不同服务版本支持的功能特性

表 4-2 不同服务版本支持的功能特性

一级功能	子功能	基础版	标准版	专业版
版本说明		提供安全总览及原始告警汇聚，了解基本安全态势信息。	提供态势感知信息、对原始告警汇聚及智能分析等能力，满足日志审计等安全合规要求。	提供态势感知信息，专业运营报告、预置安全模型及剧本，威胁检测模型告警，智能分析、安全编排及全量日志审计，满足企业日常安全运营、合规检查要求。
态势感知	总览	支持	支持	支持
	态势总览	支持	支持	支持
	安全报告	--	--	支持 支持专业的安全日报、安全周报、安全月报； 支持自定义创建安全报告；
	资产管理	支持	支持	支持
	已购资源	支持	支持	支持
	策略管理	支持	支持	支持
	基线检查	支持	支持	支持
	漏洞管理	支持	支持	支持
	安全大屏	--	支持	支持
风险预防	应急漏洞公告	支持	支持	支持

一级功能	子功能	基础版	标准版	专业版
版本说明		提供安全总览及原始告警汇聚，了解基本安全态势信息。	提供态势感知信息、对原始告警汇聚及智能分析等能力，满足日志审计等安全合规要求。	提供态势感知信息，专业运营报告、预置安全模型及剧本，威胁检测模型告警，智能分析、安全编排及全量日志审计，满足企业日常安全运营、合规检查要求。
威胁管理	事件管理	--	支持	支持
	告警管理	支持 支持各安全服务原始告警汇聚； 具体支持的日志类型如下： <ul style="list-style-type: none"> <li>主机安全基线 hss-baseline</li> <li>安全云脑基线 secmaster-baseline</li> </ul>	支持 支持各安全服务原始告警汇聚； 具体支持的日志类型如下： <ul style="list-style-type: none"> <li>主机安全基线 hss-baseline</li> <li>安全云脑基线 secmaster-baseline</li> <li>MTD告警日志 mtd-alarm</li> <li>主机安全告警 hss-alarm</li> <li>主机漏洞扫描结果 hss-vul</li> </ul> <b>说明</b> 仅支持威胁检测服务（MTD）的region才可支持接入MTD告警日志 mtd-alarm，其中支持威胁检测服务（MTD）的region请参见 <a href="#">支持接入的云服务日志</a>	支持 支持各安全服务原始告警汇聚； 支持威胁检测模型告警； 支持覆盖MITRE矩阵； 具体支持的日志类型如下： <ul style="list-style-type: none"> <li>主机安全基线 hss-baseline</li> <li>安全云脑基线 secmaster-baseline</li> <li>MTD告警日志 mtd-alarm</li> <li>主机安全告警 hss-alarm</li> <li>主机漏洞扫描结果 hss-vul</li> </ul> <b>说明</b> 仅支持威胁检测服务（MTD）的region才可支持接入MTD告警日志 mtd-alarm，其中支持威胁检测服务（MTD）的region请参见 <a href="#">支持接入的云服务日志</a>
	情报管理	--	--	支持

一级功能	子功能	基础版	标准版	专业版
版本说明		提供安全总览及原始告警汇聚，了解基本安全态势信息。	提供态势感知信息、对原始告警汇聚及智能分析等能力，满足日志审计等安全合规要求。	提供态势感知信息，专业运营报告、预置安全模型及剧本，威胁检测模型告警，智能分析、安全编排及全量日志审计，满足企业日常安全运营、合规检查要求。
	智能建模	--	--	支持 计算模型数据120 MB/天/配额； 预置模型200个； 预置剧本30个；
安全编排	运营对象	--	--	支持
	安全编排	--	--	支持 赠送规格：操作7000次
	页面布局	--	--	支持
	插件管理	--	--	支持
	目录定制	--	支持	支持
数据采集	数据采集	--	支持	支持
数据集成	数据集成	--	支持 仅支持集成云服务告警	支持
日审总览	日审总览	支持	支持	支持

一级功能	子功能	基础版	标准版	专业版
版本说明		提供安全总览及原始告警汇聚，了解基本安全态势信息。	提供态势感知信息、对原始告警汇聚及智能分析等能力，满足日志审计等安全合规要求。	提供态势感知信息，专业运营报告、预置安全模型及剧本，威胁检测模型告警，智能分析、安全编排及全量日志审计，满足企业日常安全运营、合规检查要求。
	安全数据	--	支持 安全数据采集赠送规格：120 MB/天/配额； 安全数据保留赠送规格：120 MB/天/配额； 安全数据导出赠送规格：120 MB/天/配额； 平台安全数据赠送规格：40 MB/天/配额；	支持 安全数据采集赠送规格：120 MB/天/配额； 安全数据保留赠送规格：120 MB/天/配额； 安全数据导出赠送规格：120 MB/天/配额； 平台安全数据赠送规格：40 MB/天/配额； 安全建模分析赠送规格：120 MB/天/配额；
多账号管理	多账号管理	--	--	支持
工作台	工作台管理	支持	支持	支持
	账号风控工作台	支持 仅支持AK&SK泄露、基线风险模块	支持 仅支持AK&SK泄露、基线风险模块	支持
	大模型安全工作台	--	--	支持

# 5 产品功能

安全云脑基于云原生安全，提供全面的日志采集、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 5-1 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	<ul style="list-style-type: none"><li>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。</li><li>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。</li><li>安全趋势：呈现最近7天整体资产安全健康得分的趋势图。</li></ul>	√	√	√

## 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 5-2 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	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>	√	√	√

## 多账号管理

安全云脑支持将多个云账号集合到一个账号内，对多个云账号资源进行统一安全管理、安全防护配置及数据运营监控，并实时检测各个成员账号的安全风险状况，实现多账号快捷运营。

表 5-3 多账号管理功能说明

功能模块	功能描述	基础版	标准版	专业版
多账号管理	<p>随着企业上云的广泛应用，越来越多的企业将业务迁移至云端，云端的资源、项目、人员、权限管理变得极其复杂。企业用户对于跨账号的云资源具有集中化管理需求，</p> <p>安全云脑支持将多个云账号集合到一个账号内，对多个云账号资源进行统一安全管理、安全防护配置及数据运营监控，并实时检测各个成员账号的安全风险状况，实现多账号快捷运营。</p>	×	×	√

## 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 5-4 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。	√	√	√

## 工作台

工作台是基于安全服务标准API，支持灵活拖拽快速构建管理界面，统一七层防线入口，并为AI-SPM（云安全态势感知管理）、账号风控等细分场景提供专项运营入口，实现安全云脑工作台框架全生命周期管理。

表 5-5 工作台功能说明

功能模块	功能描述	基础版	标准版	专业版
工作台管理	<p>支持管理已有工作台。</p> <ul style="list-style-type: none"><li>● <b>系统工作台</b>：安全云脑内置到系统的工作台即“账号风控工作台”、“大模型安全工作台”。</li><li>- <b>账号风控工作台</b>：账号风控工作台针对身份安全风险问题，通过<b>AK&amp;SK泄露</b>、资源类型为“账号”、“IAM”、“委托”的<b>基线风险</b>、<b>告警风险</b>三大模块，呈现身份安全风险的总体态势，帮助用户快速识别风险。</li><li>- <b>大模型安全工作台</b>：大模型安全工作台实时为您呈现大模型合规态势，支持大模型的数据语料风险运营、推理业务风险运营和环境安全风险运营，实时为您呈现<b>推理安全</b>、<b>语料安全</b>、<b>环境安全</b>的风险态势，助您识别大模型风险和潜在威胁。</li></ul>	仅支持账号风控工作台	仅支持账号风控工作台	√

功能模块	功能描述	基础版	标准版	专业版
账号风控工作台	<p>账号风控工作台针对身份安全风险问题，通过AK&amp;SK泄露、基线风险、告警风险三大模块，呈现身份安全风险总体态势，帮助用户关注身份安全风险问题。</p> <ul style="list-style-type: none"> <li>异常AccessKey泄露：统计数据泄露AK-SK风险类型的攻击，数据来源于“告警管理”中属于数据泄露AK-SK风险类型的攻击列表。</li> <li>基线风险：统计“资源类型”为“账号”、“IAM”、“委托”的<b>基线风险</b>。</li> <li>告警风险：统计“告警管理”中的身份防线的告警类型或攻击类型分布、以及身份防线告警转成的未处理的事件、以及CTS日志中的来访IP日志统计数量分布等信息。</li> </ul>	<ul style="list-style-type: none"> <li>仅支持异常AccessKey泄露模块。</li> <li>“基线风险”和“告警风险”模块的数据依赖开通安全云脑专业版。基础版因</li> </ul>	<ul style="list-style-type: none"> <li>仅支持异常AccessKey泄露模块。</li> <li>“基线风险”和“告警风险”模块的数据依赖开通安全云脑专业版。标准版因</li> </ul>	√

功能模块	功能描述	基础版	标准版	专业版
		版本过低可能无数据或数据不完整。	版本过低可能无数据或数据不完整。	
大模型安全工作台	<p>大模型安全工作台实时为您呈现大模型合规态势，支持大模型的数据语料风险运营、推理业务风险运营和环境安全风险运营，实时呈现大模型的风险概览，助您识别大模型风险和潜在威胁。“大模型安全工作台”为您呈现<b>推理安全、语料安全、环境安全</b>的风险态势。</p> <ul style="list-style-type: none"> <li>推理安全：基于WAF攻击日志和访问日志，分析呈现大模型接口的调用请求次数、调用请求命中防护策略数、以及命中防护策略数排名前5的推理模型域名和数量、提示词注入的攻击分布、推理模型攻击类型分布等。</li> <li>语料安全：基于DSC告警日志，分析呈现大模型中的语料风险类别和数量、TOP5语料风险资产分布等。</li> <li>环境安全：基于安全云脑基线检查、漏洞管理、告警管理功能，分析呈现当前工作空间的TOP5合规检查风险、TOP5漏洞风险、TOP5告警和最近攻击列表。</li> </ul>	×	×	√

## 态势感知

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

表 5-6 态势感知功能介绍

功能模块	功能描述	基础版	标准版	专业版
<b>态势总览</b>	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>安全趋势：呈现最近7天整体资产安全健康得分的趋势图。</li> </ul>	√	√	√
<b>安全大屏</b>	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。 <b>说明</b> 安全大屏功能需要在标准版/专业版基础上单独购买。	×	√	√
<b>安全报告</b>	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。	×	×	√
<b>任务中心</b>	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 5-7 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 5-8 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
<b>基线检查</b>	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。	√	√	√
<b>漏洞管理</b>	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。	√	√	√
<b>应急漏洞公告</b>	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。	√	√	√
<b>策略管理</b>	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 5-9 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
<b>事件管理</b>	集中呈现事件详情，支持人工转事件、自动化转事件。	×	√	√
<b>告警管理</b>	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。 <ul style="list-style-type: none"> <li>基础版安全云脑仅支持各安全服务的原始告警汇聚。</li> <li>标准版安全云脑仅支持各安全服务的原始告警汇聚。</li> <li>专业版安全云脑支持各安全服务的原始告警汇聚，还支持威胁检测模型告警。</li> </ul>	√	√	√

功能模块	功能描述	基础版	标准版	专业版
情报管理	<p>威胁情报是描述对系统和用户的现有或潜在威胁的信息，使用威胁情报为异常活动提供必要的上下文，以便安全负责人可以快速采取措施来保护其人员、信息和资产。</p> <p>威胁情报的形式是情报指标，情报指标是将URL或IP地址等观察项目与网络钓鱼或恶意软件等已知威胁活动关联起来的数据。它会大规模地应用于安全产品和自动化服务，以检测组织面临的潜在威胁并进行防范。通过情报指标的创建和管理，加快威胁检测和修正。安全云脑支持人工新增情报指标或导入情报指标，创建情报指标后可以通过自定义剧本实现威胁管理分析处理等操作。</p>	×	×	√

## 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）和操作连接管理等。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。

安全云脑标准版不支持安全编排功能，可以通过购买安全编排增值包使用该功能。

表 5-10 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	<p>支持对剧本、流程、操作连接、实例的全生命周期管理。</p> <p><b>说明</b> 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<a href="#">赠送规格说明</a>。</p>	×	×	√
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。	×	×	√
目录定制	支持自定义目录，根据需要对目录进行定制。	×	√	√

## 日志审计

支持接入云服务日志和数据采集功能，并通过查询与分析语法检索分析或筛选统计安全数据，支持统计日志审计结果。

表 5-11 日志审计功能说明

功能模块	功能描述	基础版	标准版	专业版
日审总览	日审总览页面呈现统计周期内当前工作空间中整体日志审计状况。	√	√	√
安全数据	<ul style="list-style-type: none"> <li>● <b>查询与分析</b> <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> </ul> </li> <li>● <b>数据投递</b>：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。</li> <li>● <b>数据监控</b>：支持数据流量端到端的监控管理。</li> <li>● <b>数据消费</b>：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。</li> </ul> <p><b>说明</b> 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<a href="#">赠送规格说明</a>。</p>	×	√	√
云服务接入	安全云脑支持集成WAF、HSS、OBS等多种华为云产品的日志数据。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。	×	√	√
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。	×	√	√

## 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 5-12 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
	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	预置威胁模型	×	计算模型数据120 MB/天/配额；预置模型200个
	预置响应剧本	×	预置剧本30个
安全编排	安全编排	×	操作7000次

# 6 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6-1所示。

表 6-1 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。

# 7 经验包

## 7.1 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](#)。

本章节介绍SecMaster云服务基线检查支持的检查项目。

表 7-1 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	13
	检测	7
	基础设施防护	20
	数据防护	22
	事件响应	13
护网检查	安全套件覆盖	6
	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

检查规范	检查类别	包含的检查项数量
华为云安全配置基线3.0	网络	18
	身份与访问管理	22
	安全	30
	日志与监控	23
	虚拟机与容器	26
	数据库	68
	存储	31
	企业智能	34
	应用中间件	11
	开发与运维	5
	CDN与智能边缘	2
GDPR ( General Data Protection Regulation )	第三方披露	5
	数据跨境转移	6
	数据使用, 保留和处置	16
	数据主体访问	10
	通知	8
	选择和同意	7
	组织架构	2
经典弱口令检测	弱口令检测	1
口令复杂度策略检测	口令复杂度	5
PCI-DSS	维护信息安全政策	25
	实施强有力的访问控制措施	35
	建立和维护安全网络和系统	21
	维护漏洞管理计划	4
	定期监控和测试网络	20
	保护账户数据	16
	其他	8

检查规范	检查类别	包含的检查项数量
NIST SP 800-53	系统和采购	8
	项目管理	7
	评估、授权和监控	7
	审计与问责	9
	媒体介质保护	2
	系统和通信保护	25
	事件与响应	5
	物理环境保护	23
	规划和策略	2
	系统和信息完整性	9
	访问控制	13
	风险评估	11
	配置管理	12
	意识与培训	5
	识别与认证	12
	个人信息处理和透明度	6
	人员安全	7
	应急计划	7
	供应链风险管理	5
	维护与运维	1
ISO/IEC 27002:2022	备份与恢复	17
	身份与访问控制	14
	数据安全	1
	应用安全	27
	运维和运营安全	15
	治理和策略	9

## 安全上云合规检查—身份与访问管理

表 7-2 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露，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	<p>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。</p> <p>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。</p> <p>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。</p> <p>检查账号锁定时限是否设置为15分钟。</p>
IAM密码策略（防止密码重复使用）检查	<p>IAM允许用户设置密码策略。</p> <p>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。</p> <p>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。</p>
会话超时策略检查	<p>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。</p> <p>检查会话时限是否设置为15分钟。</p>
账号停用策略检查	<p>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对应的控制台，建议禁用该用户的控制台访问权限。</p> <p>检查账号停用策略是否启用，且有效期设置为90天。</p>
IAM用户密码强度检查	<p>IAM用户的登录密码建议设置为安全程度强的密码。</p> <p>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。</p> <p>检查IAM用户的密码强度是否为最高级别。</p>
CBH实例登录开启多因子认证检查	<p>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。</p> <p>检查CBH实例是否已开启多因子认证。</p>

## 安全上云合规检查—检测

表 7-3 检测风险项检查项目

检查项目	检查内容
ELB健康状态检查	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
CTS启用检查	<p>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。</p> <p>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。</p>
OBS桶日志记录启用检查	<p>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。</p> <p>检查所有OBS桶，是否开启日志记录功能。</p>
数据库安全审计启用检查（云上RDS场景）	<p>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。</p> <p>检查是否已启用数据库安全审计。</p>
云监控服务启用检查	<p>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。</p> <p>检查是否已启用云监控服务。</p>
云监控服务中的主机监控检查	<p>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。</p> <p>基础监控为用户提供免安装的基础指标监控服务；操作系统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。</p> <p>检查主机监控中的弹性云服务器是否已安装监控插件。</p>

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 7-4 基础设施防护风险项检查项目

检查项目	检查内容
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，是企业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。
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，是企业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（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，是企业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，是企业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。

检查项目	检查内容
ELB实例（共享型）启用访问控制检查	<p>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。</p> <p>检查弹性负载均衡（Elastic Load Balance, ELB）实例，是否开启访问控制策略。</p>
网络ACL规则配置检查	<p>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。</p> <p>检查是否配置网络ACL规则。</p>
用于VPC对等连接路由表检查	<p>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。</p> <p>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。</p> <p>检查用于对等连接的路由表是否满足最小访问权限。</p>
VPC规划检查	<p>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。</p> <p>两个VPC之间可以采用对等连接进行互连。</p> <p>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。</p> <p>检查VPC规范是否合理。</p>
WAF启用（云模式/独享模式/ELB模式）检查	<p>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。</p> <p>检查是否已启用WAF。</p>
WAF回源配置检查（未配置ELB）	<p>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。</p> <p>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。</p>
WAF防护策略配置（地理位置访问控制）检查	<p>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）。</p>

检查项目	检查内容
Web基础防护配置检查	<p>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。</p> <p>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。</p> <p>检查是否已开启Web基础防护并设置为拦截模式。</p>
VSS启用检查	<p>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。</p> <p>检查是否已启用VSS服务。</p>
Anti-DDoS流量清洗启用检查	<p>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。</p> <p>检查是否已启用Anti-DDoS流量清洗服务。</p>
DDoS高防启用检查	<p>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。</p> <p>检查是否已启用DDoS高防。</p>
云堡垒机启用检查	<p>云堡垒机（Cloud Bastion Host, CBH）是华为云的一款4A统一安全管控平台，为企业集中提供集中的账号、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。</p> <p>检查是否已启用云堡垒机服务。</p>
主机安全防护启用检查	<p>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。</p> <p>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）。</p> <p>检查主机是否开启主机安全防护。</p>

检查项目	检查内容
HSS网页防篡改启用与防护目录配置检查	<p>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。</p> <p>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。</p> <p>检查主机是否开启网络防篡改防护且已配置好防护目录。</p>
主机紧急修复漏洞检查	<p>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。</p> <p>检查HSS中是否存在紧急修复漏洞。</p>
CDN访问控制配置检查	<p>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。</p> <p>检查CDN是否配置访问控制规则。</p>

## 安全上云合规检查—数据防护

表 7-5 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	<p>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。</p> <p>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。</p>
CDN证书有效性检查	<p>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。</p> <p>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。</p>
SSL证书有效性检查	<p>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。</p> <p>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。</p>

检查项目	检查内容
RDS数据库绑定EIP时的安全设置检查	<p>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。</p> <p>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。</p>
DDS数据库绑定EIP时的安全设置检查	<p>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。</p> <p>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。</p>
DCS数据库绑定EIP时的安全设置检查	<p>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。</p> <p>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。</p>
云数据库GaussDB绑定EIP时的安全设置检查	<p>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。</p> <p>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。</p>
RDS数据库绑定EIP检查	<p>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。</p> <p>检查当RDS数据库配置，是否开通公网连接方式。</p>
DDS数据库绑定EIP检查	<p>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。</p> <p>检查当DDS数据库配置，是否开通公网连接方式。</p>
DCS数据库绑定EIP检查	<p>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。</p> <p>检查当DCS数据库配置，是否开通公网连接方式。</p>
云数据库GaussDB绑定EIP检查	<p>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。</p> <p>检查当云数据库GaussDB配置，是否开通公网连接方式。</p>

检查项目	检查内容
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
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。

检查项目	检查内容
DCS数据库实例安全组入方向规则检查	<p>安全组入方向规则应满足最小化访问控制原则。</p> <p>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）：</p> <p>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</p> <p>IPv6：源地址为::/0</p> <p>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。</p>
DDS数据库实例安全组入方向规则检查	<p>安全组入方向规则应满足最小化访问控制原则。</p> <p>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）：</p> <p>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</p> <p>IPv6：源地址为::/0</p> <p>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。</p>
RDS数据库实例安全组端口开放检查	<p>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。</p> <p>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。</p> <p>检查RDS实例是否开放非必要的端口。</p>
DCS数据库实例安全组端口开放检查	<p>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。</p> <p>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。</p> <p>检查DCS实例是否开放非必要的端口。</p>
DDS数据库实例安全组端口开放检查	<p>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。</p> <p>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。</p> <p>检查DDS实例是否开放非必要的端口。</p>

## 安全上云合规检查—事件响应

表 7-6 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。
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。

检查项目	检查内容
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，以使用于恢复。
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 7-7 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。

检查项目	检查内容
主机Agent状态检查	<p>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。</p> <p>在主机中安装Agent后，您的主机才能受到HSS的保护。</p> <p>检查主机Agent是否为在线状态。</p>
主机安全检测状态检查	<p>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。</p> <p>检查主机的检测结果是否存在异常。</p>
WAF（云模式）基础防护配置检查	<p>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。</p> <p>检查WAF在云模式下是否已开启Web基础防护。</p>
WAF（云模式）防护策略配置检查	<p>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。</p> <p>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。</p> <p>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。</p>
WAF（独享模式）基础防护配置检查	<p>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。</p> <p>检查WAF在独享模式下是否已开启Web基础防护。</p>
WAF（独享模式）防护策略配置检查	<p>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。</p> <p>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。</p> <p>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。</p>

检查项目	检查内容
主机Agent版本检查	<p>在主机中安装Agent后，您的主机将受到HSS云端防护中心全面的安全保障，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。</p> <p>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。</p> <p>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。</p> <p>检查所有主机Agent是否为企业版及以上版本。</p>

## 护网检查—账号加固

表 7-8 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	<p>访问密钥（AK/SK，Access Key ID/Secret Access Key）是账号的长期身份凭证。</p> <p>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。</p> <p>检查管理员账户是否启用访问密钥。</p>
主机弱密码检查	<p>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。</p> <p>检查主机是否存在弱口令。</p>
委托账号检查	<p>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。</p> <p>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。</p> <p>检查是否存在个人委托账号。</p>
全局服务中的委托权限配置检查	<p>检查全局服务中的委托权限是否存在Security Administrator，Tenant Administrator。</p>
项目服务中的委托权限配置检查	<p>检查项目服务中的委托权限是否存在Security Administrator，Tenant Administrator。</p>

## 护网检查—主机加固

表 7-9 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	<p>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。</p> <p>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。</p> <p>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。</p>
CCE集群Kubernetes版本检查	<p>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。</p> <p>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。</p> <p>检查CCE集群Kubernetes版本是否在1.15以下。</p>
VPC配置（对等连接）检查	<p>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。</p> <p>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。</p>
VPC配置（VPN网关）检查	<p>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。</p> <p>检查VPC是否已经创建了VPN网关。</p>

## 护网检查—Sudo 漏洞

表 7-10 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	<p>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。</p> <p>检查所有主机是否存在Sudo漏洞。</p>

## 护网检查—访问控制

表 7-11 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	<p>安全组入方向规则应满足最小化访问控制原则。</p> <p>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。</p> <p>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。</p> <p>IPv6：源地址为::/0。</p>

## 护网检查—敏感信息排查

表 7-12 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	<p>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。</p> <p>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。</p> <p>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。</p>
OBS桶日志记录启用检查	<p>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。</p> <p>检查所有OBS桶，是否开启日志记录功能。</p>
数据库中敏感信息检查	<p>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。</p> <p>检查数据库中是否存在敏感信息。</p>
OBS中敏感信息检查	<p>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。</p> <p>检查OBS中是否存在敏感信息。</p>

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。

## 华为云安全配置基线 3.0—网络

表 7-13 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。如业务所必需，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。如业务所必需，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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
确保VPC对等连接满足最小化访问控制	<p>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。</p> <p>建议本端路由的目的地址，建议限定在最小子网网段内。对端路由的目的地址，建议限定在最小子网网段内。</p>
负载均衡实例需要多AZ部署	ELB实例需要多AZ部署，保证具备容灾能力。
确保弹性公网IP在指定天数内绑定到资料实例	该控制项用于检查租户的EIP资源在指定的时间内是否绑定到相应的资源实例上，如果不需要使用的EIP，可以释放。
确保负载均衡开启删除保护	ELB实例对客户流量转发非常关键，需要开启删除保护。未开启删除保护存在安全风险，不符合安全要求。
负载均衡必须配置HTTPS或TLS	TLS/HTTPS协议数据传输是加密传输，能够有效的防止数据泄露篡改风险，要求所有监听器必须为HTTPS监听器。如果其他协议监听器存在安全风险，不符合安全要求。
确保ELB监听器绑定的安全策略中使用安全的TLS版本和加密套件	ELB（弹性负载均衡）支持在HTTPS或TLS监听器中配置安全策略，允许用户选择安全的TLS版本和加密套件。通过选择最新的TLS版本（如TLS1.2或TLS1.3）和强加密套件，ELB可以确保客户端与服务器之间的通信安全，防止数据在传输过程中被窃听或篡改。使用安全的TLS版本和加密套件可以应对中间人攻击、降级攻击、数据泄露等风险。如果未配置，则可能导致因使用旧版本TLS协议或加密套件导致的数据泄露与篡改，并且可能面临中间人攻击的风险。使用安全的TLS版本和加密套件可能导致兼容性问题，旧版本浏览器或客户端可能不支持最新的TLS版本。
应配置为将所有 HTTP 请求重定向到 HTTPS	HTTP协议不安全，要求所有HTTP请求必须重定向到HTTPS。

检查子项目	检查项目
带有SSL/HTTPS监听器的负载均衡器应使用由证书管理服务提供的证书	推荐您在华为云云证书与管理服务购买服务器证书，并通过华为云云证书与管理服务对证书进行管理。
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。
确保ELB实例多AZ部署	ELB（弹性负载均衡）支持多AZ（可用区）部署，允许用户将ELB实例部署在多个可用区。通过多AZ部署，ELB可以提高服务的可用性和容灾能力，确保在某个可用区发生故障时，服务仍可通过其他可用区继续提供。采用多AZ部署可以应对单点/区域故障、负载不均等风险。若未采用多AZ部署，则服务可能因可用区或可用区ELB实例发生故障而中断，并且可能会导致流量分布不均的问题。多AZ部署会导致网络流量经过更长的网络路径，可能增加数据传输的延迟，并导致云服务网络成本的上升。
负载均衡实例需要配置WAF策略	ELB实例需要配置waf策略。
确保不存在未绑定任何资源的弹性公网IP	该控制项用于检查是否存在未使用的EIP资源，帮助客户维护准确的资产清单，如果确认不需要使用，可以释放未使用的EIP。
确保负载均衡实例不绑定EIP	ELB负载均衡器应根据业务需求配置公网或内网访问。对于仅需内网访问的场景，应避免配置弹性公网IP；公网访问场景绑定弹性公网IP，同时配置安全组、ACL和WAF等安全措施。

## 华为云安全配置基线 3.0—身份与访问管理

表 7-14 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。

检查子项目	检查项目
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露，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）。
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： <ul style="list-style-type: none"><li>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。</li><li>密码中允许同一字符连续出现次数（最大次数设置为 1）。</li></ul>
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	<p>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：</p> <ol style="list-style-type: none"><li>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。</li><li>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。</li><li>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：<ol style="list-style-type: none"><li>a. 控制台访问：仅对账号下的IAM用户登录对应的控制台生效，对账号本身不生效。</li><li>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。</li></ol></li></ol>
确保管理员账号禁用 AK/SK	<p>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。</p>
确保不创建允许“*:*”管理权限的IAM策略	<p>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。</p>

检查子项目	检查项目
配置登录验证策略	<p>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”。</p> <ol style="list-style-type: none"> <li>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。</li> <li>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： <ul style="list-style-type: none"> <li>● 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。</li> <li>● 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。</li> <li>● 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。</li> </ul> </li> <li>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。</li> <li>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。</li> <li>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。</li> </ol>
确保不创建非管理员权限的IAM用户	<p>“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。</p>
确保IAM用户不直接附加策略或权限，而是通过“继承所选用户组的策略”的方式给IAM用户授权	<p>IAM用户直接附加了策略或权限，视为“不合规”。建议您通过“继承所选用户组的策略”的方式给IAM用户授权，而不是“直接给用户授权”。这可以降低访问管理的复杂性，并减少IAM用户无意中接收或保留过多权限的风险。</p>

检查子项目	检查项目
应避免根用户以外的IAM用户加入admin用户组，防止授权过大	根用户以外的IAM用户加入admin用户组，视为“不合规”。“admin”为缺省用户组，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。
确保创建的IAM策略已正确附加到IAM用户、用户组或委托	IAM策略未附加到IAM用户、用户组或委托，视为“不合规”。避免长期存在未绑定的IAM策略，防止因管理疏漏引发计划外授权，从而导致恶意操作。长期未绑定的IAM策略，建议删除处理。
确保IAM角色正确附加到IAM用户、用户组或委托	IAM角色未附加到IAM用户、用户组或委托，视为“不合规”。避免长期存在未绑定的IAM权限，防止因管理疏漏引发计划外授权，从而导致恶意操作。
确保IAM用户组已加权限	IAM用户组未添加任意权限，视为“不合规”。管理员可以创建用户组，并给用户组授予策略或角色，然后将用户加入用户组，使得用户组中的用户获得相应的权限。如果您的用户组没有配置任何授权，则不会带来任何有效授权行为，建议您定时检查并清理无效的IAM用户组，提升运行和管理效率。
确保对IAM服务的操作已记录审计日志	用户可以通过开启CTS服务来记录对IAM服务操作的审计日志，开启审计日志对于保护信息安全、确保合规性、提高系统稳定性和透明度等方面都具有重要意义。1、增强安全性：审计日志记录了系统中发生的所有重要操作，包括登录尝试、文件访问、配置更改等。通过分析这些日志，安全团队可以及时发现异常行为，比如未授权的访问尝试或恶意活动，从而采取措施防止潜在的安全威胁。2、满足合规要求：许多行业标准和法律法规（如GDPR、HIPAA、SOX等）要求组织必须记录和保留特定类型的活动日志。开启审计日志有助于满足这些合规性要求，避免因不合规而面临的罚款或其他法律后果。3、追责：在多用户环境中，审计日志能够记录每个用户的具体操作，这对于明确责任、防止内部欺诈行为非常重要。一旦发生问题，可以通过日志追踪到具体的操作者，便于进行责任追究。4、提高透明度：对于外部审计或监管机构来说，审计日志提供了透明度，证明了组织在数据处理、安全管理和合规性方面的努力。这有助于建立信任，增强组织的声誉。

## 华为云安全配置基线 3.0—安全

表 7-15 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巨大挑战之一。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	启用密码安全中心（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，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。
安全组端口检查，避免安全组入方向设置为0.0.0.0/0或::/0	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”。0.0.0.0/0表示所有IPv4地址，::/0表示所有IPv6地址。如果允许任何IP都可以访问任何端口，会极大地增加被攻击的风险。强烈建议您遵循最小权限原则配置安全组规则，避免过度授权。
应确保WAF防护策略配置防护规则	WAF防护策略可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。确保防护策略不是空置状态，而是根据自己网站防护的需要，灵活配置防护规则，才能更好的防护您的网站业务。
应确保CSMS轮转凭据启用自动轮转	如果长时间不更新凭据，凭据内保护的重要信息（例如：重要密码、令牌、证书、SSH密钥、API密钥等）的泄露风险也会增加，定期轮换凭据会增加所保护的明文信息安全性。

检查子项目	检查项目
配置KMS禁用或计划删除密钥的事件监控告警	CES配置监控KMS禁用或计划删除密钥的事件监控告警，旨在提供对关键云资源安全事件的实时监控与响应。通过事件监控功能，用户能够对云环境中重要的操作事件进行数据上报和查询，尤其是针对KMS密钥禁用或删除的高风险操作。一旦发生此类事件，系统将触发告警，并通过多种通知方式及时提醒用户，确保其能够迅速采取措施防止潜在的安全风险。此功能主要应对的风险是密钥管理不当带来的安全隐患，包括未经授权的密钥禁用、删除或其他操作，可能导致加密数据泄露、身份验证失败或数据完整性受损，请确保配置CES配置监控KMS禁用或计划删除密钥的事件监控告警。
应确保WAF防护域名配置防护策略	WAF防护策略可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。确保防护策略不是空置状态，而是根据自己网站防护的需要，灵活配置防护规则，才能更好的防护您的网站业务。
启用KMS密钥轮换	启用密码安全中心（Data Encryption Workshop, DEW）密钥轮换策略，定期更换原密钥的密钥材料，提升加密密钥的安全性。
应确保CSMS凭据在指定天数内轮转	CSMS凭据可以配置轮转，可以使用轮转来将长期机密信息替换为短期机密信息。如果长时间不更新凭据，凭据内保护的重要信息（例如：重要密码、令牌、证书、SSH密钥、API密钥等）的泄露风险也会增加，轮转机密信息可以增加所保护的明文信息安全性、限制非授权用户使用被泄露机密信息的时间。因此，应该定期轮转CSMS凭据。PCI DSS要求至少每90天更改一次用户密码或凭据轮转。
VPC默认安全组不应允许入站或出站流量	默认安全组的规则允许与同一安全组分配的网络接口（及其关联实例）之间的所有出站和入站流量。建议不要使用默认安全组。由于默认安全组无法删除，您应更改默认安全组规则设置以限制入站和出站流量。这样可以防止在意外将默认安全组配置给ECS实例等资源时，出现非预期的流量。
ACL要管理子网，未使用的网络访问控制列表应被移除	未使用的网络ACL（访问控制列表）可能增加安全风险，因为它们可能包含过时或宽松的规则，若被错误关联到子网，可能导致意外的网络访问权限。
安全组入站流量限制指定端口	当安全组的入站流量不限制指定端口的所有IPv4地址(0.0.0.0/0)或所有IPv6地址(::/0)，视为不合规。0.0.0.0/0表示所有IPv4地址，::/0表示所有IPv6地址。如果允许任何IP都可以访问您指定的高危端口，会极大地增加被攻击的风险。 1、如数据库服务（如MySQL的3306端口）允许0.0.0.0/0或::/0访问，可能导致未授权用户访问敏感数据。 2、如管理端口（如SSH的22端口、RDP的3389端口）允许0.0.0.0/0或::/0访问，可能导致服务器被入侵。建议遵循最小权限原则配置安全组规则，避免过度授权。

检查子项目	检查项目
应确保配置了自动轮转的CSMS凭据轮转成功	CSMS凭据轮转成功或不涉及轮转，视为合规。当您为凭据开启轮转后，您需要确保轮转执行是成功的。如果轮转失败，可能导致以下问题：凭据泄露风险：长期不轮转的凭据更容易被攻击者获取，增加数据泄露或服务滥用的可能性。服务中断风险：轮转失败可能导致凭据过期，引发服务中断或应用故障。约束：该合规规则只检查定时轮转是否成功，不检查立即轮转是否成功。该合规规则受制于Config收集资源的实时性，可能存在最多不超过24小时的滞后。
确保安全组连接到弹性网络接口	默认安全组以外的安全组未关联弹性网络接口，视为“不合规”。安全组的规则是通过关联弹性网卡来生效的。如果没有关联弹性网卡，安全组的规则将无法对实例的流量进行过滤和控制，可能导致敏感数据泄露或未授权访问。
确保CFW实例绑定标签	通过CFW添加标签，实现资源的分类，可通过标签进行权限管理。
应确保启用Web应用防火墙功能	Web应用防火墙（Web Application Firewall, WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。
确保CFW实例配置外部访问默认阻断策略	开启防护后，云防火墙默认放行所有流量，配置合适的访问控制策略能有效地帮助您对内部服务器与外网之间的流量进行精细化管控。为了提升安全性，建议配置外网访问默认阻断策略。
启用DEW凭据自动轮转功能	启用密码安全中心（Data Encryption Workshop, DEW）凭据轮换功能，实现对敏感凭据的定期更新，提升系统的安全性。

## 华为云安全配置基线 3.0—日志与监控

表 7-16 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。

检查子项目	检查项目
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。
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	<p>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：</p> <ul style="list-style-type: none"> <li>• IAM: createUser、deleteUser、createAgency、DeleteAgency 等</li> <li>• ECS: rebootServer、updateSecurityGroup、removeSecurityGroup 等</li> <li>• VPC: modifySecurityGroup 等</li> <li>• CTS: updateTracker、deleteTracker 等</li> <li>• OBS: setBucketAcl、setBucketPolicy 等</li> </ul> <p>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。</p> <p>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。</p>
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。

检查子项目	检查项目
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。
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： <ul style="list-style-type: none"> <li>● OBS：提供日志存储功能，长期保存日志。</li> <li>● 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。</li> </ul>
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。
应确保DDoS原生基础防护开启LTS日志记录	启用Anti-DDoS防护功能后，您可以将攻击日志记录到云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的Anti-DDoS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。
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。

检查子项目	检查项目
启用CTS并配置LTS转储	云审计服务（Cloud Trace Service），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。
确保CTS实例添加标签	云审计服务（Cloud Trace Service），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。
启用CES资源告警功能	云监控服务(CES)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。告警功能提供对监控指标的告警功能，用户对云服务的核心监控指标设置告警规则，当监控指标触发用户设置的告警条件时，支持以邮箱、短信、HTTP、HTTPS等方式通知用户，让用户在第一时间得知云服务发生异常，迅速处理故障，避免因资源问题造成业务损失。该服务应对的主要风险包括资源使用异常、业务性能下降及潜在故障风险。如果告警功能未能启用或配置不当，可能导致用户无法及时察觉资源问题，进而影响业务运行的稳定性，甚至可能造成业务停机、数据丢失或财务损失。因此，确保告警机制的正常运作对于云环境中的资源管理和故障响应至关重要。
应确保ER服务启用安全审计日志	<p>用户可以通过开启CTS服务来记录对ER服务操作的审计日志，开启审计日志对于保护信息安全、确保合规性、提高系统稳定性和透明度等方面都具有重要意义。</p> <ol style="list-style-type: none"> <li>1、增强安全性：审计日志记录了系统中发生的所有重要操作，包括登录尝试、文件访问、配置更改等。通过分析这些日志，安全团队可以及时发现异常行为，比如未授权的访问尝试或恶意活动，从而采取措施防止潜在的安全威胁。</li> <li>2、满足合规要求：许多行业标准和法律法规（如GDPR、HIPAA、SOX等）要求组织必须记录和保留特定类型的活动日志。开启审计日志有助于满足这些合规性要求，避免因不合规而面临的罚款或其他法律后果。</li> <li>3、追责：在多用户环境中，审计日志能够记录每个用户的具体操作，这对于明确责任、防止内部欺诈行为非常重要。一旦发生问题，可以通过日志追踪到具体的操作者，便于进行责任追究。</li> <li>4、提高透明度：对于外部审计或监管机构来说，审计日志提供了透明度，证明了组织在数据处理、安全管理和合规性方面的努力。这有助于建立信任，增强组织的声誉。</li> </ol>

检查子项目	检查项目
CES配置监控VPC变更的事件监控告警	CES配置监控VPC变更的事件监控告警，可以帮助用户实时监控和响应VPC中网络架构的关键变化。通过事件监控功能，用户能够对VPC相关的操作事件进行数据上报和查询，尤其是针对删除VPC、修改VPC等操作。一旦发生这些高风险的配置变更，系统将触发告警，及时通知用户，帮助其快速审查和采取必要的安全措施，确保网络架构的稳定和安全。如果未及时监控VPC的配置变更，可能会导致关键网络组件暴露或无法访问，进而影响云环境中的其他服务和资源。确保VPC变更事件得到及时监控和告警，对于防止不必要的网络安全漏洞和保障业务的正常运行至关重要。
应配置华为云账号通过Organizations进行纳管	华为云账号配置通过Organizations服务进行纳管，主要通过集中管理多账号关系、设置组织单元与服务控制策略，实现账号资源的统一策略管控与权限最小化分配。此配置直接应对分散账号管理引发的安全与合规风险：若账号未纳入组织，各账号独立配置易出现安全策略不一致，导致越权操作难追溯或配置漏洞被利用。若不满足此要求，一旦攻击者利用某账号的配置弱点横向渗透，将因缺乏跨账号监控与策略联动而延误响应，引发数据泄露、服务中断及多区域合规处罚。开启纳管对业务负面影响需要用户使用组织对多账号进行结构化管理。

## 华为云安全配置基线 3.0—虚拟机与容器

表 7-17 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。

检查子项目		检查项目
	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。
	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。

检查子项目		检查项目
	集群节点不要暴露到公网	<p>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。</p> <p>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。</p> <p>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</p>
	加固K8S集群所在VPC的安全组规则	<p>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。</p>

检查子项目		检查项目
	应确保使用在维护周期内的CCE集群版本	<p>云容器引擎（CCE）严格遵循社区一致性认证，每年发布3个Kubernetes版本，每个版本发布后提供至少24个月的维护周期，CCE保证维护周期内的Kubernetes版本的稳定运行。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CCEConsole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。主动升级集群有以下好处：</p> <ol style="list-style-type: none"> <li>1、降低安全和稳定性风险：Kubernetes版本迭代过程中，会不断修复发现的安全及稳定性漏洞，长久使用EOS版本集群会给业务带来安全和稳定性风险。</li> <li>2、支持新功能和操作系统：Kubernetes版本的迭代过程中，会不断带来新的功能、优化。您可通过CCE集群版本发布说明查看最新版本的特性说明。</li> <li>3、避免大跨度兼容风险：Kubernetes版本的迭代过程中，会不断带来API变更与功能废弃。长久未升级的集群，在需要升级时需要更大的运维保障投入。周期性的跟随升级能有效缓解版本差异累积导致的兼容性风险。建议用户每季度升级一次补丁版本，每年升级一次大版本至当前支持的最新版本。</li> <li>4、更加有效的技术支持：对于EOS的Kubernetes版本集群，CCE不再提供安全补丁和问题修复，同样无法保证EOS版本集群的技术支持质量。升级集群可能会带来如下影响：Kubernetes不同版本之间存在一些兼容性问题，升级集群前可能需要租户适配应用；另外，升级集群属于高危操作，在生产环境升级集群前要充分验证。</li> </ol>
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。

检查子项目		检查项目
	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。
	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。
	确保ECS实例关闭公网访问	ECS实例具有弹性公网IP，视为“不合规”。由于华为云ECS实例可能包含敏感信息，如果您的业务不需要与公网交互，请避免将实例直接暴露在公网。
	确保ECS实例开启主机安全防护	ECS实例未绑定HSS Agent并启用防护，视为“不合规”。弹性云服务器应安装企业主机安全防护（HSS）且启用防护，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。

检查子项目		检查项目
裸金属服务器 BMS	使用密钥对安全登录BMS	<p>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。</p> <p>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。</p> <p>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。</p>
	确保BMS内的重置密码插件更新到最新版本	<p>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。</p> <p>及时更新重置密码插件可确保漏洞及时得到修复。</p>
	在BMS内设置防火墙策略限制对元数据的访问	<p>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。</p> <p>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。</p>
容器镜像服务 SWR	SWR企业仓私有仓库至少需要配置一条老化策略	配置镜像老化规则是容器化运维的核心实践，通过自动化清理冗余镜像，实现存储成本控制、安全风险降低和系统性能优化。
	SWR企业仓私有仓库需要配置镜像不可变规则	配置镜像不可变规则是容器化应用的基石实践，通过强制版本唯一性和完整性，有效防御人为错误、供应链攻击和合规风险。

检查子项目		检查项目
	SWR企业仓需要使用用户自定义的KMS密钥对镜像加密存储	使用用户自定义密钥加密镜像仓库，是提升数据安全性和合规性的关键措施，尤其适用于对敏感数据控制严格、需满足多层级审计要求的场景。SWR企业仓使用OBS对象存储作为后端存储，支持使用用户已有的OBS桶，用户创建OBS桶的时候，可以使用自己管理的KMS密钥。
	通过VPCEP访问SWR企业仓Docker Registry API必须配置VPCEP策略	配置VPCEP策略，限定VPC只能上传下载指定的镜像，避免数据泄露，提升系统安全性。
	SWR企业的公开仓需要支持标签	命名空间用于管理多个具有关联属性的镜像，不直接存储容器镜像，可对应企业内部的一个产品项目或部门。当公司部门繁多时，可以通过添加命名空间标签，方便后续通过标签对命名空间进行查找及管理。仓库归属于命名空间，当命名空间公开时，该命名空间下的所有仓库中的镜像均能被匿名下载。

检查子项目		检查项目
弹性伸缩 AS	确保弹性伸缩组创建的ECS实例覆盖多AZ	<p>华为云弹性伸缩组（AS）支持将新创建的ECS实例分布到多个可用区（AZ）。每个AZ是具备独立风火水电设施的物理数据中心隔离单元，同一Region内的多个AZ通过高速光纤互联，这是构建高可用应用架构的基础。配置伸缩组使用多AZ部署，核心目的是应对单AZ故障风险。如果所有ECS实例都集中在单个AZ内，一旦该AZ因基础设施故障（如断电、断网）或自然灾害发生中断，将导致整个伸缩组内的实例不可用，业务服务完全中断，丧失连续性。即使伸缩组状态正常，如果所选AZ不支持伸缩配置中指定的ECS实例类型，可能导致伸缩组无法使用或扩容活动异常，资源弹性扩展能力受限。此外，即使部分AZ支持所需实例类型，扩容时实例也无法均匀分布，削弱了跨AZ的高可用性。启用此规则（即配置多AZ）后，主要业务影响体现在跨AZ通信会引入轻微的网络时延增加（相比同AZ内通信），对于网络时延要求极高的业务（如毫秒级响应的金融交易系统）可能需注意。同时，配置时需确保所选的所有AZ都支持您需要的ECS实例类型，否则扩容仍可能集中在支持的AZ中，达不到理想的均匀分布效果。因此，建议在创建伸缩组时至少选择2个可用区，并优先采用“均衡分布”扩展策略，以实现最佳的高可用性。</p>

检查子项目		检查项目
	确保弹性伸缩组使用弹性负载均衡健康检查	<p>华为云弹性伸缩服务（Auto Scaling, AS）与弹性负载均衡（Elastic Load Balance, ELB）结合使用时，可以自动调整计算资源，以适应业务负载的变化。通过配置ELB健康检查，可以确保只有健康状态的实例参与负载均衡，从而提高服务的可用性和稳定性。健康检查功能会定期检查后端服务器的健康状态，一旦发现异常，会自动将流量重定向到其他健康的实例，避免了单点故障对业务的影响。不使用ELB健康检查可能会导致异常的实例继续接收流量，影响用户体验和业务连续性。在高并发场景下，异常实例可能会成为性能瓶颈，甚至导致整个服务不可用。此外，未及时发现和隔离故障实例，还可能增加安全风险，如被攻击者利用进行DDoS攻击等。若不使用健康检查，则异常实例可能继续接收流量，可导致用户请求失败或响应时间增加，并同时造成资源的浪费。同时，未及时隔离并清理故障实例，可导致实例被攻击者利用，增加安全风险。若健康检查频率设置不当，可能导致健康检查频率过高，增加负载并影响性能。</p>

## 华为云安全配置基线 3.0—数据库

表 7-18 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。

检查子项目		检查项目
	开启加密通信	如果未启用TLS加密连接，那么在MySQL客户端和服务端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。
	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。

检查子项目		检查项目
	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。
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
	GaussDB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。

检查子项目		检查项目
	WAL归档配置	WAL ( Write Ahead Log ) 即预写式日志, 也称为Xlog。
	GaussDB应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。
	应确保GaussDB实例不使用数据库引擎的默认端口	确保GaussDB实例不使用数据库引擎的默认端口是一项关键的网络安全加固措施, 其核心目的是规避自动化攻击和降低被入侵风险。
	应确保GaussDB数据库实例不具有弹性公网IP ( EIP )	GaussDB数据库实例不绑定弹性公网IP ( EIP ) 是一项主动的网络安全加固设计, 其核心目的是通过强制隔离公网访问, 降低外部攻击风险, 保障数据库的机密性与完整性。
	GaussDB实例应开启慢日志	租户在开启GaussDB实例慢日志功能后, 租户可以通过GaussDB慢日志定位SQL语句执行慢的问题。当前慢日志功能默认开启。
	GaussDB实例应开启错误日志	租户开启GaussDB错误日志功能后, 可以通过分析GaussDB错误日志来定位错误原因。当前错误日志功能默认开启。
	GaussDB 数据库实例应配置为跨多个可用区 ( AZ ) 部署	可用区 ( AZ, Availability Zone ) : 一个AZ是一个或多个物理数据中心的集合, 有独立的风火水电, AZ内逻辑上再将计算、网络、存储等资源划分成多个实例。一个Region中的多个AZ间通过高速光纤相连, 以满足用户跨AZ构建高可用性系统的需求。
	GaussDB应开启数据库审计日志功能	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。
DDS 文档数据库	开启加密通信	<p>如果未启用TLS加密连接, 那么在MongoDB客户端和服务端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。</p> <p>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。</p>

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mongodb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。

检查子项目		检查项目
RDS for SQL Server 数据库	确保Cloud SQL Server实例的‘cross db ownership chaining’数据库标志设置为'off' (自动执行)	使用 cross db ownership chaining 选项可以为 Microsoft SQL Server 实例配置跨数据库所有权链。
	RDS数据库实例应将日志发布至日志跟踪服务 (LTS)	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SQLServer日志数据, 应在 LTS 中配置日志转储。
	启用备份功能并配置备份策略	SQLServer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。
	SQLServer配置合理的安全组规则	安全组是一个逻辑上的分组, 在Cloud SQLServer中, 可以保障数据库的安全性和稳定性。
	确保Cloud SQL Server实例的'user Connections'数据库标志设置为非限制值 (自动执行)	user connections使用此选项有助于避免将服务器重载为过多的并发连接。可以根据系统和用户要求估计连接数。
	确保Cloud SQL数据库实例未分配公网IP (自动执行)	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。如非必要, 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。
	RDS集群快照和数据库快照应启用静态加密	SQLServer中通过启用磁盘加密, 可以提高数据安全性, 但对数据库读写性能有少量影响。
	RDS实例不应使用数据库引擎默认端口	使用默认SQLServer端口容易被监听, 存在安全隐患, 推荐使用非默认端口。

检查子项目	检查项目
RDS 数据库实例应建议默认不开启公共访问	数据库开放EIP后，如果公网上的恶意人员获取到您的EIP DNS和数据库端口，那么便可尝试破解您的数据库并进行进一步破坏。因此，强烈建议您保护好EIP、DNS、数据库端口、数据库账号和密码等信息，并通过RDS for SQL Server实例的安全组限定源IP，保障只允许可信源连接数据库。
启用透明数据加密	在Cloud SQLServer数据库中，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。当前只有2019和2022标准版以及所有企业版支持此功能。
确保数据库实例不绑定公网IP地址	数据库开放EIP后，如果公网上的恶意人员获取到您的EIP DNS和数据库端口，那么便可尝试破解您的数据库并进行进一步破坏。因此，强烈建议您保护好EIP DNS、数据库端口、数据库账号和密码等信息，并通过RDS for SQL Server实例的安全组限定源IP，保障只允许可信源连接数据库。
确保Cloud SQL Server实例的 'contained database authentication'数据库标志未设置 'on' (自动执行)	contained database authentication包括定义数据库所需的所有数据库设置和元数据，它与安装数据库的 数据库引擎 实例没有配置依赖关系。用户可以连接到数据库而无需在 数据库引擎 级别对登录名进行身份验证。
数据库实例应启用静态数据加密	启用SQLServer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。
RDS数据库实例应配置多可用区部署	SQLServer实例部署在不同的可用区，可提高容灾能力。
确保Cloud SQL Server实例的 'external scripts enabled'数据库标志设置为'off' (自动执行)	使用 external scripts enabled 选项可启用包含某些远程语言扩展的脚本在服务器执行。
确保Cloud SQL数据库实例要求所有入向连接使用SSL	如果未启用 SSL 加密连接，那么在客户端和服务器之间为明文形式传输数据，容易受到窃听、篡改和"中间人"攻击。

检查子项目		检查项目
	确保Cloud SQL Server实例不配置 'user options'数据库标志 ( 自动执行 )	user options 选项指定所有用户的全局默认值。将建立一个用户工作会话期间使用的默认查询处理选项的列表。使用 user options 此选项可以更改选项的 SET 默认值。
	RDS数据库集群应配置多可用区部署	SQLServer集群/主备节点部署在不同的可用区，可提高集群/主备实例的容灾能力。
	RDS实例开启慢日志	查询慢日志用来记录执行时间超过当前慢日志阈值“long_query_time”（默认是1秒）的语句，您可以通过慢查询日志的日志明细，查找出执行效率低的语句，进行优化。您也可以下载慢查询日志进行业务分析。
TaurusDB 数据库	TaurusDB实例应开启备份	创建TaurusDB数据库实例时，系统默认开启自动备份策略。实例创建成功后，您可根据业务需要设置自动备份策略。TaurusDB按照用户设置的自动备份策略对数据库进行备份。TaurusDB的备份操作是实例级的，而不是数据库级的。当数据库故障或数据损坏时，可以通过备份恢复数据库，从而保证数据可靠性。由于开启备份会损耗数据库读写性能，建议您选择业务低峰时间段启动自动备份。设置自动备份策略后，会按照策略中的备份时间段和备份周期进行全量备份。实例在执行备份时，按照策略中的保留天数进行存放，备份时长和实例的数据量有关。在进行全量备份的同时系统每5分钟会自动生成增量备份，用户不需要设置。生成的增量备份可以用来将库表数据恢复到指定时间点。
	TaurusDB实例开启慢日志	慢日志用来记录执行时间超过当前慢日志阈值“long_query_time”（默认是10秒）的语句，建议设置为1s，锁等待时间不计算在执行时间内。您可以通过查询慢日志的日志明细、统计分析情况，查找出执行效率低的语句，进行优化。

检查子项目	检查项目
	<p>TaurusDB实例不应绑定弹性公网</p> <p>1、云服务安全特性介绍：TaurusDB实例不应绑定弹性公网IP（EIP，ElasticIP）是一项重要的网络安全最佳实践。TaurusDB作为托管型数据库服务，其设计初衷是部署在私有网络（如VPC）内部，通过内网与其他云资源（如ECS、容器等）安全通信。若为数据库实例绑定弹性公网IP，相当于将其直接暴露在互联网上，极大增加了被外部攻击的风险。云平台通常提供安全组、VPC隔离、私有连接（如Private Link）等机制，确保数据库仅在受控网络中访问，避免公网暴露。</p> <p>2、应对什么样的风险：该要求主要应对以下安全风险：暴力破解风险：数据库端口（如3306）暴露在公网后，极易成为黑客暴力破解、密码爆破的目标。漏洞利用风险：若数据库存在未修复的漏洞（如CVE漏洞），攻击者可通过公网直接发起攻击，导致数据泄露或服务被控。数据泄露风险：公网暴露的数据库可能被扫描工具发现（如Shodan、Censys），一旦认证机制薄弱，可能导致敏感数据大规模泄露。DDoS攻击风险：公网IP可能成为分布式拒绝服务（DDoS）攻击的目标，导致服务不可用。合规风险：等保2.0、GDPR、金融行业规范等均要求核心数据资产不得直接暴露于公网，否则无法通过合规审计。</p> <p>3、如果不满足，有什么影响：数据库面临持续的网络扫描和攻击尝试，安全事件发生概率显著上升。一旦被攻破，可能导致数据被窃取、篡改或勒索加密（如勒索软件）。企业面临声誉损失、客户信任下降，甚至法律追责和监管处罚。增加安全运维压力，需投入更多资源进行入侵检测、日志审计和应急响应。可能触发云平台的安全告警或自动阻断机制，影响业务正常运行。</p> <p>4、如果开启后对业务有负面影响，也请说明：绑定EIP虽然便于远程访问和调试，但应通过更安全的方式替代，而非直接暴露数据库。若因业务需要“开启”公网访问（如临时运维），应注意：短期影响：开发或运维人员可能认为“绑定EIP更方便连接数据库”，但实际上可通过跳板机（堡垒机）、VPN、云专线或数据库代理等方式安全访问，无需直接暴露。误操作风险：一旦绑定</p>

检查子项目		检查项目
		EIP且安全组配置不当，可能长期未被发现，形成“影子资产”，成为安全隐患。替代方案成熟：主流云平台均提供安全的远程访问方案，如华为云的“数据库安全访问服务”或“DAS（数据库自治服务）”支持通过Web客户端安全连接内网数据库，无需公网IP。建议：严禁为TaurusDB实例绑定弹性公网IP。所有数据库访问应通过VPC内网进行，应用服务器与数据库同属一个VPC或通过VPC对等连接互通。运维访问应通过堡垒机、SSH隧道或云平台提供的安全Web客户端实现。配合安全组策略，限制仅允许特定IP或安全组访问数据库端口。通过以上措施，在保障安全性的同时，兼顾运维便利性，实现安全与效率的平衡。
	TaurusDB实例开启审计日志	数据库审计日志是数据库安全管理和运维的重要工具，它能够提供全面的安全监控、满足合规性要求、辅助故障诊断、支持业务分析，并帮助实现有效的风险管控，虽然会带来一定的性能和存储成本，但对保障数据库安全和合规运营具有不可替代的价值。
GeminiDB 数据库	GeminiDB实例开启错误日志	GeminiDB实例的日志管理功能支持查看数据库级别的错误日志，包括数据库运行的Warning和Error级别的信息，有助于您分析系统中存在的问题。
	GeminiDB实例开启备份	GeminiDB支持数据库实例的备份，以保证数据可靠性。实例删除后，手动备份数据保留。自动备份的数据和实例一起释放，备份的数据不支持下载导出。强烈建议您配置合适的自动备份策略，防止客户误操作或者服务异常的情况下，因没有开启备份而造成数据丢失的情况。
	不应使用GeminiDB开源Cassandra、Influx引擎的默认端口	使用默认端口容易被监听，存在安全隐患，推荐您使用非默认端口。Redis的默认端口号是6379；Cassandra的默认端口号是7199；Influx的默认端口号是8086；Mongo的默认端口号是27017。其中Cassandra、Influx默认不能为社区默认端口，Redis需要为默认端口。

检查子项目		检查项目
	GeminiDB实例支持多可用区	可用区指在同一区域下，电力、网络隔离的物理区域，可用区之间网互通，不同可用区之间物理隔离。目前支持将实例部署在单可用区或3可用区。业务有跨可用区容灾需求或业务对跨可用区延时不敏感，推荐使用多可用区，主节点和只读节点可以跨可用区部署，以获得更高的可用性和可靠性。
	GeminiDB实例开启慢查询日志	GeminiDB实例的日志管理功能支持查看数据库级别的慢日志，执行时间的单位为ms。通过该日志，可查找出执行效率低的语句，以便优化。
数据复制服务 DRS	DRS实时迁移任务不使用公网网络	实时迁移是指在数据复制服务能够同时连通源数据库和目标数据库的情况下，只需要配置迁移的源、目标数据库实例及迁移对象即可完成整个数据迁移过程，再通过多项指标和数据的对比分析，帮助确定合适的业务割接时机，实现最小化业务中断的数据库迁移。详见迁移方案概览。尽量不使用EIP网络，采用VPN等安全网络进行数据传输，通过防火墙、安全组、ACL规则等网络配置，减少攻击面，提升数据同步网络的安全性。详见安全最佳实践。
	DRS实时灾备任务不使用公网网络	DRS服务启用灾备任务时尽量不使用公网网络，采用VPN等安全网络进行数据传输，通过防火墙、安全组、ACL规则等网络配置，减少攻击面，提升数据同步网络的安全性。详见安全最佳实践。
	DRS实时同步任务不使用公网网络	数据复制服务的实时同步任务旨在通过同步技术，在不同的系统之间将数据从一个数据源实时拷贝到其他数据库，并确保数据的一致性，实现关键业务数据的实时流动。为了保障数据同步的安全性和效率，实时同步任务不应使用公网网络。公网网络可能存在延迟、带宽限制和安全隐患，这会影响数据同步的性能和可靠性。通过使用私有网络或专用连接来进行数据同步，可以有效减少网络不稳定因素对数据传输的影响，并加强数据安全性，防止敏感信息在公网传输过程中遭遇潜在威胁。尽量不使用EIP网络，采用VPN等安全网络进行数据传输，通过防火墙、安全组、ACL规则等网络配置，减少攻击面，提升数据同步网络的安全性。详见安全最佳实践。

检查子项目		检查项目
文档数据库服务 DDS	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DDS数据库中的配置，是否开通公网连接方式。

## 华为云安全配置基线 3.0—存储

表 7-19 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。

检查子项目		检查项目
	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，防止对象数据泄露。
	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。
	确保禁用ACL，并使用OBS存储桶策略实现更精细的访问控制	OBS提供多种权限控制方式，包括IAM权限、桶策略、对象ACL、桶ACL。访问控制列表（Access Control List, ACL）用于资源所有者给其他账号授予资源的访问权限。OBS ACL是基于账号级别的读写权限控制，且主要用于授予基本的读/写权限，权限控制细粒度不如桶策略和IAM权限。一般情况下，建议使用IAM权限和桶策略进行访问控制。否则会泄露权限配置规则及相应的domain id, domain name。在特定的权限配置场景下，攻击者可能会根据泄露的权限配置规则，构造请求非法操作桶内资源。
	配置监控OBS桶策略变更的事件监控告警	CES配置监控OBS桶策略变更的事件监控告警，旨在帮助用户实时监控和响应对云存储资源的安全操作，特别是针对OBS桶策略变更的事件。通过事件监控功能，用户能够收集和上报业务中的关键事件及对云资源的操作记录，一旦发现OBS桶策略发生变更，系统会立即触发告警并通知用户，帮助用户及时进行干预，确保数据存储的安全性和合规性。该服务主要应对对象存储桶策略的误配置或恶意修改，可能导致数据泄露、权限滥用或资源滥用等风险。因此，应确保CES配置监控OBS桶策略变更的事件监控告警。
	通用存储桶应禁止公共写访问	通过桶策略，桶的拥有者可以向IAM用户或其他账户授予对桶及其对象的操作权限。访问控制列表（ACL）是一个规则列表，用于指定授予或拒绝哪些用户或系统对特定存储桶或对象的访问权限。

检查子项目		检查项目
	OBS生命周期规则，数据自动清理	OBS支持设置桶的生命周期规则，自动转换对象的存储类别，删除过期的对象，从而有效地利用存储特性，优化存储空间。可以根据前缀设置多条生命周期规则。
	通用存储桶应禁止公共读访问	通过桶策略，桶的拥有者可以向IAM用户或其他账户授予对桶及其对象的操作权限。访问控制列表（ACL）是一个规则列表，用于指定授予或拒绝哪些用户或系统对特定存储桶或对象的访问权限。
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。
	确保SFS Turbo文件系统最近一次备份距离现在不超过指定时间	云备份（CBR）可以为SFS Turbo文件系统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。当备份的时间间隔过大时，数据丢失风险增加：如果在两次备份之间发生了数据损坏或丢失的情况，那么从最近一次备份恢复时，会丢失这段时间内的所有更改和新增数据。这可能对业务造成严重影响。
	确保SFS Turbo文件系统在备份存储库中	云备份（CBR）可以为SFS Turbo文件系统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。
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。

检查子项目		检查项目
	<p>确保开启存储库中的备份策略</p>	<p>需要对备份对象执行自动备份操作时，可以设置备份策略。通过在策略中设置备份任务执行的时间、周期以及备份数据的保留规则，将备份存储库绑定备份策略，可以为存储库执行自动备份。备份策略需要绑定存储库才可以生效，若存储库未执行备份，确保绑定的备份策略状态为开启，防范数据丢失风险（如误删除、硬件故障）和业务中断风险，确保关键数据可恢复，满足合规性要求（如等保2.0）。若未开启备份策略，可能导致备份缺失，数据损坏或丢失后无法恢复，业务连续性受损，且可能违反数据保护法规。开启备份策略后：</p> <ol style="list-style-type: none"> <li>1、存储成本增加：频繁备份可能占用更多存储空间，需合理规划保留周期。</li> <li>2、资源占用：备份任务可能轻微影响I/O性能，但对业务运行无显著影响。</li> </ol>

检查子项目		检查项目
	建议开启CBR存储库备份锁定功能	<p>备份锁定功能是指将备份数据置为WORM（一次写入，多次读取）状态。开启该功能后，存储库中的所有备份都将进入WORM状态。处于WORM状态的备份数据，任何用户都不能提前删除。主要防范勒索软件攻击、内部误操作或恶意删除，确保备份数据在关键恢复点（如被加密前）始终可用。备份数据可能被篡改或删除，导致灾难恢复失败，业务连续性受损，且无法满足数据保护合规要求。开启备份锁定后，会有如下影响：</p> <ol style="list-style-type: none"> <li>1、该功能无法关闭，请谨慎操作。开启后如果存储库容量已满，由于无法提前删除备份，可能会导致资源备份失败。</li> <li>2、绑定的资源无法解绑和迁移资源。</li> <li>3、策略生成的备份只支持过期自动删除，不支持手动删除。</li> <li>4、如果有备份副本，对于按需购买的存储库不允许删除，对于包周期购买的存储库支持退订。</li> <li>5、修改存储库绑定的策略时，只能选择当前保留类型或修改为按照时间的保留类型。如策略的保留规则为按数量保留时，则保留数量不允许减少。</li> <li>6、新创建的开启备份锁定的存储库，仅支持绑定保留规则为按时间保留的备份策略。</li> <li>7、开启备份锁定后，存储库仅支持重新绑定保留规则为按时间保留的备份或复制策略。</li> </ol>
	确保ECS资源开启备份功能	<p>ECS实例没有关联备份存储库，视为“不合规”。云备份（CBR）可以为云服务器、云硬盘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。详见云备份概述。相比数据丢失后的恢复，备份的成本更低。</p>

检查子项目		检查项目
	建议CBR存储库备份库有足够长的备份保留周期	<p>确保备份保留时间足够长。防止需要使用备份进行业务恢复时，备份被过早清理，满足数据可恢复性和合规性要求。主要防范因备份保留周期过短导致数据无法恢复的风险，例如误删、恶意删除或自动化策略误清理关键备份，影响业务连续性。CBR备份保留日期过短可能导致备份被提前删除，灾难恢复时无可用备份，业务中断风险增加，且可能违反数据保留法规（如金融、医疗行业）。</p> <p>潜在影响：</p> <ol style="list-style-type: none"> <li>1、存储成本增加：长期保留备份会占用更多存储空间，需平衡成本与安全性。</li> <li>2、管理复杂度：需定期检查保留策略，避免因保留过多备份导致存储库容量不足。</li> </ol>
	确保ECS云服务区在指定周期内创建备份	<p>ECS实例最近一次备份创建时间超过参数要求，视为“不合规”。云备份（CBR）可以为云服务器、云硬盘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。详见云备份概述。当备份的时间间隔过大时，数据丢失风险增加：如果在两次备份之间发生了数据损坏或丢失的情况，那么从最近一次备份恢复时，会丢失这段时间内的所有更改和新增数据，这可能对业务造成严重影响。</p>

检查子项目		检查项目
	建议CBR存储库开启多AZ备份	<p>CBR支持创建多AZ存储库，将备份数据存储到同区域的多个AZ。当某个AZ不可用时，仍然能够从其他AZ正常访问数据，适用于对可靠性要求较高的场景。主要防范单AZ故障（如硬件损坏、电力中断等）导致备份数据不可用，确保业务连续性，满足金融、医疗等行业的高可用性要求。若仅单AZ存储，一旦该AZ故障，可能导致备份数据无法访问，影响灾难恢复能力，增加业务中断风险。</p> <p>潜在影响：</p> <ol style="list-style-type: none"> <li>1、存储成本略增：多AZ存储会占用额外空间，但相比数据丢失风险可接受；</li> <li>2、备份/恢复延迟：跨AZ同步可能轻微增加备份时间，但对业务影响有限。约束限制：                     <ol style="list-style-type: none"> <li>a、暂不支持更换已创建存储库的备份数据冗余策略。</li> <li>b、暂不支持将已创建的备份副本迁移至多AZ备份存储库中。</li> <li>c、复制存储库暂不支持多AZ备份冗余策略。</li> <li>d、启用后不支持修改</li> </ol> </li> </ol>
	建议CBR备份策略执行频率不低于最小频率	<p>华为云CBR支持配置最小备份频率策略，通过策略引擎强制要求备份周期（如每天/每周），确保关键数据定期保护，避免备份遗漏。应对风险：防范因备份间隔过长导致的数据丢失风险（如系统故障时丢失过多增量数据），满足RPO（恢复点目标）要求，确保业务数据可回溯。若不满足：可能导致备份间隔超出安全阈值，故障时丢失大量未备份数据，延长恢复时间，违反行业合规性要求（如等保）。潜在影响：</p> <ol style="list-style-type: none"> <li>1、资源消耗：高频备份增加存储和计算负载；</li> <li>2、性能波动：备份时可能短暂影响业务I/O性能。</li> </ol>

## 华为云安全配置基线 3.0—企业智能

表 7-20 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。
	确保通过安全组和VPC限制公网访问	华为云DWS服务支持安全组和虚拟私有云（VPC）的配置，通过安全组规则可以控制DWS实例的入站和出站流量，而VPC则提供了一个隔离的虚拟网络环境，确保DWS实例只能在特定的网络范围内被访问。这种配置能够有效限制公网访问，防止未经授权的访问。DWS服务通常处理大量敏感数据，如果公网访问没有被适当限制，攻击者可能利用漏洞或弱密码等手段入侵DWS实例，导致数据泄露、数据篡改或数据删除等安全事件。此外，未授权的访问还可能导致服务被滥用，影响业务的正常运行。如果不通过安全组和VPC限制公网访问，DWS实例将暴露在互联网上，面临更高的安全风险。

检查子项目		检查项目
	确保开启DWS数据库审计日志	DWS（数据仓库服务）支持数据库审计日志功能，可以记录用户对数据库的访问行为、SQL操作、权限变更等关键事件。通过开启审计日志功能，可以有效追踪和分析数据库的操作历史，及时发现和应对潜在的安全威胁。该规则旨在应对以下风险：未开启审计日志功能可能会导致无法追踪和监控数据库的操作行为。攻击者可能利用未审计的环境进行未授权的访问或恶意操作，进而窃取敏感数据或破坏数据库的完整性。此外，内部人员的误操作或恶意行为也可能导致数据泄露或损坏，而无法追溯。如未开启审计日志功能，可能会导致以下影响：无法追踪和分析数据库的操作行为，增加数据泄露和篡改的风险。此外，无法及时发现和应对潜在的安全威胁，影响数据库的稳定性和数据的完整性。审计日志的生成和存储可能会占用额外的存储空间，增加存储成本。
	确保已开启DWS数据库审计日志转储	DWS（数据仓库服务）具备审计日志转储功能，该功能能够记录用户对数据库的所有操作行为，包括查询、修改、删除等，并将这些日志转储到指定的存储系统（如OBS对象存储服务）。通过审计日志转储，可以有效应对未经授权的数据访问、潜在的安全威胁以及内部人员的不当操作风险。如果不开启审计日志转储，将无法及时发现和追踪数据库的异常操作，可能导致数据泄露、篡改或删除等安全事件，影响业务的合规性和数据的完整性。在开启审计日志转储后，可能会对存储资源和网络带宽产生一定影响，因此建议根据实际需求合理配置日志转储策略。

检查子项目		检查项目
	确保DWS集群启用自动快照	华为云DWS服务支持自动快照功能，能够定期自动创建集群的数据备份。这些快照可以用于在集群发生故障或数据损坏时，快速恢复数据，确保业务的连续性。通过启用自动快照，用户可以有效保护数据，防止数据丢失。如果DWS集群没有启用自动快照，则DWS集群将无法自动创建数据备份。一旦发生硬件故障、人为错误或恶意攻击导致数据丢失，将无法快速恢复数据，导致业务中断和数据损失。此外，缺乏定期备份还可能导致数据无法恢复到最近的稳定状态，增加数据丢失的风险。虽然自动快照提供了数据保护，但频繁的快照创建可能会占用更多的存储空间，增加存储成本。
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，还可以提供更安全更安全的资源隔离能力。
	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。

检查子项目		检查项目
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。
	确保MRS集群节点未绑定公网IP	弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。为MRS集群绑定弹性公网IP后，集群直接暴露在公网上，因此如非必需，MRS集群不建议绑定弹性公网IP，以减少攻击面降低敏感数据泄露风险。
应用与数据集成平台 ROMA	ROMA建立网络分段边界，通过网络控制措施	租户资源隔离，租户使用自建VPC保证不同实例间网络隔离。
	确保ROMA APIC使用安全协议版本	用户开放API，数据传输通道支持安全加密协议，保障数据安全传输，避免数据泄露。
	ROMA API授权使用安全鉴权方式	用户开放API，需要保证API权限安全，保证鉴权通过才能访问API。如果配置为“无认证”，允许所有用户调用，不符合安全要求。
	非面向客户的API必须限制可访问IP地址范围	开放API需要配置访问控制策略，保证API在可控访问内为可见状态。保障API安全。
函数工作流 FunctionGraph	FunctionGraph函数应该打标签进行分类	在VPC内部署资源能够提供更高的安全性和对网络配置的控制。
	FunctionGraph数据加密存储	用户环境变量通常包含敏感信息，为防止敏感信息泄露，应该使用加密环境变量存储。

检查子项目		检查项目
	启用 FunctionGraph 函数日志功能	开启函数日志功能后，用户函数每次调用执行日志都会保存在 LTS，方便用户定位问题和记录函数执行过程。
	FunctionGraph 函数需要部署在 VPC 内	使用标签可以按目的，环境或某个标准对函数进行分类进行管理，并且可以在 IAM 授权策略中针对标签进行权限控制。
	确保 FunctionGraph 函数不能访问公网	函数工作流的函数开启“函数访问公网”的开关，视为“不合规”。函数创建成功后，默认具有公网访问权限，即函数可直接访问公网上的服务，存在数据泄露的风险。
云桌面 Workspace	Workspace 资源应开启备份存储库	云桌面支持备份存储库功能，当发生病毒入侵、人为误删除、软硬件故障等事件时，可通过 CBR 的备份服务将云桌面的数据恢复至任意备份点。备份恢复过程中，CBR 会保障用户数据的安全性和正确性，确保业务安全。
	Workspace 应设置合理的备份周期	云桌面使用云备份服务中的“云桌面备份”功能进行桌面备份。保障用户数据的安全性和正确性，确保业务安全。当备份的时间间隔过大时，数据丢失风险增加：如果在两次备份之间发生了数据损坏或丢失的情况，那么从最近一次备份恢复时，会丢失这段时间内的所有更改和新增数据。这可能会对业务造成严重影响。
云搜索服务 CSS	CSS 集群开启慢日志	Elasticsearch 和 OpenSearch 集群备份的日志文件主要包括废弃操作日志、运行日志、慢索引日志、慢查询日志，用户可以使用日志定位问题。CSS 集群默认记录慢日志，建议保持开启，并将其转储在 OBS 桶中进行备份。
	CSS 集群至少包含 3 个数据节点	为防止数据丢失，并确保在服务中断情况下能降低集群的停机时间，从而增强集群的高可用性，请确保 CSS 集群的实例个数大于 2 个。部署至少 3 个实例，可以确保当一个节点发生故障时，集群能够正常运行。

检查子项目		检查项目
	CSS集群应关闭公网访问和Kibana公网访问能力	避免将CSS集群部署在公网或者DMZ里，应该部署在公司内部网络，并使用路由器或者防火墙技术把集群保护起来，避免通过直接绑定弹性公网IP（简称EIP）的方式从互联网访问集群，防止未授权的访问及DDoS攻击等。为避免公网暴露风险，建议关闭集群的公网访问，如果业务必须通过公网访问，请配置独享型负载均衡访问CSS集群，并严格配置独享型负载均衡器的安全组规则限制。
	CSS集群应启用快照	为避免数据丢失，您可以将集群的索引数据进行备份，当数据发生丢失或者想找回某一时间段数据时，您可以通过恢复索引操作快速获得数据。索引的备份是通过创建集群快照实现。第一次备份时，建议将所有索引数据进行备份。CSS服务的快照备份功能提供数据保护和恢复能力。通过快照备份，可以将集群的数据状态保存到OBS桶中，以便在需要时进行恢复。CSS集群快照分为两种方式：自动创建快照和手动创建快照。影响：当使用快照备份功能时，备份的快照存储在OBS桶中需要额外收费。集群快照会导致CPU、磁盘IO上升等影响，建议在业务低峰期进行操作。
	CSS集群应启用HTTPS	CSS集群的安全模式下可以选择使用HTTP协议或者HTTPS协议。安全模式+HTTP协议的集群采用HTTP协议明文传输数据，优点是安全认证提升了集群安全性。通过HTTP协议访问集群又能保留集群的高性能。支持用户权限隔离。缺点是不支持启用公网访问。适合对安全性有一定要求，但对性能要求较高的场景。安全模式+HTTPS协议的集群采用HTTPS协议进行通信加密，使数据更安全。优点是安全认证提升了集群安全性。HTTPS协议提升了集群公网访问的安全性。支持用户权限隔离。缺点是与HTTP协议相比，通过HTTPS协议访问集群会因加密和解密操作导致集群的读写性能有所下降。适合对安全性和数据传输加密要求较高、且需要公网访问的场景。在对性能要求不高、且需要公网访问的场景，建议使用安全模式+HTTPS模式协议。

检查子项目		检查项目
	确保CSS集群多AZ部署	<p>可用区（Availability Zone, AZ）指在同一区域（Region）下，电力、网络隔离的物理区域。同一地域内的可用区之间通过内网互通，但彼此在物理层面保持隔离，以降低单点故障风险。多可用区部署是CSS服务提供的高可用性解决方案。通过在同一个地域内选择2个或3个不同的可用区部署集群，可有效防止数据丢失并降低服务中断风险。为防止数据丢失，并确保在服务中断情况下能降低集群的停机时间，从而增强集群的高可用性，CSS服务支持跨可用区（即多可用区）部署。创建集群时，如果选择多可用区部署，CSS服务会自动启用跨AZ高可用特性，确保节点在所选可用区中均匀分布（各AZ的节点数量差异不超过1）。多可用区部署时，建议优先选择3个可用区，而非2个可用区。当仅选择2个可用区时，如果其中一个可用区发生故障，可能导致无法选举Master节点，从而引发集群不可用风险。影响：在创建集群时，选择的任意类型的节点数需大于或等于所选AZ数，否则跨可用区部署会失败。当集群中数据节点数或冷数据节点数和可用区数不是整数倍关系时，集群的数据分布可能会不均匀，从而影响数据查询或写入业务。</p>

## 华为云安全配置基线 3.0—应用中间件

表 7-21 应用中间件风险项检查项目

检查项目		检查内容
API网关 APIG	API配置SSL证书用于后端双向认证	用户开放API，需要保证API网关和后端服务在通信过程中互相验证对方的身份，防止未授权访问和中间人攻击。
	API配置链路追踪	API开启链路追踪，通过接入APM，提供完整的调用链及业务拓扑。
	确保APIG专享版实例不对公网开放	建议您不要直接为APIG实例绑定EIP，通过直接EIP的访问会导致后端服务暴露在公网的威胁之中。如您的业务场景需要绑定EIP开放公网访问，请参考“使用WAF对APIG进行安全防护”开通WAF并启用对APIG的安全防护。

检查项目		检查内容
	API授权使用安全认证方式	用户开放API，需要保证API权限安全，认证通过才能访问API。如果配置为“无认证”，允许所有用户调用，不符合安全要求。
	API网关配置WAF进行安全保护	为了保护APIG及后端服务器免受恶意攻击，可在APIG和外部网络之间部署WAF。此项能力为WAF提供，需要订购WAF服务。
	确保APIG专享版实例配置访问日志	APIG提供了API的可视化分析和统计能力，支持查看API的调用日志。可以带来如下好处： 异常检测：通过审计日志，识别异常访问行为，如频繁失败请求、异常IP等，及时发现潜在攻击； 问题定位：通过日志快速定位API调用失败的原因，如参数错误、服务不可用等； 用户行为分析：分析API调用模式，了解用户行为，支持产品优化； 资源使用监控：监控API调用频率和资源消耗，防止资源浪费。
分布式缓存服务Redis版	应配置DCS Redis实例不存在弹性公网IP	DCSRedis实例禁止绑定弹性公网IP，主要利用VPC网络的内生安全隔离特性，强制实例仅通过私有网络通信，从网络层彻底规避公网暴露风险。此配置直接应对互联网侧的高危攻击风险，若Redis实例绑定EIP，将直接暴露于公网扫描与暴力破解，或遭遇DDoS攻击导致服务不可用。若不满足此要求，一旦攻击者通过公网入侵实例，可能窃取敏感数据、植入恶意程序或清空数据库，引发数据泄露与服务瘫痪。禁用EIP对业务负面影响，需确保客户端均通过同VPC或VPN/专线等安全通道访问，公网用户需经前端代理中转，可能增加架构复杂度。
	应配置RDS Redis实例端口检查	DCSRedis实例配置端口检查，主要通过修改默认端口规避自动化扫描攻击，大幅降低实例被恶意探测发现的概率。若使用默认端口，攻击者可快速定位Redis实例并发起未授权访问、暴力破解或漏洞利用。若不满足此要求，一旦实例暴露于风险网络，将导致数据被窃取、服务遭瘫痪。修改默认端口对业务负面影响，仅需客户端同步更新连接端口配置。

检查项目		检查内容
分布式消息服务 RabbitMQ版	应关闭DMS RabbitMq实例公网访问	应关闭DMS RabbitMq实例公网访问，这是云服务基础网络隔离安全特性，通过禁止公网暴露强制仅允许内网/VPC访问，应对外部恶意扫描、未授权访问及数据窃取风险。若实例暴露在公网上，实例面临直接攻击导致数据泄露或服务中断，且违反等保、GDPR等合规要求；开启后负面影响为依赖公网的业务若不经修改，将无法访问到该实例。
分布式消息服务 RocketMQ版	应关闭DMS RocketMQ实例公网访问	应关闭DMS RocketMQ实例公网访问，这是云服务的关键网络隔离安全特性，通过禁止从互联网直接访问实例，强制仅允许VPC内网或白名单IP接入，从而应对外部恶意扫描、未授权访问及暴力破解风险。若不满足此配置，实例暴露于公网可能导致数据被窃取、服务遭攻击入侵，同时违反等保2.0或GDPR等合规要求；关闭公网访问后，主要负面影响是依赖公网调用的外部系统将无法直连。
分布式消息服务 Kafka版	应关闭DMS Kafka队列公网访问	应关闭DMSKafka队列公网访问，旨在通过限制服务仅可通过内网私有网络访问，而非暴露在公共互联网上，从而构建隔离边界并减少攻击面，有效应对未经授权的外部访问、数据窃取和恶意攻击风险。如果不满足此配置，服务暴露在公网下可能导致敏感数据泄露；然而，开启后对业务可能造成负面影响，如影响依赖公网API调用的外部集成系统，需额外设置VPN、专线或代理网关来维持连接，增加架构复杂性和延迟。

## 华为云安全配置基线 3.0—开发与运维

表 7-22 开发与运维风险项检查项目

检查项目		检查内容
云应用引擎 CAE	CAE创建环境时需选择不同VPC进行网络隔离	建议客户通过业务划分环境，建立网络边界。
	建议敏感数据托管到DEW，CAE通过DEW获取使用，确保敏感数据不泄露	建议密码等通过dew配置，防止敏感信息泄露。

检查项目		检查内容
	CAE日志信息应发送至LTS	CAE提供了日志采集的功能，当前只支持日志采集到LTS，可以配置日志采集路径，高级设置可配置单行日志或者多行合并为一行，默认为单行日志。
	升级CAE组件镜像版本防止使用过低的镜像版本	客户如果使用旧版本可能会涉及开源镜像的漏洞。
	建议CAE应用组件七层访问使用HTTPS协议，确保数据传输过程中不被窃取和破坏	建议客户配置HTTPS的访问方式。

## 华为云安全配置基线 3.0—CDN 与智能边缘

表 7-23 CDN 与智能边缘风险项检查项目

检查项目		检查内容
CDN与智能边缘	应确保CDN回源方式使用HTTPS	如果CDN节点没有缓存该资源，就会回源请求资源并缓存到CDN节点。回源协议也应当设置为HTTPS以确保数据传输的安全。
	应确保配置安全的TLS版本	传输层安全性协议（TLS: Transport Layer Security），是一种安全协议，目的是为互联网通信提供安全及数据完整性保障，最典型的应用就是HTTPS。目前，有四个版本的TLS协议：TLS1.0/1.1/1.2/1.3，版本越高，安全性相对更高，但是对老版本的浏览器兼容性相对较差。

## GDPR-第三方披露

表 7-24 第三方披露风险项检查项目

检查项目	检查内容
您作为数据控制者，在将数据披露、公开给第三方之前是否告知数据主体并获取数据主体同意。	您作为数据控制者，在将数据披露、公开给第三方之前是否告知数据主体并获取数据主体同意。 检查所有向第三方披露、公开个人数据的场景，数据披露、公开之前是否告知数据主体并获取数据主体同意。

检查项目	检查内容
<p>当您作为数据控制者委托第三方处理个人数据时，是否与第三方签署了合同协议（数据处理协议DPA），明确第三方作为数据处理者的责任和义务。</p>	<p>当您作为数据控制者委托第三方处理个人数据时，是否与第三方签署了合同协议（数据处理协议DPA），明确第三方作为数据处理者的责任和义务。</p> <p>检查是否通过合同协议在以下方面明确作为数据处理者的责任与义务：</p> <ul style="list-style-type: none"> <li>● 处理的个人数据的类型。</li> <li>● 数据处理的目的和性质。</li> <li>● 数据处理的责任和义务界定。</li> <li>● 数据处理的方式、保留期限、存储位置。</li> <li>● 数据处理的安全保护措施。</li> <li>● 数据子处理者的存在。</li> <li>● 数据主体类型。</li> <li>● 数据处理的法律约束。</li> </ul>
<p>您作为数据控制者或数据处理者，向第三方披露个人信息时，是否通过合同协议约束第三方或联合控制者的角色责任和数据处理措施，并在披露个人信息的第三方发生变更时及时做出响应。</p>	<p>您作为数据控制者或数据处理者，向第三方披露个人信息时，是否通过合同协议约束第三方或联合控制者的角色责任和数据处理措施，并在披露个人信息的第三方发生变更时及时做出响应。</p> <ul style="list-style-type: none"> <li>● 检查是否通过合同协议约束第三方或联合控制者的角色责任和数据处理措施。</li> <li>● 检查在第三方或联合控制者发生变更时，是否存在以下机制： <ul style="list-style-type: none"> <li>- 作为数据控制者时，应重新获取个人信息主体的同意。</li> <li>- 作为数据处理者时，应重新获取数据控制者正式授权。</li> </ul> </li> </ul>
<p>若您在数据处理活动中承担数据处理者角色，是否建立机制，在第三方请求贵公司披露个人信息时通知数据控制者。</p>	<p>在数据处理活动中承担数据处理者角色，在第三方请求披露个人信息时是否通知数据控制者。</p>
<p>对于将个人数据披露/公开给第三方的场景，您作为数据控制者是否提供将更正、清除个人数据或限制处理的信息告知第三方的机制。</p>	<p>对于将个人数据披露/公开给第三方的场景，您作为数据控制者是否提供将更正、清除个人数据或限制处理的信息告知第三方的机制。</p> <ul style="list-style-type: none"> <li>● 检查是存在第三方披露的场景。</li> <li>● 检查是否存在告知第三方进行数据同步的机制。</li> </ul>

## GDPR-数据跨境转移

表 7-25 数据跨境转移风险项检查项目

检查项目	检查内容
您的业务涉及数据跨境时，是否有完整的流程和制度来确保数据跨境满足GDPR要求。	检查是否通过制度规范数据跨境流程，并安排相关人员审核相关文档，监督流程实施。
当您的业务涉及数据跨境时，您是否考虑对个人数据进行过滤或匿名化处理，确保不能以任何方式还原个人数据，再按照非个人数据跨境传输。	<p>当您的业务涉及数据跨境时，您是否考虑对个人数据进行过滤或匿名化处理，确保不能以任何方式还原个人数据，再按照非个人数据跨境传输。</p> <ul style="list-style-type: none"> <li>• 检查在不影响业务的情况下是否可以将个人数据进行过滤和匿名化处理。</li> <li>• 检查是否对个人数据进行过滤和匿名化处理。</li> </ul>
当您的业务涉及个人数据跨境时，您是否满足数据传入方所在国家列属于欧盟委员会在其网站上公布的充分性决议清单中的要求。	<p>当您的业务涉及个人数据跨境时，您是否满足数据传入方所在国家列属于欧盟委员会在其网站上公布的充分性决议清单中的要求。</p> <ul style="list-style-type: none"> <li>• 检查数据传入方所在国家是否属于欧盟委员会在其网站上公布的充分性决议清单中。</li> <li>• 检查是否有数据传输过程是否安全可控，并保留相关记录。</li> </ul>
当您的业务涉及个人数据跨境时且数据传入方所在国家不属于欧盟委员会在其网站上公布的充分性决议清单中，您是否提供适当的保障措施并为数据主体提供可执行的权利与有效的法律救济措施。	<p>当您的业务涉及个人数据跨境时且数据传入方所在国家不属于欧盟委员会在其网站上公布的充分性决议清单中，您是否提供适当的保障措施并为数据主体提供可执行的权利与有效的法律救济措施。</p> <ul style="list-style-type: none"> <li>• 检查是否根据签署数据保护标准条款（SCC）来提供适当的保障。</li> <li>• 检查第三国法律是否会影响SCC的有效性，采取适当的补充措施保证可以提供适当的保障。</li> <li>• 检查是否有数据传输过程是否安全可控，并保留相关记录。</li> </ul>

检查项目	检查内容
当您的业务涉及数据跨境时且数据传入方所在国家不属于欧盟委员会在其网站上公布的充分性决议清单中，以及缺乏适当保障的情况下，数据的跨境传输是否满足GDPR要求。	<p>当您的业务涉及数据跨境时且数据传入方所在国家不属于欧盟委员会在其网站上公布的充分性决议清单中，以及缺乏适当保障的情况下，数据的跨境传输是否满足GDPR要求。</p> <ul style="list-style-type: none"> <li>检查是否存在数据跨境前获取数据主体单独同意的机制。</li> <li>检查是否有数据传输过程是否安全可控，并保留相关记录。</li> </ul>
您作为数据处理者，主动将数据跨境转移，需获得数据控制者的同意。	<p>您作为数据处理者，主动将数据跨境转移，需获得数据控制者的同意。</p> <p>检查在数据跨境相关流程中是否存在获取数据控制者同意的机制。</p>

## GDPR-数据使用，保留和处置

表 7-26 数据使用，保留和处置风险项检查项目

检查项目	检查内容
您在收集个人信息时是否仅收集与处理目的相关且必要的个人数据，个人数据收集范围、使用目的不得超出隐私声明和用户协议，符合最小化原则。	<p>您在收集个人信息时是否仅收集与处理目的相关且必要的个人数据，个人数据收集范围、使用目的不得超出隐私声明和用户协议，符合最小化原则。</p> <p>检查在收集个人信息时是否已遵循最小化原则，收集个人信息的最小化原则包括：</p> <ul style="list-style-type: none"> <li>收集个人信息的类型仅为实现产品或服务功能所必须的。</li> <li>收集个人信息的频率仅为实现产品或服务功能所必须的最低频率。</li> <li>收集个人信息的数量要控制在满足目的范围内的最少数量。</li> </ul>
您在处理特殊类型个人数据及社保号、身份证号、银行卡号、护照号时，是否采用比普通个人数据更高级别的安全措施进行保护。	<p>您在处理特殊类型个人数据及社保号、身份证号、银行卡号、护照号时，是否采用比普通个人数据更高级别的安全措施进行保护。</p> <ul style="list-style-type: none"> <li>检查是否存在处理特殊类型个人数据的场景。</li> <li>检查针对特殊类型数据是否采取了严格的安全措施，比如加密保存传输，访问控制等。</li> </ul>

检查项目	检查内容
对于收集和处理个人数据的系统，您是否提供个人数据备份和恢复的机制，能够恢复系统中存储的个人数据。	对于收集和处理个人数据的系统，您是否提供个人数据备份和恢复的机制，能够恢复系统中存储的个人数据。 检查系统是否提供个人数据备份和恢复机制。
您是否对高风险场景进行识别（特殊个人数据处理，批量个人数据）通过实施技术措施，以确保数据在传输的真实性、保密性和完整性。	您是否对高风险场景进行识别（特殊个人数据处理，批量个人数据）通过实施技术措施，以确保数据在传输的真实性、保密性和完整性。 <ul style="list-style-type: none"><li>检查是否采取技术措施确保数据传输时的真实性、保密性和完整性，技术措施包括但不限于以下：<ul style="list-style-type: none"><li>在通信前对通信双方进行认证，确保通信的真实。</li><li>使用安全的协议（包括TLS、IPSec、SSH等），确保协议支持安全的版本与配置</li></ul></li><li>检查是否有禁止使用不安全的协议：SSL2.0，SSL3.0，TLS1.0，TLS1.1，SSHv1，IKEv1等。</li></ul>
系统的默认设置是否保护隐私。	系统的默认设置是否保护隐私。 检查系统所有默认设置，是否选择最安全的选项。比如： <ul style="list-style-type: none"><li>如匿名化、假名化、加密等应默认设置成开启状态。</li><li>一些非基本业务的隐私敏感功能应默认关闭，如人脸识别。</li><li>如果处于非保护状态可能导致数据主体隐私的泄露或造成其他损失。数据主体对于客户有明确要求或者符合业界惯例的情况，可以按照客户要求或业界惯例执行，其中对于客户的明确要求，应该将该要求提交客户需求管理流程（例如合同提交到合同评审流程），并按照流程评审结果执行。</li></ul>
对于个人数据公开、共享的场景，是否使用假名化、匿名化等技术降低个人数据重标识或泄露的风险。	对于个人数据公开、共享的场景，是否使用假名化、匿名化等技术降低个人数据重标识或泄露的风险。
对于收集和处理个人数据的系统，须提供最终用户对个人数据的访问控制机制。	对于收集和处理个人数据的系统，须提供最终用户对个人数据的访问控制机制。 检查所有访问个人数据的接口是否存在合适的认证和鉴权机制。

检查项目	检查内容
对于收集和处理个人数据的系统中，是否对数据主体对个人数据的操作进行日志记录。	对于收集和处理个人数据的系统中，是否对数据主体对个人数据的操作进行日志记录。 检查是否对个人数据的操作进行日志记录。
您是否提供假名化或加密的机制对个人数据进行保护。	您是否提供假名化或加密的机制对个人数据进行保护。 <ul style="list-style-type: none"> <li>检查系统是否提供假名化或加密机制。</li> <li>检查个人数据是否假名化或加密传输和存储。</li> </ul>
是否可以通过DPIA来证明您满足GDPR要求。	是否可以通过DPIA来证明您满足GDPR要求。 <ul style="list-style-type: none"> <li>建议进行数据保护影响评估（DPIA）。</li> <li>检查是否建立与监管机构进行咨询的具体机制，如果DPIA表明数据处理将会给数据主体的个人数据安全带来较高风险，则控制者应当在进行数据处理之前与监管机构进行协商和咨询。</li> </ul>
您作为数据控制者，是否对涉及其决策对自然人产生法律影响或类似重大影响的用户画像、大规模系统监控、大规模敏感数据处理、数据跨境转移、向第三方披露等业务场景，进行数据保护影响评估（DPIA）。	您作为数据控制者，是否对涉及其决策对自然人产生法律影响或类似重大影响的用户画像、大规模系统监控、大规模敏感数据处理、数据跨境转移、向第三方披露等业务场景，进行数据保护影响评估（DPIA）。 <ul style="list-style-type: none"> <li>检查内部是否对其决策对自然人产生法律影响或类似重大影响的用户画像、大规模系统监控、大规模敏感数据处理、数据跨境转移、向第三方披露等场景进行数据保护影响评估，留有记录。</li> <li>检查针对隐私影响评估识别出的风险，是否采取合理的风险应对措施。</li> </ul>
对于提供自动化决策的系统，如用户画像（Profiling）等，您是否为用户提供退出的机制。	对于提供自动化决策的系统，如用户画像（Profiling）等，您是否为用户提供退出的机制。 <ul style="list-style-type: none"> <li>检查是否提供自动化决策的机制。</li> <li>检查是否在用户反对自动化决策时，可以提供数据主体可以拒绝自动化决策的机制（确保数据主体可以不受此机制影响）。</li> </ul>

检查项目	检查内容
<p>您是否已制定合适的个人信息保留期限和提供删除或者匿名化超过存留期的个人数据的机制。</p>	<p>您是否已制定合适的个人信息保留期限和提供删除或者匿名化超过存留期的个人数据的机制。</p> <ul style="list-style-type: none"> <li>● 检查是否已制定个人信息保留期限或策略。</li> <li>● 检查制定的个人信息保留期限或策略是否合理，可参考以下方面： <ul style="list-style-type: none"> <li>- 遵从当地适用的法律法规和行业规范。</li> <li>- 考虑个人数据当前和未来价值，以及个人数据被用于或最初被收集的商业目的。</li> <li>- 考虑留存个人数据的成本、风险和责任，包括为保障数据主体权利而做的努力(如访问权)。</li> <li>- 确保个人数据“准确、最新”的难易程度。</li> </ul> </li> <li>● 当个人信息已达到保留期限或策略时，是否对个人信息进行删除或去标识化处理，可参考以下情况： <ul style="list-style-type: none"> <li>- 当个人信息不再用于原有的目的，或已达到个人信息制定的保留期限或策略时，对此类个人信息进行删除或去标识化处理，包括因处理个人信息而生成的临时文件。 注：去标识化是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联数据主体的过程。</li> <li>- 在没有其他适用法律要求组织继续保留个人信息时，当数据主体发出删除其个人信息请求后，立即删除个人信息。</li> <li>- 在收集个人信息的方式或目的违反了法律法规要求或与数据主体的约定时，删除个人信息。</li> </ul> </li> </ul>
<p>您作为数据控制者是否提供记录个人数据泄露的机制。</p>	<p>您作为数据控制者是否提供记录个人数据泄露的机制。 检查是否有记录个人数据泄露的机制。</p>

检查项目	检查内容
您作为数据控制者是否对数据处理活动进行记录。	您作为数据控制者是否对数据处理活动进行记录。 检查是否有记录数据处理活动的机制，包括以下： <ul style="list-style-type: none"><li>● 个人信息处理的记录。</li><li>● 个人信息跨境转移记录。</li><li>● 向第三方披露的记录。</li><li>● 数据主体的同意与撤回同意的记录。</li><li>● 数据主体提出的请求。</li></ul>
您作为数据处理者是否对数据处理活动进行记录。	您作为数据处理者是否对数据处理活动进行记录。 检查是否有记录数据处理活动的机制，包括以下： <ul style="list-style-type: none"><li>● 个人信息处理的记录。</li><li>● 个人信息跨境转移记录。</li><li>● 向第三方披露的记录。</li></ul>

## GDPR-数据主体访问

表 7-27 数据主体访问风险项检查项目

检查项目	检查内容
<p>对于收集、处理、存储个人数据的系统，您是否提供数据主体可以访问其个人数据的机制。</p>	<p>对于收集、处理、存储个人数据的系统，您是否提供数据主体可以访问其个人数据的机制。</p> <p>检查是否提供数据主体可以访问数据主体提供的个人数据的机制。检查数据主体是否可以从系统获取确认他的个人数据是否在被处理，并能够访问个人数据和以下信息：</p> <ul style="list-style-type: none"> <li>● 处理数据的目的。</li> <li>● 相关个人数据的类别。</li> <li>● 已经或者将要个人数据向其披露的数据接收者或其分类，特别是第三国或国际组织的数据接收者。</li> <li>● 若有可能，访问个人数据将被存储的预设期限；若不可能，访问决定期限的通常标准。</li> <li>● 数据主体享有请求数据控制者更正、清除与数据主体相关的数据的权利，或者限制、拒绝其处理该个人数据的权利。</li> <li>● 向监管机构提出投诉的权利。</li> <li>● 若个人数据并非收集自数据主体，则可以访问有关数据来源的任何可获得的信息。</li> <li>● 包括识别分析在内的自动化决策的存在，至少可以访问关于决策中所运用的逻辑的有用信息以及该处理的重要性和其对数据主体造成的可能后果。</li> </ul>

检查项目	检查内容
<p>对于收集、处理、存储个人数据的系统，您作为设备提供者是否提供数据主体或数据控制者可以访问其个人数据的机制。</p>	<p>对于收集、处理、存储个人数据的系统，您作为设备提供者是否提供数据主体或数据控制者可以访问其个人数据的机制。</p> <p>检查是否提供数据主体可以访问数据主体提供的个人数据的机制。检查数据主体是否可以从系统获取确认他的个人数据是否在被处理，并能够访问个人数据和以下信息：</p> <ul style="list-style-type: none"> <li>● 处理数据的目的。</li> <li>● 相关个人数据的类别。</li> <li>● 已经或者将要个人数据向其披露的数据接收者或其分类，特别是第三国或国际组织的数据接收者。</li> <li>● 若有可能，访问个人数据将被存储的预设期限；若不可能，访问决定期限的通常标准。</li> <li>● 数据主体享有请求数据控制者更正、清除与数据主体相关的数据的权利，或者限制、拒绝其处理该个人数据的权利；</li> <li>● 向监管机构提出投诉的权利。</li> <li>● 若个人数据并非收集自数据主体，则可以访问有关数据来源的任何可获得的信息。</li> <li>● 包括识别分析在内的自动化决策的存在，至少可以访问关于决策中所运用的逻辑的有用信息以及该处理的重要性和其对数据主体造成的可能后果。</li> </ul>
<p>对于收集、处理、存储个人数据的系统，您作为数据控制者是否提供数据主体可以修改数据主体提供的个人数据的机制。</p>	<p>对于收集、处理、存储个人数据的系统，您作为数据控制者是否提供数据主体可以修改数据主体提供的个人数据的机制。</p> <p>检查是否提供数据主体可以修改数据主体提供的个人数据的机制。</p>
<p>对于收集、处理、存储个人数据的系统，您作为设备提供者是否提供数据主体可以修改数据主体提供的个人数据的机制。</p>	<p>对于收集、处理、存储个人数据的系统，您作为设备提供者是否提供数据主体可以修改数据主体提供的个人数据的机制。</p> <p>检查是否提供数据主体可以修改数据主体提供的个人数据的机制。</p>

检查项目	检查内容
对于收集、处理、存储个人数据的系统，您作为数据控制者是否提供数据主体可以删除数据主体提供的个人数据的机制。	对于收集、处理、存储个人数据的系统，您作为数据控制者是否提供数据主体可以删除数据主体提供的个人数据的机制。 检查是否提供数据主体可以删除数据主体提供的个人数据的机制。
对于收集、处理、存储个人数据的系统，您作为设备提供者是否提供数据主体或数据控制者可以删除数据主体提供的个人数据的机制。	对于收集、处理、存储个人数据的系统，您作为设备提供者是否提供数据主体或数据控制者可以删除数据主体提供的个人数据的机制。 检查是否提供数据主体可以删除数据主体提供的个人数据的机制。
对于收集、处理、存储个人数据的系统，您是否提供数据主体限制其个人数据处理机制。	对于收集、处理、存储个人数据的系统，您是否提供数据主体限制其个人数据处理机制。 检查是否提供数据主体限制其个人数据处理机制。
对于收集、处理、存储个人数据的系统，您是否提供数据主体的个人数据能够被导出的机制。	对于收集、处理、存储个人数据的系统，您是否提供数据主体的个人数据能够被导出的机制。 检查是否提供数据主体导出其个人数据处理机制。
您是否按照相应法规、标准的要求，在规定时间内响应数据主体合法请求的机制，以保障数据主体的合法权利。	您是否按照相应法规、标准的要求，在规定时间内响应数据主体合法请求的机制，以保障数据主体的合法权利。 询问内部负责个人信息合规的人员，是否按照相应法规、标准的要求提供处理数据主体合法请求的机制，检查是否对响应时间有明确的限制，以保障数据主体的合法权利，机制包括但不限于以下： <ul style="list-style-type: none"><li>● 告知机制。</li><li>● 访问机制。</li><li>● 提供副本机制。</li><li>● 更改机制。</li><li>● 反对机制。</li><li>● 删除机制。</li><li>● 撤回同意机制。</li><li>● 注销机制。</li><li>● 响应其他合理请求的机制。</li></ul>

检查项目	检查内容
您将个人数据使用到直接营销目的时，系统是否提供供撤销个人数据用于营销活动同意的机制并告知用户。	<p>您将个人数据使用到直接营销目的时，系统是否提供供撤销个人数据用于营销活动同意的机制并告知用户。</p> <ul style="list-style-type: none"> <li>• 检查是存在否将个人数据直接使用到营销目的的场景或业务。</li> <li>• 检查系统是否提供撤销同意或退订的机制。</li> </ul>

## GDPR-通知

表 7-28 通知风险项检查项目

检查项目	检查内容
您作为数据控制者是否向数据主体提供隐私声明。	<p>您作为数据控制者是否向数据主体提供隐私声明。</p> <ul style="list-style-type: none"> <li>• 检查是否提供隐私声明。</li> <li>• 检查隐私声明中信息是否完善，隐私声明必须包括以下信息： <ul style="list-style-type: none"> <li>- 数据控制者的身份信息和联系方式。</li> <li>- 处理个人数据的目的、方式、范围。</li> <li>- 个人数据的存储期限或决定存储期限的标准。</li> <li>- 数据主体享有向数据控制者请求访问、更正、清除个人数据的权利，限制、拒绝处理个人数据的权利以及可携带权。</li> <li>- 数据主体有权随时撤销同意。</li> <li>- 向监管机构投诉的权利。</li> <li>- 自动化决策（包括识别分析、用户画像）及可能对数据主体造成的后果。</li> <li>- 数据保护官的详细联系方式（如果适用的话）。</li> <li>- 个人数据接收者或者接受者的类型（如果有的话）。</li> </ul> </li> <li>• 检查隐私声明是否清晰明确，且易于理解和阅读。</li> </ul>

检查项目	检查内容
您作为设备供应者是否提供产品处理的个人数据的说明，并按照数据控制者的要求提供隐私声明的界面。	您作为设备供应者是否提供产品处理的个人数据的说明，并按照数据控制者的要求提供隐私声明的界面。 <ul style="list-style-type: none"><li>• 检查是否提供个人数据说明。</li><li>• 检查是否提供隐私声明的界面。</li></ul>
您作为设备供应者在从第三方获取个人数据时，是否提供产品处理的个人数据的说明。	您作为设备供应者在从第三方获取个人数据时，是否提供产品处理的个人数据的说明。 检查是否提供产品处理的个人数据的说明文档。
对于面向最终用户的系统，数据主体在注册个人信息时，您是否提供验证数据主体身份的机制。	对于面向最终用户的系统，数据主体在注册个人信息时，您是否提供验证数据主体身份的机制。 检查是否提供验证数据主体身份的机制。
您作为数据处理者在聘用另一个处理者或涉及到补充或替换其他处理者的变动，是否通知数据控制者，并获取数据控制者的书面授权	您作为数据处理者在聘用另一个处理者或涉及到补充或替换其他处理者的变动，是否通知数据控制者，并获取数据控制者的书面授权。 在处理涉及到补充或替换其他处理者的变动，检查是否有通知数据控制者，并获取数据控制者的书面授权的机制和流程。
您作为数据控制者是否有向数据主体报告个人数据泄露的机制。	您作为数据控制者是否有向数据主体报告个人数据泄露的机制。 检查是否有向数据主体报告个人数据泄露的机制或流程。
您作为数据控制者是否有向监管机构报告个人数据泄露的机制。	您作为数据控制者是否有向监管机构报告个人数据泄露的机制。 检查是否有向监管机构报告个人数据泄露的机制和流程。
您作为数据处理者是否有向数据控制者报告个人数据泄露的机制。	您作为数据处理者是否有向数据控制者报告个人数据泄露的机制。 检查是否有向数据控制者报告个人数据泄露的机制和流程。

## GDPR-选择和同意

表 7-29 选择和同意风险项检查项目

检查项目	检查内容
您作为数据控制者，在进行个人信息的收集、处理时，是否已征得数据主体的同意、合同协议的履行或者其他法定事由，并提供撤销同意的机制。	<p>您作为数据控制者，在进行个人信息的收集、处理时，是否已征得数据主体的同意、合同协议的履行或者其他法定事由，并提供撤销同意的机制。</p> <ul style="list-style-type: none"> <li>检查个人信息收集流程规范相关文档，获取同意的机制是否基于数据主体的同意、合同协议的履行或者其他法定事由。</li> <li>检查是否存在对应退出同意的机制。</li> </ul>
如果您处理个人数据的合法依据是“合法利益”，您是否已经进行了隐私影响评估（PIA）。	<p>如果您处理个人数据的合法依据是“合法利益”，您是否已经进行了隐私影响评估（PIA）。</p> <p>检查是否存在进行隐私影响评估（PIA）的机制和流程。</p>
隐私政策和用户协议是否可供随时查看。	<p>隐私政策和用户协议是否可供随时查看。</p> <p>检查隐私政策和用户协议查看的位置是否方便且清晰。</p>
您是否提供获取用户明示同意的机制（即用户主动单击），在收集用户的个人数据前（如：用户注册、首次使用APP）获取用户的同意。	<p>您是否提供获取用户明示同意的机制（即用户主动单击），在收集用户的个人数据前（如：用户注册、首次使用APP）获取用户的同意。</p> <p>检查在是否在收集个人数据前获取用户同意，获取用户同意时是否需要用户主动操作，且没有误导行为。</p>
您在处理涉及犯罪定罪与违法的个人数据时，是否获取官方机构授权。	<p>您在处理涉及犯罪定罪与违法的个人数据时，是否获取官方机构授权。</p> <ul style="list-style-type: none"> <li>检查是否有处理涉及犯罪定罪与违法的个人数据的场景。</li> <li>检查是否有获取官方机构授权的机制和流程。</li> </ul>

检查项目	检查内容
您是否给数据主体提供撤销同意或退出个人数据收集的方式、渠道。数据主体撤销同意之后，产品必须禁止继续收集和使用相应的个人数据。	<p>您是否给数据主体提供撤销同意或退出个人数据收集的方式、渠道。数据主体撤销同意之后，产品必须禁止继续收集和使用相应的个人数据。</p> <p>检查是否提供部分同意和撤销同意的机制。</p> <p>注：撤销同意为数据主体可以通过便捷的形式，如与提供同意保持一致的形式，撤回对其所有个人信息收集的同意。</p>
您是否提供个人数据同意的撤销机制，撤销同意是否与表达同意一样简单。	<p>您是否提供个人数据同意的撤销机制，撤销同意是否与表达同意一样简单。</p> <ul style="list-style-type: none"> <li>● 检查系统是否提供撤销同意机制（如：单击退订链接、回复退订短信、单击不同意按钮，或者是向隐私政策中预留联系方式发送申请等）。</li> <li>● 检查用户撤销同意后，是否立即停止收集和处理用户个人数据。如果由于计算周期长等合理原因而无法马上停止处理，须保证在下一周期前停止处理。</li> <li>● 检查撤销同意的方法足够明了（例如，某个APP的撤销同意的配置项处于3层以及3层菜单之内）。</li> <li>● 检查是否对用户撤销同意做记录。</li> </ul>

## GDPR-组织架构

表 7-30 组织架构风险项检查项目

检查项目	检查内容
您作为控制者或处理者为欧盟内的数据主体提供相关商品或服务，或者监控数据主体的行为，是否以书面形式在欧盟委任一名代表。	<p>您作为控制者或处理者为欧盟内的数据主体提供相关商品或服务，或者监控数据主体的行为，是否以书面形式在欧盟委任一名代表。</p> <ul style="list-style-type: none"> <li>● 检查业务中是否为欧盟内的数据主体提供相关商品或服务，或者监控数据主体的行为。</li> <li>● 检查是否在欧盟委任一名代表。</li> </ul>

检查项目	检查内容
您是否委任数据保护官。	您是否委任数据保护官。 <ul style="list-style-type: none"><li>• 检查是否委任数据保护官。</li><li>• 检查是否发布数据保护官的详细联系方式，并向监管机构进行报告。</li></ul>

## 经典弱口令检测-弱口令检测

表 7-31 弱口令检测风险项检查项目

检查项目	检查内容
弱口令检测	检测账号口令是否属于常用的弱口令，提示用户修改不安全的口令

## 口令复杂度策略检测-口令复杂度

表 7-32 口令复杂度检测风险项检查项目

检查项目	检查内容
口令长度检测	目标服务器设置的口令长度策略是否符合标准，口令长度不能小于设定的某一个长度
大写字母检测	目标服务器设置的口令长度策略是否符合标准，口令中的大写字母个数不能小于某个数值
小写字母检测	目标服务器设置的口令长度策略是否符合标准，口令中的小写字母个数不能小于某个数值
数字检测	目标服务器设置的口令长度策略是否符合标准，口令中的数字个数不能小于某个数值
特殊字符检测	目标服务器设置的口令长度策略是否符合标准，口令中的特殊字符个数不能小于某个数值

## PCI-DSS-维护信息安全政策

表 7-33 维护信息安全政策风险项检查项目

检查项目	检查内容
您是否已准备充足的资源以确保网络安全与隐私保护管理目标的达成，制定包括对人员、技术、环境、设施、信息和财务等资源的需求预算。	检查是否制定网络安全与隐私保护的预算规划，预算规划包括人员、技术、环境、设施、信息和财务等，例如指定特定人员，每天 24 小时随时响应警报。
您是否已由管理层正式授权或指定了专门的团队或个人来负责网络安全与隐私保护工作并且明确了这些角色的具体职责和权限。	<ul style="list-style-type: none"><li>• 检查是否有正式的文件（如职位描述、组织结构图、政策手册等）表明有特定的团队或个人被赋予了管理网络安全和隐私保护的责任。</li><li>• 被指定负责网络安全和隐私保护工作的团队成员或个人进行交流，了解其对自己职责的理解以及如何执行这些职责。</li><li>• 检查内部沟通记录（如会议纪要、电子邮件链），以确定管理层对网络安全和隐私保护工作的支持程度及指示传达情况。</li></ul>
您是否根据持续监测和定期评估中获得的信息，至少每年一次审核并更新网络安全与隐私保护的管理策略、流程、标准及相关文件，并明确制定、分发和更新相关文档的人员。	<ul style="list-style-type: none"><li>• 检查是否有审核记录，每年审核网络安全与隐私保护管理策略、流程、标准及相关文件。</li><li>• 检查网络安全与隐私保护的相关文件是否有指定的人员去制定、分发和更新。</li></ul>
您是否已识别您范围内的资产（物理设备、系统、虚拟设备、软件和数据流等），根据资产的关键性、威胁影响和可能性来确定相关的风险。	检查资产风险威胁报告，是否识别出范围内的资产，根据资产的关键性、威胁影响和可能性来确定相关的风险，其中资产包括： <ul style="list-style-type: none"><li>• 物理设备</li><li>• 系统</li><li>• 虚拟设备</li><li>• 软件</li><li>• 数据流等</li></ul>
您是否建立和维护资产清单，内容需覆盖您拥有的所有组件，且资产清单包括资产重要性、责任人、位置、状态和资产关联关系等内容。	<ul style="list-style-type: none"><li>• 检查是否制定与维护资产清单。</li><li>• 检查是否将拥有的所有组件均列入清单。</li><li>• 检查资产清单是否包括资产重要性、责任人、位置、状态和资产关联关系等内容。</li></ul>

检查项目	检查内容
您是否根据制定的数据安全治理策略，应明确数据的责任归属，和数据采集、使用、存储、传输、共享、披露和销毁等数据生命周期中各方的角色、职责。	<ul style="list-style-type: none"> <li>● 检查是否制定数据管理策略。</li> <li>● 检查数据管理策略里是否有明确数据的责任归属。</li> <li>● 检查数据管理策略里是否明确数据采集、使用、存储、传输、共享、披露和销毁等数据生命周期中各方的角色、职责。</li> <li>● 如涉及处理持卡人数据，还应检查对于通过远程访问客户数据的工作人员，是否明确规定禁止将持卡人数据复制、移动和存储到本地硬盘及可移动电子媒介上。</li> </ul>
您是否针对不同岗位制定相应的安全意识培训和岗位技能培训计划，并定期刷新计划和培训内容。	<ul style="list-style-type: none"> <li>● 检查是否有根据不同岗位举行安全意识培训和岗位技能培训的记录。</li> <li>● 检查是否有对培训计划内容更新的记录。</li> </ul>
您是否至少每年一次或当发生重大变更时执行内部和外部审计，以确保符合安全策略、标准和要求。若您作为服务提供商，是否每季度进行一次审查并维护季度审查流程文档记录。	<p>检查审计记录，是否每年一次或发生重大变更时执行内部和外部审计，包括但不限于以下方面：</p> <ul style="list-style-type: none"> <li>● 网络安全管理体系的适宜性、充分性和有效性。</li> <li>● 法律法规的遵从性。</li> <li>● 业务流程信息安全控制的有效性。</li> </ul> <p>检查审计记录，作为个人数据控制者，在执行内部审计时，是否做到以下：</p> <ul style="list-style-type: none"> <li>● 建立自动化的审计流程、程序和系统。</li> <li>● 形成相应的审计记录或日志。</li> <li>● 加强对审计记录的保护，防止未授权的访问、篡改或删除。</li> <li>● 应及时处理审计过程中发现的个人信息违规处理行为。</li> </ul> <p>如作为服务供应商，是否每季度进行一次审查并维护季度审查流程文档记录，审查内容包括但不限于：</p> <ul style="list-style-type: none"> <li>● 日常日志审查。</li> <li>● 防火墙规则集审查。</li> <li>● 将配置标准应用于新系统。</li> <li>● 响应安全警报。</li> <li>● 更改管理流程。</li> </ul>

## PCI-DSS-实施强有力的访问控制措施

表 7-34 实施强有力的访问控制措施风险项检查项目

检查项目	检查内容
您是否根据业务关键性、数据敏感性等要素对资产进行分级分类和标识。	检查是否有资产分级分类记录，对资产进行分级分类和标识。 检查是否有资产标识记录，记录对资产的保护需求。
您是否至少每年一次或在重大变更时对资产进行盘点。	询问资产管理人员是否至少每年一次，对资产进行盘点。 询问资产管理人员否在重大变更时，对资产进行盘点。
您是否建立介质管理机制，对介质的使用和访问进行限制和保护，并实施物理保护和逻辑保护等措施。	询问资产管理人员是否对介质的使用采用物理、逻辑保护措施。 询问资产管理人员采用哪些措施限制介质使用。
您是否对介质的转移建立授权机制并实施了安全控制。运送过程中是否采取了保护措施。	检查介质保护策略，是否建立机制以保护存储了信息的介质： <ul style="list-style-type: none"> <li>• 运送和转移过程中受到保护。</li> <li>• 不被未授权的访问。</li> <li>• 不当使用以及毁坏。</li> </ul> 检查在运送或转移机制的过程中是否实施保护措施，包括但不限于以下内容： <ul style="list-style-type: none"> <li>• 通过可靠的快递公司或其他可准确跟踪的投递方法递送介质。</li> <li>• 凡自安全区域转移介质时（包括将介质分发给个人），确保经过管理层批准。</li> </ul>
当硬件资产下线时，您是否针对承载数据的资产，进行安全销毁，包括对数据的永久删除与介质销毁。	询问资产管理人员是否在硬件资产下线时，针对承载数据的资产，进行安全销毁。 询问资产管理人员是否采用粉碎、焚烧等方式进行物理销毁。 如果由有资质的第三方进行销毁，询问资产管理人员销毁要求是否采用物理销毁，是否获得数据销毁证明。
您是否实施了适当的用户标识管理策略，包括为用户分配了唯一账号名、唯一身份鉴别码、设置有效期，并对跨组织的账号进行标识等。	检查用户账号管理系统配置，是否满足： <ul style="list-style-type: none"> <li>• 为用户分配唯一账号名。</li> <li>• 禁止分配已失效或已过期的用户名。</li> <li>• 禁止使用组、共享或通用用户名。</li> <li>• 设置账号有效期。</li> </ul> 检查是否有跨组织的账号区分机制。

检查项目	检查内容
您是否有符合标准要求的账号登录失败自动锁定的安全控制。	检查是否有账号自动锁定的机制。 账号锁定的配置是否满足锁定6次以上尝试失败的账号，锁定持续时间至少为30分钟。
您现有的权限管理机制是否遵循了按需分配、最小授权及职责分离原则。	检查现有的权限管理规范，是否包含以下原则： <ul style="list-style-type: none"> <li>• 按需分配，根据职位、角色以及访问的必要性对数据中心进行细粒度的物理访问授权。</li> <li>• 最小授权，根据职位、角色以及访问的必要性对数据中心进行细粒度的物理访问授权。</li> <li>• 职责分离原则，遵循不相容的职责互相分离。例如授权、签发、审核、执行、记录等工作不应由同一个人负责。</li> </ul>
您是否已采用了基于角色或属性的访问控制机制，定义每个角色的访问需求，根据角色需求分配访问权限。	检查权限管理策略，是否包括但不限于以下内容： <ul style="list-style-type: none"> <li>• 定义每个角色的访问需求，包括每个角色需要访问其作业功能所需的系统组件和数据资源，和访问资源所需的权限级别（例如，用户、管理员等）。</li> <li>• 根据角色需求分配访问权限，例如根据个人职位分类和职能分配访问权限。</li> </ul> 如涉及管理持卡人数据，还应检查是否限制对任何包含持卡人数据的数据库的所有访问（包括应用程序、管理员和其他所有用户的访问）。
当内外部职员工作职责发生变化时，您是否在24小时内完成账号与权限的变更。	检查转岗或离职的人员账号与权限是否在24小时内完成变更。
您的密码策略是否遵循了行业标准，并禁止使用通用、共享、与账号一样的密码。	检查系统密码策略是否满足强度要求： <ul style="list-style-type: none"> <li>• 密码长度至少为8个字符。</li> <li>• 密码至少包含（大写字母、小写字母、数字、特殊符号）中的三种的组合。</li> <li>• 密码历史为4个。</li> <li>• 密码最小有效期限为1天。</li> <li>• 密码最大有效期限为90天，至少每90天更改一次密码。</li> </ul>
您是否建立了密码分配的策略。例如在首次登录时分配随机的初始密码，并在首次登录后强制要求更改密码且更改后的密码应满足公司的密码复杂度要求。	检查对密码是否有管理规范相关文档，包括但不限于以下内容： <ul style="list-style-type: none"> <li>• 首次登录时分配随机的初始密码。</li> <li>• 首次登录后强制要求更改密码，且更改后的密码满足设置的密码复杂度要求。</li> </ul> 检查密码分配记录，是否对初始密码和密码复杂度有要求。

检查项目	检查内容
您在验证凭证（例如密码/口令）进行传输、存储时，是否对验证凭证使用AES、RSA、IDEA等加密算法进行加密，并在传输时使用加密通道。	<p>检查密码传输和存储策略，是否对验证凭证（例如密码/口令）使用加密算法（例如AES、TDES/TDEA、RSA）等加密。</p> <p>检查密码传输时是否对传输通道进行加密。</p> <p>检查是否禁止未加密的静态鉴别凭证嵌入到应用、访问脚本中。</p>
您实施多因素认证时，是否满足相应标准的要求，确保多因素认证是否绑定唯一的账号，禁止在多个账号之间共享；并且至少对其中一种鉴别技术使用密码技术来实现。	<p>检查制定的权限管理规范中对于多因素认证鉴别因子的管理要求是否包括但不限于以下：</p> <ul style="list-style-type: none"> <li>多因素认证是否绑定唯一的账号，禁止在多个账号之间共享，且明确最小、最大有效期限，及再利用条件，当人员角色、属性发生变更时，应及时更新。</li> <li>是否至少对其中一种鉴别技术使用密码技术来实现。</li> </ul> <p>注：多因素认证的鉴别因子为采用口令、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。</p>
您是否至少定期，如一个月审核一次所有账号与权限，并在审核发现账号与权限存在偏差时，于规定期限内完成整改。	<p>检查是否有维护所有账号与权限的清单。</p> <p>检查维护清单的记录，是否至少定期审核一次所有账号与权限，并在审核发现账号与权限存在偏差时，于规定期限内完成整改。</p>
您是否实施物理访问控制措施，限制对物理端口、网络插孔、无线接入点、电信线路等资产的物理访问。	<p>检查是否制定资产的物理访问控制策略文档，文档里包括但不限于以下内容：</p> <ul style="list-style-type: none"> <li>明确物理和/或逻辑控制，限制实际接触公共网络插座交换机。</li> <li>限制实际接触无线访问点、网关、手持式设备、网络/通信硬件和电信线路。</li> <li>保护通过直接接触卡本身便可捕获支付卡数据的设备，以避免设备被篡改和替换。</li> <li>定期检查设备的表面，以检查篡改（例如给设备增加读卡器）或替换（例如通过检查序列号或其他设备特征确认其未被欺诈性设备调换）迹象。</li> </ul> <p>检查访问控制的资产是否包括：</p> <ul style="list-style-type: none"> <li>物理端口</li> <li>网络插孔</li> <li>无线接入点</li> <li>网关</li> <li>手持设备</li> <li>信息系统</li> <li>通信硬件</li> <li>电信线路等</li> </ul>

## PCI-DSS-建立和维护安全网络和系统

表 7-35 建立和维护安全网络和系统风险项检查项目

检查项目	检查内容
您是否维护数据流图和数据清单，对数据存储、处理和传输的过程、数据的位置进行记录。	<p>检查是否有制定和维护数据流和数据清单，记录数据的位置，内容参考如下：</p> <ul style="list-style-type: none"> <li>● 敏感数据</li> <li>● 网络架构层面的数据流</li> <li>● 数据的位置</li> </ul>
您是否已根据安全配置基线对所有软硬件资产进行了适当的加固处理。	<p>检查是否有正式的安全配置基线文档，该文档应详细列出针对不同类型的软硬件资产（如操作系统、数据库、网络设备等）的具体安全配置要求。</p> <p>通过自动化工具或手动方式审计现有的软硬件配置，确保它们符合既定的安全配置基线。这包括但不限于防火墙规则、用户权限设置、服务和端口的状态等。</p> <p>确认在部署新系统或更新现有系统时，是否遵循了基于安全配置基线的加固步骤，并且这些步骤被纳入到变更管理流程中。</p>
<p>您是否已建立符合行业标准的的安全配置基线，并满足以下要求：</p> <ol style="list-style-type: none"> <li>1. 按照最小化原则，仅启用必要且安全的服务、协议、端口等；</li> <li>2. 网络设备默认拒绝所有网络通信流量，并保持最新稳定版本；</li> <li>3. 禁用不必要的服务、协议、功能、端口等；</li> <li>4. 删除默认账号，或修改默认账号名及口令；</li> <li>5. 如需启用不安全的功能，应实施额外的安全控制措施；</li> <li>6. 时钟同步服务器符合行业标准，及使用三种同步的时间源；</li> <li>7. 保留文档化记录；</li> <li>8. 获取审批</li> </ol>	<p>检查是否有安全配置基线。</p> <p>检查安全配置基线的配置是否满足以下要求：</p> <ul style="list-style-type: none"> <li>● 按照最小化原则，仅启用必要且安全的服务、协议、端口等。</li> <li>● 网络设备默认拒绝所有网络通信流量。</li> <li>● 禁用不必要的服务、协议、功能、端口等。</li> <li>● 删除默认账号，或修改默认账号名及口令。</li> <li>● 如需启用不安全的功能，应实施额外的安全控制措施。</li> <li>● 保留文档化记录。</li> <li>● 获取审批。</li> </ul> <p>检查时钟同步服务器的时间源是否符合行业标准。</p>

检查项目	检查内容
您是否提供自动化检查工具，集中管理安全配置基线，定期检测配置文件的更改、内容文件的完整性。	检查是否有对安全配置基线的管理与验证部署自动化检查工具。 检查自动化检查工具是否满足以下要求： <ul style="list-style-type: none"><li>● 定期检查配置的更改，如SAN、路由器配置。</li><li>● 定期查检内容文件完整性，如关键系统文件、内容文件。</li></ul>
您是否根据风险影响分析，进行了变更与回退方案的测试，以确保对组织的运行和安全没有负面影响。	检查是否有变更与回退测试的流程规范。 检查变更与回退测试是否满足以下要求： <ul style="list-style-type: none"><li>● 明确测试类型和范围。</li><li>● 执行变更与回退方案测试。</li><li>● 对发现的问题进行整改或采取缓解措施。</li><li>● 根据合同要求，安排云客户参与变更测试。</li></ul>
您是否集中部署防恶意软件工具，确保能够检测、删除和抵御所有已知类型的恶意软件或代码。	检查是否集中部署防恶意软件工具，确保能够检查、删除和抵御所有已知类型的恶意软件或代码。 检查部署的恶意软件防护工具的配置是否满足但不限于以下要求： <ul style="list-style-type: none"><li>● 配置自动监控，如果出现异常，可向管理员报告。</li><li>● 配置定期执行扫描的策略。</li><li>● 恶意软件防护工具无法被禁用或更改。</li><li>● 至少每天或在供应商发布新的更新时，对恶意软件防护工具进行更新。</li><li>● 至少每天更新病毒特征和行为库。</li><li>● 更新可以回滚，以防更新导致系统故障。</li></ul>
您是否在网络拓扑文档中记录网络安全相关的设计与配置信息，并保持更新。	检查是否有网络拓扑文档，文档中是否记录网络安全相关的设计与配置信息，并保持更新，文档内容是否包括但不限于以下内容： <ul style="list-style-type: none"><li>● 包括云服务网络逻辑架构，架构图是持续更新的，并可以追溯。</li><li>● 包括因业务原因和授权适用的所有服务、协议和端口。</li><li>● 显示子网的分配方式，以及网络的分区和分段方式。</li><li>● 显示数据的存储区域。</li><li>● 记录因采用了不安全的协议所采取的额外安全措施。</li></ul>

检查项目	检查内容
您是否在网络边界部署了安全设备/服务，确保跨边界的网络流量安全受控。	<p>检查网络边界部署策略，是否在网络边界部署了安全设备/服务，确保跨边界的网络流量安全受控，部署的安全设备/服务包括但不限于：</p> <ul style="list-style-type: none"> <li>• 入侵检测/防御系统</li> <li>• 防火墙</li> <li>• 安全网关</li> <li>• 网络协议分析工具</li> <li>• 网络扫描工具</li> <li>• 网络嗅探工具</li> </ul>
您是否对网络区域边界实施了访问控制，并设置满足行业标准的访问控制规则以控制数据包进出。	<p>检查访问控制列表（ACL）是否拒绝恶意IP地址或默认拒绝受控端口和IP以外的通信。</p> <p>检查访问控制列表（ACL）的维护记录，是否删除无效规则。</p> <p>检查跨网络的访问是否需要经过评估与授权。</p>
您是否根据已识别的漏洞制定了详细的修补方案，并确保所有关键资产都得到了适当的保护。	<p>检查是否有正式的漏洞管理策略或流程文档，明确规定了如何识别、评估和修复系统中的漏洞。该文档应包括漏洞扫描工具的选择与使用、漏洞优先级排序、修补时间表及验证修补效果的方法。</p> <p>查看修补计划文档和相关日志文件，确认针对每个已识别的漏洞都制定了具体的修补方案，并且这些修补活动都被详细记录下来，包括修补的具体步骤、责任人、预计完成时间和实际执行结果。</p>

## PCI-DSS-维护漏洞管理计划

表 7-36 维护漏洞管理计划风险项检查项目

检查项目	检查内容
您是否定期对承担安全角色和关键职责的内外部员工开展岗位安全技能培训和考核，并检查对员工的绩效机制已包含信息安全的有关要求。	<ul style="list-style-type: none"> <li>• 检查是否有对担任安全角色和关键职责的人员进行岗位技能培训。</li> <li>• 检查员工的绩效考核机制是否有包括信息安全的要求。</li> <li>• 检查技术技能考核记录，包括对开发人员进行最新的安全编码技术进行培训和考核。</li> </ul>

检查项目	检查内容
您是否存在正式的设计规范和安全架构文档，指导软件开发与系统部署，涵盖了关键的安全领域，如身份验证、授权、加密、日志记录与监控等。	<ul style="list-style-type: none"><li>● 文档审查：检查是否有详细的文档集，包括但不限于设计规范、安全架构蓝图、技术指南等。确保这些文档清晰地定义了系统的整体结构及其各个组成部分如何协同工作。</li><li>● 内容评估：仔细审阅现有文档的内容，确认其覆盖了所有必要的安全方面，例如身份验证机制、访问控制策略、数据保护措施（如加密）、日志记录与审计功能等。</li><li>● 版本控制检查：查看文档的版本历史记录，了解它们是否定期更新并反映了最新的技术和最佳实践。</li><li>● 一致性验证：对比实际部署的系统架构与设计规范及安全架构文档的一致性，确保两者之间没有显著差异。</li></ul>
您是否制定了详细的代码编写安全规范，并确保开发人员参照这些规范进行编码，涵盖关键的安全实践如输入验证、错误处理、数据加密和会话管理等。	<ul style="list-style-type: none"><li>● 检查是否有正式的安全编码指南或手册，其中详细描述代码编写时应注意的安全最佳实践和标准。该文档应涵盖输入验证、错误处理、数据加密、会话管理等方面。</li><li>● 评估现有的代码审查（Code Review）流程，确认是否包含对安全编码规范遵守情况的检查。这可以通过查看代码审查工具中的检查清单或规则集来实现。</li><li>● 检查是否采用了静态应用安全测试（SAST）工具或其他自动化分析工具来帮助识别不符合安全编码规范的代码段。</li></ul>
您是否对主机、容器、服务器等实施恶意软件防护。	<ul style="list-style-type: none"><li>● 检查是否部署恶意软件防护工具。</li><li>● 检查是否在易受恶意软件影响的系统部署防病毒软件，并确保防病毒机制保持最新。</li><li>● 检查恶意防护工具的部署范围、数量、病毒库更新策略。</li><li>● 检查对外来计算机或存储设备接入系统前是否有流程机制要求对恶意代码检查。</li><li>● 检查是否具备预防和检测常见类型的恶意攻击的工具。</li><li>● 检查是否有恶意代码告警的相关记录，对恶意代码告警进行检查和分析。</li></ul>

## PCI-DSS-定期监控和测试网络

表 7-37 定期监控和测试网络风险项检查项目

检查项目	检查内容
您是否制定了渗透测试计划，并至少每年一次以及应用程序有任何重要升级或修改时，在授权后由专人对Web应用程序、内部支撑系统等进行渗透测试。	<ul style="list-style-type: none"> <li>• 询问负责渗透测试的人员，了解渗透测试计划与渗透测试流程。</li> <li>• 检查渗透测试计划文档。</li> <li>• 询问负责渗透测试的人员，当聘请第三方人员进行渗透测试时，是否检查第三方人员的资格认证。</li> </ul>
您是否部署了变更检测机制以发现未经授权的修改，并对于此类发现进行整改。	<ul style="list-style-type: none"> <li>• 检查安全配置基线策略。</li> <li>• 检查对配置基线的偏离情况是否有进行分析整改记录，对偏离情况进行分析整改。如以下内容： <ul style="list-style-type: none"> <li>- 在关键系统文件、配置文件或内容文件发生非授权修改（包括变更、添加和删除）时警示工作人员。</li> <li>- 软件配置至少每周执行一次关键对比。</li> </ul> </li> </ul>
您是否对网络设备、主机、虚拟化平台、应用软件等系统开启了日志功能。	<ul style="list-style-type: none"> <li>• 检查日志管理策略文档。</li> <li>• 检查系统类型是否满足以下要求： <ul style="list-style-type: none"> <li>- 应用软件、杀毒软件等。</li> <li>- 网络设备，如边界、重要节点设备。</li> <li>- 主机，如服务器、虚拟化平台等。</li> </ul> </li> </ul>
您是否对访问控制、运维操作、敏感数据访问、系统事件等类型开启了日志功能。	<ul style="list-style-type: none"> <li>• 检查是否有日志管理策略文档。</li> <li>• 检查日志类型是否满足以下要求： <ul style="list-style-type: none"> <li>- 访问控制日志</li> <li>- 运维操作日志</li> <li>- 敏感数据访问日志</li> <li>- 系统事件日志等</li> </ul> </li> </ul>
您是否使用了满足相应外部标准或内部管理要求的日志管理系统，对日志进行集中收集和分析。	<ul style="list-style-type: none"> <li>• 检查是否有日志管理系统，对日志进行集中收集和分析。</li> <li>• 检查是否有日志管理系统是否满足外部标准或内部管理要求。</li> <li>• 检查是否在集中管理日志系统出现故障时，是否自动报告给相关责任人，是否有组件冗余。</li> <li>• 检查日志服务器与资产之间的身份认证是否在传输和存储使用加密技术或带外管理。</li> </ul>

检查项目	检查内容
您是否定期备份日志，并对日志及其备份采取保护措施。	<ul style="list-style-type: none"><li>● 检查是否有日志保护策略文档。</li><li>● 检查日志保护措施是否满足以下要求。<ul style="list-style-type: none"><li>- 通过访问控制防止未授权更改。</li><li>- 写入只写媒体。</li><li>- 禁止远程访问日志服务器。</li><li>- 当日志存储容量用完时，覆盖最早的记录。</li><li>- 日志数据的传输与存储应与客户数据隔离。</li><li>- 备份位于不同的物理位置。</li></ul></li></ul>
您是否确保了安全审计日志记录保留至少一年，并且至少三个月内可在线查询或立即可从备份中恢复。	<ul style="list-style-type: none"><li>● 检查是否有安全审计日志策略文档。</li><li>● 抽查是否可以立即在线查询三个月内的安全审计日志（包括联机、存档或可从备份中恢复）。</li><li>● 抽查离线归档是否保存一年以上。</li></ul>
您是否制定漏洞扫描计划，并有专人负责通过手动检测或自动的漏洞扫描工具，定期（至少每季度一次）对网络环境进行漏洞扫描。	<ul style="list-style-type: none"><li>● 检查漏洞扫描计划文档。</li><li>● 检查是否由具有经验和资质的专人使用漏洞扫描工具，并在发生重大变更后重新执行内部和外部扫描（重大变更：例如数据访问权限被修改或数据环境安全受到影响）。</li><li>● 检查漏洞扫描工具是否具备以下能力：<ul style="list-style-type: none"><li>- 实时更新漏洞库。</li><li>- 发现系统漏洞缺陷和不安全配置。</li><li>- 支持标准化的漏洞检查表和扫描流程。</li><li>- 对漏洞进行影响评估。</li><li>- 展示已扫描的信息系统组件和已核查过的漏洞。</li><li>- 需从正规渠道获取，商业工具要具备合法授权。</li><li>- 不影响业务的运行。</li></ul></li><li>● 检查是否对漏洞扫描中涉及的资料严格保密，不得向未经授权的非相关人员和组织公开披露。</li></ul>

检查项目	检查内容
您是否已实施入侵检测、防火墙、DDoS防护系统等技术措施，集中监控针对网络设备、主机与容器、应用系统、安全设备的网络攻击。	<ul style="list-style-type: none"> <li>● 检查是否对网络设备、主机与容器、应用系统、安全设备等进行集中安全监控。</li> <li>● 检查是否使用如下监控技术措施： <ul style="list-style-type: none"> <li>- 入侵检测/入侵防御</li> <li>- 防火墙</li> <li>- DDoS防护系统/设备</li> <li>- 物理访问控制</li> <li>- 逻辑访问控制</li> <li>- 检查日志，例如访问控制日志、运维操作日志、系统时间日志等</li> <li>- 沙箱</li> <li>- 网络通讯监测</li> <li>- 访问及数据传输侦测</li> </ul> </li> </ul>
您是否已通过安全监控平台对采集的安全日志进行持续监控，识别与记录对关键系统的未授权更改、日志文件完整性监控或更改检测、特权账号异常行为、无效逻辑访问尝试等攻击或异常行为。	<ul style="list-style-type: none"> <li>● 检查是否通过安全监控平台进行采集告警、日志。</li> <li>● 检查安全监控平台是否可以进行分析。</li> <li>● 检查是否识别并记录以下行为： <ul style="list-style-type: none"> <li>- 识别与记录对关键系统的未授权更改。</li> <li>- 日志文件完整性监控或更改检测。</li> <li>- 特权账号异常行为。</li> <li>- 无效逻辑访问尝试等攻击或异常行为。</li> </ul> </li> </ul>
系统在发生网络攻击或异常情况时，是否触发告警并分配相关责任人对告警进行跟踪、验证和处理。	<ul style="list-style-type: none"> <li>● 检查是否有网络异常情况告警记录。</li> <li>● 检查异常情况告警分发记录，是否将告警分配给相关责任人，并对告警进行跟踪、验证和处理。</li> </ul>

## PCI-DSS-保护账户数据

表 7-38 保护账户数据风险项检查项目

检查项目	检查内容
您是否根据数据的分级分类，识别出需要加密传输的场景。	<p>检查是否根据数据的分级分类，识别出需要加密传输的场景，包括但不限于：</p> <ul style="list-style-type: none"> <li>● 通过公共网络的数据传输。</li> <li>● 非控制台访问的管理操作数据。</li> </ul>

检查项目	检查内容
您是否实施技术措施，以确保数据在传输的真实性、保密性和完整性。	<p>检查是否采取技术措施确保数据传输时的真实性、保密性和完整性，技术措施包括但不限于以下：</p> <ul style="list-style-type: none"> <li>在通信前对通信双方进行认证，确保通信的真实性。</li> <li>使用安全的协议（包括TLS、IPSec、SSH等），确保协议支持安全的版本与配置。</li> </ul> <p>检查是否有禁止使用不安全的协议：SSL2.0，SSL3.0，TLS1.0，TLS1.1，SSHv1，IKEv1等。</p>
您是否已实施技术措施，确保数据在存储过程中的保密性和完整性。	<ul style="list-style-type: none"> <li>检查是否已实施技术措施，确保数据在存储过程中的保密性和完整性。</li> <li>保密性技术措施参考：AES、RSA、IDES等加密算法，如涉及国家机密信息还应使用国密算法。完整性技术措施参考：哈希、签名等。</li> <li>如数据存储涉及到持卡人数据，检查是否使用以下任一方法使PAN在任何存储位置（包括便携式数字媒体、备份媒体和日志中）不可读： <ul style="list-style-type: none"> <li>基于强加密的单向哈希（哈希必须是整个PAN）。</li> <li>截断（哈希不能用来替换PAN的截断段）。</li> <li>索引令牌和焊盘（焊盘必须安全存放）。</li> <li>使用强密码，并对密钥进行管理。</li> </ul> </li> </ul>
您是否已建立了定期识别并删除超出保留期限或不再需要的数据的机制。	<ul style="list-style-type: none"> <li>检查是否有正式的数据保留和删除政策，明确规定了不同类型数据的保留期限以及如何处理过期数据。</li> <li>查看现有的数据管理流程，确认是否存在系统化的方法用于定期识别即将到期或已过期的数据，并确保这些数据能够被及时标记出来以供审核或删除。</li> <li>评估所使用的数据管理和存储解决方案是否具备自动化功能来帮助识别、分类及删除不再需要的数据。例如，使用数据生命周期管理（DLM）工具或归档系统。</li> <li>查阅相关日志或报告，确认所有数据删除操作都有详细记录，包括执行时间、涉及的数据集、负责人员等信息。</li> </ul>
您是否已制定密钥使用和保护策略，并贯穿其整个生命周期。	<p>检查是否已制定满足以下要求的密钥使用和保护策略，并贯穿其整个生命周期：</p> <ul style="list-style-type: none"> <li>明确密钥主要保管人的责任，并最大限度地减少保管人数。</li> <li>明确密钥的生成、分发、使用、轮换、归档、销毁所需要的授权。</li> <li>如果手动明文进行密钥管理，应实施知识拆分和双重控制进行管理。</li> </ul>

## PCI-DSS-其他

表 7-39 其他风险项检查项目

检查项目	检查内容
您是否对变更进行记录，并进行风险评估和分类分级。	检查是否有对变更进行风险评估与分级记录。 检查变更风险评估分析维度是否包括如下内容： <ul style="list-style-type: none"><li>● 受影响的设备或系统组件。</li><li>● 复杂度。</li><li>● 时间窗口。</li><li>● 对基础架构、网络及上下游系统的影响，如安全隐患、兼容性问题、隐私问题等。</li></ul>
您是否有变更通知与实施策略，在变更实施后，对变更有效性进行验证，并同步更新配置库及适用的文件。	检查是否有变更通知与实施策略等文件，包括以下要求： <ul style="list-style-type: none"><li>● 对变更后的有效性进行验证，同步更新配置库，有效性验证包括变更符合安全配置基线要求，以及对业务造成不利影响。</li><li>● 对于未通过评审的变更，予以关闭，并保留相关文档记录。</li></ul>

## NIST SP 800-53-系统和采购

表 7-40 系统和采购风险项检查项目

检查项目	检查内容
您是否制定了详细的代码编写安全规范，并确保开发人员参照这些规范进行编码，涵盖关键的安全实践如输入验证、错误处理、数据加密和会话管理等。	<ul style="list-style-type: none"><li>● 检查是否有正式的安全编码指南或手册，其中详细描述代码编写时应注意的安全最佳实践和标准。该文档应涵盖输入验证、错误处理、数据加密、会话管理等方面。</li><li>● 评估现有的代码审查（Code Review）流程，确认是否包含对安全编码规范遵守情况的检查。这可以通过查看代码审查工具中的检查清单或规则集来实现。</li><li>● 检查是否采用了静态应用安全测试（SAST）工具或其他自动化分析工具来帮助识别不符合安全编码规范的代码段。</li></ul>

## NIST SP 800-53-项目管理

表 7-41 项目管理风险项检查项目

检查项目	检查内容
您是否已准备充足的资源以确保网络安全与隐私保护管理目标的达成，制定包括对人员、技术、环境、设施、信息和财务等资源的需求预算。	检查是否制定网络安全与隐私保护的预算规划，预算规划包括人员、技术、环境、设施、信息和财务等，例如指定特定人员，每天 24 小时随时响应警报。
您是否已由管理层正式授权或指定了专门的团队或个人来负责网络安全与隐私保护工作并且明确了这些角色的具体职责和权限。	<ul style="list-style-type: none"> <li>检查是否有正式的文件（如职位描述、组织结构图、政策手册等）表明有特定的团队或个人被赋予了管理网络安全和隐私保护的责任。</li> <li>被指定负责网络安全和隐私保护工作的团队成员或个人进行交流，了解其对自己职责的理解以及如何执行这些职责。</li> <li>检查内部沟通记录（如会议纪要、电子邮件链），以确定管理层对网络安全和隐私保护工作的支持程度及指示传达情况。</li> </ul>
您是否根据制定的数据安全治理策略，应明确数据的责任归属，和数据采集、使用、存储、传输、共享、披露和销毁等数据生命周期中各方的角色、职责。	<ul style="list-style-type: none"> <li>检查是否制定数据管理策略。</li> <li>检查数据管理策略里是否有明确数据的责任归属。</li> <li>检查数据管理策略里是否明确数据采集、使用、存储、传输、共享、披露和销毁等数据生命周期中各方的角色、职责。</li> <li>如涉及处理持卡人数据，还应检查对于通过远程访问客户数据的工作人员，是否明确规定禁止将持卡人数据复制、移动和存储到本地硬盘及可移动电子媒介上。</li> </ul>

## NIST SP 800-53-评估、授权和监控

表 7-42 评估、授权和监控风险项检查项目

检查项目	检查内容
您是否制定了渗透测试计划，并至少每年一次以及应用程序有任何重要升级或修改时，在授权后由专人对 Web 应用程序、内部支撑系统等系统进行渗透测试。	<ul style="list-style-type: none"> <li>询问负责渗透测试的人员，了解渗透测试计划与渗透测试流程。</li> <li>检查渗透测试计划文档。</li> <li>询问负责渗透测试的人员，当聘请第三方人员进行渗透测试时，是否检查第三方人员的资格认证。</li> </ul>

检查项目	检查内容
<p>您是否至少每年一次或当发生重大变更时执行内部和外部审计，以确保符合安全策略、标准和要求。若您作为服务提供商，是否每季度进行一次审查并维护季度审查流程文档记录。</p>	<ul style="list-style-type: none"> <li>● 检查审计记录，是否每年一次或发生重大变更时执行内部和外部审计，包括但不限于以下方面： <ul style="list-style-type: none"> <li>- 网络安全管理体系的适宜性、充分性和有效性。</li> <li>- 法律法规的遵从性。</li> <li>- 业务流程信息安全控制的有效性。</li> </ul> </li> <li>● 检查审计记录，作为个人数据控制者，在执行内部审计时，是否做到以下： <ul style="list-style-type: none"> <li>- 建立自动化的审计流程、程序和系统。</li> <li>- 形成相应的审计记录或日志。</li> <li>- 加强对审计记录的保护，防止未授权的访问、篡改或删除。</li> <li>- 应及时处理审计过程中发现的个人信息违规处理行为。</li> </ul> </li> <li>● 如作为服务供应商，是否每季度进行一次审查并维护季度审查流程文档记录，审查内容包括但不限于： <ul style="list-style-type: none"> <li>- 日常日志审查。</li> <li>- 防火墙规则集审查。</li> <li>- 将配置标准应用于新系统。</li> <li>- 响应安全警报。</li> <li>- 更改管理流程。</li> </ul> </li> </ul>
<p>您是否根据已识别的漏洞制定了详细的修补方案，并确保所有关键资产都得到了适当的保护。</p>	<ul style="list-style-type: none"> <li>● 检查是否有正式的漏洞管理策略或流程文档，明确规定了如何识别、评估和修复系统中的漏洞。该文档应包括漏洞扫描工具的选择与使用、漏洞优先级排序、修补时间表及验证修补效果的方法。</li> <li>● 查看修补计划文档和相关日志文件，确认针对每个已识别的漏洞都制定了具体的修补方案，并且这些修补活动都被详细记录下来，包括修补的具体步骤、责任人、预计完成时间和实际执行结果。</li> </ul>

## NIST SP 800-53-审计与问责

表 7-43 审计与问责风险项检查项目

检查项目	检查内容
<p>您是否根据数据的分级分类，识别出需要加密传输的场景。</p>	<p>检查是否根据数据的分级分类，识别出需要加密传输的场景，包括但不限于：</p> <ul style="list-style-type: none"> <li>● 通过公共网络的数据传输。</li> <li>● 非控制台访问的管理操作数据。</li> </ul>

检查项目	检查内容
<p>您是否对网络设备、主机、虚拟化平台、应用软件等系统开启了日志功能。</p>	<p>检查日志管理策略文档。</p> <p>检查系统类型是否满足以下要求：</p> <ul style="list-style-type: none"> <li>● 应用软件、杀毒软件等。</li> <li>● 网络设备，如边界、重要节点设备。</li> <li>● 主机，如服务器、虚拟化平台等</li> </ul>
<p>您是否对访问控制、运维操作、敏感数据访问、系统事件等类型开启了日志功能。</p>	<p>检查是否有日志管理策略文档。</p> <p>检查日志类型是否满包括以下：</p> <ul style="list-style-type: none"> <li>● 访问控制日志</li> <li>● 运维操作日志</li> <li>● 敏感数据访问日志</li> <li>● 系统事件日志等</li> </ul>
<p>您是否使用了满足相应外部标准或内部管理要求的日志管理系统，对日志进行集中收集和分析。</p>	<ul style="list-style-type: none"> <li>● 检查是否有日志管理系统，对日志进行集中收集和分析。</li> <li>● 检查是否有日志管理系统是否满足外部标准或内部管理要求。</li> <li>● 检查是否在集中管理日志系统出现故障时，是否自动报告给相关责任人，是否有组件冗余。</li> <li>● 检查日志服务器与资产之间的身份认证是否在传输和存储使用加密技术或带外管理。</li> </ul>
<p>您是否定期备份日志，并对日志及其备份采取保护措施。</p>	<p>检查是否有日志保护策略文档。</p> <p>检查日志保护措施是否满足以下要求：</p> <p>通过访问控制防止未授权更改。</p> <ul style="list-style-type: none"> <li>● 写入只写媒体。</li> <li>● 禁止远程访问日志服务器。</li> <li>● 当日志存储容量用完时，覆盖最早的记录。</li> <li>● 日志数据的传输与存储应与客户数据隔离。</li> <li>● 备份位于不同的物理位置。</li> </ul>
<p>您是否确保了安全审计日志记录保留至少一年，并且至少三个月内可在线查询或立即可从备份中恢复。</p>	<ul style="list-style-type: none"> <li>● 检查是否有安全审计日志策略文档。</li> <li>● 抽查是否可以立即在线查询三个月内的安全审计日志（包括联机、存档或可从备份中恢复）。</li> <li>● 抽查离线归档是否保存一年以上。</li> </ul>

检查项目	检查内容
您是否已通过安全监控平台对采集的安全日志进行持续监控，识别与记录对关键系统的未授权更改、日志文件完整性监控或更改检测、特权账号异常行为、无效逻辑访问尝试等攻击或异常行为。	<ul style="list-style-type: none"> <li>● 检查是否通过安全监控平台进行采集告警、日志。</li> <li>● 检查安全监控平台是否可以进行分析。</li> <li>● 检查是否识别并记录以下行为： <ul style="list-style-type: none"> <li>- 识别与记录对关键系统的未授权更改。</li> <li>- 日志文件完整性监控或更改检测。</li> <li>- 特权账号异常行为。</li> <li>- 无效逻辑访问尝试等攻击或异常行为。</li> </ul> </li> </ul>

## NIST SP 800-53-媒体介质保护

表 7-44 媒体介质保护风险项检查项目

检查项目	检查内容
您是否建立介质管理机制，对介质的使用和访问进行限制和保护，并实施物理保护和逻辑保护等措施。	<ul style="list-style-type: none"> <li>● 询问资产管理人員是否对介质的使用采用物理、逻辑保护措施。</li> <li>● 询问资产管理人員采用哪些措施限制介质使用。</li> </ul>
您是否对介质的转移建立授权机制并实施了安全控制。运送过程中是否采取了保护措施。	<ul style="list-style-type: none"> <li>● 检查介质保护策略，是否建立机制以保护存储了信息的介质： <ul style="list-style-type: none"> <li>- 运送和转移过程中受到保护。</li> <li>- 不被未授权的访问。</li> <li>- 不当使用以及毁坏。</li> </ul> </li> <li>● 检查在运送或转移机制的过程中是否实施保护措施，包括但不限于以下内容： <ul style="list-style-type: none"> <li>- 通过可靠的快递公司或其他可准确跟踪的投递方法递送介质。</li> <li>- 凡自安全区域转移介质时（包括将介质分发给个人），确保经过管理层批准。</li> </ul> </li> </ul>

## NIST SP 800-53-系统和通信保护

表 7-45 系统和通信保护风险项检查项目

检查项目	检查内容
您是否实施技术措施，以确保数据在传输的真实性、保密性和完整性。	<p>检查是否采取技术措施确保数据传输时的真实性、保密性和完整性，技术措施包括但不限于以下：</p> <ul style="list-style-type: none"> <li>在通信前对通信双方进行认证，确保通信的真实性。</li> <li>使用安全的协议（包括TLS、IPSec、SSH等），确保协议支持安全的版本与配置。</li> </ul> <p>检查是否有禁止使用不安全的协议：SSL2.0，SSL3.0，TLS1.0，TLS1.1，SSHv1，IKEv1等。</p>
您是否已实施技术措施，确保数据在存储过程中的保密性和完整性。	<ul style="list-style-type: none"> <li>检查是否已实施技术措施，确保数据在存储过程中的保密性和完整性。 <ul style="list-style-type: none"> <li>保密性技术措施参考：AES、RSA、IDES等加密算法，如涉及国家机密信息还应使用国密算法。</li> <li>完整性技术措施参考：哈希、签名等。</li> </ul> </li> <li>如数据存储涉及到持卡人数据，检查是否使用以下任一方法使PAN在任何存储位置（包括便携式数字媒体、备份媒体和日志中）不可读： <ul style="list-style-type: none"> <li>基于强加密的单向哈希（哈希必须是整个PAN）。</li> <li>截断（哈希不能用来替换PAN的截断段）。</li> <li>索引令牌和焊盘（焊盘必须安全存放）。</li> <li>使用强密码，并对密钥进行管理。</li> </ul> </li> </ul>
您是否已制定密钥使用和保护策略，并贯穿其整个生命周期。	<p>检查是否已制定满足以下要求的密钥使用和保护策略，并贯穿其整个生命周期：</p> <ul style="list-style-type: none"> <li>明确密钥主要保管人的责任，并最大限度地减少保管人数。</li> <li>明确密钥的生成、分发、使用、轮换、归档、销毁所需要的授权。</li> <li>如果手动明文进行密钥管理，应实施知识拆分和双重控制进行管理。</li> </ul>

检查项目	检查内容
<p>您是否已建立符合行业标准的安全配置基线，并满足以下要求：（1）按照最小化原则，仅启用必要且安全的服务、协议、端口等；（2）网络设备默认拒绝所有网络通信流量，并保持最新稳定版本；（3）禁用不必要的服务、协议、功能、端口等；（4）删除默认账号，或修改默认账号名及口令；（5）如需启用不安全的功能，应实施额外的安全控制措施；（6）时钟同步服务器符合行业标准，及使用三种同步的时间源；（7）保留文档化记录；（8）获取审批</p>	<ul style="list-style-type: none"> <li>● 检查是否有安全配置基线。</li> <li>● 检查安全配置基线的配置是否满足以下要求： <ul style="list-style-type: none"> <li>- 按照最小化原则，仅启用必要且安全的服务、协议、端口等。</li> <li>- 网络设备默认拒绝所有网络通信流量。</li> <li>- 禁用不必要的服务、协议、功能、端口等。</li> <li>- 删除默认账号，或修改默认账号名及口令。</li> <li>- 如需启用不安全的功能，应实施额外的安全控制措施。</li> <li>- 保留文档化记录。</li> <li>- 获取审批。</li> </ul> </li> <li>● 检查时钟同步服务器的时间源是否符合行业标准。</li> </ul>
<p>您是否集中部署防恶意软件工具，确保能够检测、删除和抵御所有已知类型的恶意软件或代码。</p>	<ul style="list-style-type: none"> <li>● 检查是否集中部署防恶意软件工具，确保能够检查、删除和抵御所有已知类型的恶意软件或代码。</li> <li>● 检查部署的恶意软件防护工具的配置是否满足但不限于以下要求： <ul style="list-style-type: none"> <li>- 配置自动监控，如果出现异常，可向管理员报告。</li> <li>- 配置定期执行扫描的策略。</li> <li>- 恶意软件防护工具无法被禁用或更改。</li> <li>- 至少每天或在供应商发布新的更新时，对恶意软件防护工具进行更新。</li> <li>- 至少每天更新病毒特征和行为库。</li> <li>- 更新可以回滚，以防更新导致系统故障。</li> </ul> </li> </ul>
<p>您是否在网络拓扑文档中记录网络安全相关的设计与配置信息，并保持更新。</p>	<p>检查是否有网络拓扑文档，文档中是否记录网络安全相关的设计与配置信息，并保持更新，文档内容是否包括但不限于以下内容：</p> <ul style="list-style-type: none"> <li>● 包括云服务网络逻辑架构，架构图是持续更新的，并可以追溯。</li> <li>● 包括因业务原因和授权适用的所有服务、协议和端口。</li> <li>● 显示子网的分配方式，以及网络的分区和分段方式。</li> <li>● 显示数据的存储区域。</li> <li>● 记录因采用了不安全的协议所采取的额外安全措施。</li> </ul>

检查项目	检查内容
您是否在网络边界部署了安全设备/服务，确保跨边界的网络流量安全受控。	<p>检查网络边界部署策略，是否在网络边界部署了安全设备/服务，确保跨边界的网络流量安全受控，部署的安全设备/服务包括但不限于：</p> <ul style="list-style-type: none"> <li>• 入侵检测/防御系统</li> <li>• 防火墙</li> <li>• 安全网关</li> <li>• 网络协议分析工具</li> <li>• 网络扫描工具</li> <li>• 网络嗅探工具</li> </ul>
您是否对网络区域边界实施了访问控制，并设置满足行业标准的访问控制规则以控制数据包进出。	<ul style="list-style-type: none"> <li>• 检查访问控制列表（ACL）是否拒绝恶意IP地址或默认拒绝受控端口和IP以外的通信。</li> <li>• 检查访问控制列表（ACL）的维护记录，是否删除无效规则。</li> <li>• 检查跨网络的访问是否需要经过评估与授权。</li> </ul>
您是否已实施入侵检测、防火墙、DDoS防护系统等技术措施，集中监控针对网络设备、主机与容器、应用系统、安全设备的网络攻击。	<ul style="list-style-type: none"> <li>• 检查是否对网络设备、主机与容器、应用系统、安全设备等进行集中安全监控。</li> <li>• 检查是否使用如下监控技术措施： <ul style="list-style-type: none"> <li>- 入侵检测/入侵防御</li> <li>- 防火墙</li> <li>- DDoS防护系统/设备</li> <li>- 物理访问控制</li> <li>- 逻辑访问控制</li> <li>- 检查日志，例如访问控制日志、运维操作日志、系统时间日志等</li> <li>- 沙箱</li> <li>- 网络通讯监测</li> <li>- 访问及数据传输侦测</li> </ul> </li> </ul>

## NIST SP 800-53-事件与响应

表 7-46 事件与响应风险项检查项目

检查项目	检查内容
系统在发生网络攻击或异常情况时，是否触发告警并分配相关责任人对告警进行跟踪、验证和处理。	<ul style="list-style-type: none"> <li>• 检查是否有网络异常情况告警记录。</li> <li>• 检查异常情况告警分发记录，是否将告警分配给相关责任人，并对告警进行跟踪、验证和处理。</li> </ul>

## NIST SP 800-53-物理环境保护

表 7-47 物理环境保护风险项检查项目

检查项目	检查内容
<p>当硬件资产下线时，您是否针对承载数据的资产，进行安全销毁，包括对数据的永久删除与介质销毁。</p>	<ul style="list-style-type: none"> <li>● 询问资产管理人員是否在硬件资产下线时，针对承载数据的资产，进行安全销毁。</li> <li>● 询问资产管理人員是否采用粉碎、焚烧等方式进行物理销毁。</li> <li>● 如果由有资质的第三方进行销毁，询问资产管理人員销毁要求是否采用物理销毁，是否获得数据销毁证明。</li> </ul>
<p>您是否实施物理访问控制措施，限制对物理端口、网络插孔、无线接入点、电信线路等资产的物理访问。</p>	<ul style="list-style-type: none"> <li>● 检查是否制定资产的物理访问控制策略文档，文档里包括但不限于以下内容： <ul style="list-style-type: none"> <li>- 明确物理和/或逻辑控制，限制实际接触公共网络插座交换机。</li> <li>- 限制实际接触无线访问点、网关、手持式设备、网络/通信硬件和电信线路。</li> <li>- 保护通过直接接触卡本身便可捕获支付卡数据的设备，以避免设备被篡改和替换。</li> <li>- 定期检查设备的表面，以检查篡改（例如给设备增加读卡器）或替换（例如通过检查序列号或其他设备特征确认其未被欺诈性设备调换）迹象。</li> </ul> </li> <li>● 检查访问控制的资产是否包括： <ul style="list-style-type: none"> <li>- 物理端口</li> <li>- 网络插孔</li> <li>- 无线接入点</li> <li>- 网关</li> <li>- 手持设备</li> <li>- 信息系统</li> <li>- 通信硬件</li> <li>- 电信线路等</li> </ul> </li> </ul>

## NIST SP 800-53-规划和策略

表 7-48 规划和策略风险项检查项目

检查项目	检查内容
<p>您是否已经制定了网络安全与隐私保护的战略规划，并设定了明确的里程碑，同时确保这些规划和目标与企业的整体业务战略相一致。</p>	<ul style="list-style-type: none"> <li>● 验证网络安全与隐私保护的战略规划是否真正与企业的业务战略保持一致。检查是否有定期的审查机制来确保两者的一致性，并根据业务发展的变化及时调整安全策略。</li> <li>● 查看设定的里程碑是否合理且具有可操作性。里程碑应当具体、可衡量、可实现、相关性强且时限明确（SMART原则），并能够支持实现总体战略目标。</li> <li>● 检查实际的实施进展，确认是否按照规划的时间表和里程碑推进工作。记录任何偏差或挑战，并分析其原因。</li> </ul>
<p>您是否存在正式的设计规范和安全架构文档，指导软件开发与系统部署，涵盖了关键的安全领域，如身份验证、授权、加密、日志记录与监控等。</p>	<ul style="list-style-type: none"> <li>● 文档审查：检查是否有详细的文档集，包括但不限于设计规范、安全架构蓝图、技术指南等。确保这些文档清晰地定义了系统的整体结构及其各个组成部分如何协同工作。</li> <li>● 内容评估：仔细审阅现有文档的内容，确认其覆盖了所有必要的安全方面，例如身份验证机制、访问控制策略、数据保护措施（如加密）、日志记录与审计功能等。</li> <li>● 版本控制检查：查看文档的版本历史记录，了解它们是否定期更新并反映了最新的技术和最佳实践。</li> <li>● 一致性验证：对比实际部署的系统架构与设计规范及安全架构文档的一致性，确保两者之间没有显著差异。</li> </ul>

## NIST SP 800-53-系统和信息完整性

表 7-49 系统和信息完整性风险项检查项目

检查项目	检查内容
您是否已建立了定期识别并删除超出保留期限或不再需要的数据的机制。	<ul style="list-style-type: none"> <li>● 检查是否有正式的数据保留和删除政策，明确规定了不同类型数据的保留期限以及如何处理过期数据。</li> <li>● 查看现有的数据管理流程，确认是否存在系统化的方法用于定期识别即将到期或已过期的数据，并确保这些数据能够被及时标记出来以供审核或删除。</li> <li>● 评估所使用的数据管理和存储解决方案是否具备自动化功能来帮助识别、分类及删除不再需要的数据。例如，使用数据生命周期管理（DLM）工具或归档系统。</li> <li>● 查阅相关日志或报告，确认所有数据删除操作都有详细记录，包括执行时间、涉及的数据集、负责人员等信息。</li> </ul>
您是否部署了变更检测机制以发现未经授权的修改，并对于此类发现进行整改。	<ul style="list-style-type: none"> <li>● 检查安全配置基线策略。</li> <li>● 检查对配置基线的偏离情况是否有进行分析整改记录，对偏离情况进行分析整改。如以下内容： <ul style="list-style-type: none"> <li>- 在关键系统文件、配置文件或内容文件发生非授权修改（包括变更、添加和删除）时警示工作人员。</li> <li>- 软件配置至少每周执行一次关键对比。</li> </ul> </li> </ul>
您是否已制定变更与回退方案，明确只有在评审、审批通过后才可实施方案，并采取技术手段限制未授权的变更。	<ul style="list-style-type: none"> <li>● 检查是否有制定变更与回退的流程规范。</li> <li>● 检查变更与回退方案是否采取技术手段限制未授权的变更。</li> <li>● 检查变更与回退方案是否包括但不限于以下内容： <ul style="list-style-type: none"> <li>- 变更需求、影响分析和分类分级说明</li> <li>- 变更实施、回退的过程、方法和人员职责</li> <li>- 通知计划等</li> </ul> </li> </ul>
您是否根据风险影响分析，进行了变更与回退方案的测试，以确保对组织的运行和安全没有负面影响。	<ul style="list-style-type: none"> <li>● 检查是否有变更与回退测试的流程规范。</li> <li>● 检查变更与回退测试是否满足以下要求： <ul style="list-style-type: none"> <li>- 明确测试类型和范围。</li> <li>- 执行变更与回退方案测试。</li> <li>- 对发现的问题进行整改或采取缓解措施。</li> <li>- 根据合同要求，安排云客户参与变更测试。</li> </ul> </li> </ul>

检查项目	检查内容
您是否对主机、容器、服务器等实施恶意软件防护。	<ul style="list-style-type: none"> <li>检查是否部署恶意软件防护工具。</li> <li>检查是否在易受恶意软件影响的系统部署防病毒软件，并确保防病毒机制保持最新。</li> <li>检查恶意防护工具的部署范围、数量、病毒库更新策略。</li> <li>检查对外来计算机或存储设备接入系统前是否有流程机制要求对恶意代码检查。</li> <li>检查是否具备预防和检测常见类型的恶意攻击的工具。</li> <li>检查是否有恶意代码告警的相关记录，对恶意代码告警进行检查和分析。</li> </ul>

## NIST SP 800-53-访问控制

表 7-50 访问控制风险项检查项目

检查项目	检查内容
您是否有符合标准要求的账号登录失败自动锁定的安全控制。	<ul style="list-style-type: none"> <li>检查是否有账号自动锁定的机制。</li> <li>账号锁定的配置是否满足锁定6次以上尝试失败的账号，锁定持续时间至少为30分钟。</li> </ul>
您现有的权限管理机制是否遵循了按需分配、最小授权及职责分离原则。	<p>检查现有的权限管理规范，是否包含以下原则：</p> <ul style="list-style-type: none"> <li>按需分配，根据职位、角色以及访问的必要性对数据中心进行细粒度的物理访问授权。</li> <li>最小授权，根据职位、角色以及访问的必要性对数据中心进行细粒度的物理访问授权。</li> <li>职责分离原则，遵循不相容的职责互相分离。例如授权、签发、审核、执行、记录等工作不应由同一个人负责。</li> </ul>
您是否已采用了基于角色或属性的访问控制机制，定义每个角色的访问需求，根据角色需求分配访问权限。	<ul style="list-style-type: none"> <li>检查权限管理策略，是否包括但不限于以下内容： <ul style="list-style-type: none"> <li>定义每个角色的访问需求，包括每个角色需要访问其作业功能所需的系统组件和数据资源，和访问资源所需的权限级别（例如，用户、管理员等）。</li> <li>根据角色需求分配访问权限，例如根据个人职位分类和职能分配访问权限。</li> </ul> </li> <li>如涉及管理持卡人数据，还应检查是否限制对任何包含持卡人数据的数据库的所有访问（包括应用程序、管理员和其他所有用户的访问）。</li> </ul>
当内外部职员工作职责发生变化时，您是否在24小时内完成账号与权限的变更。	检查转岗或离职的人员账号与权限是否在24小时内完成变更。

检查项目	检查内容
您是否至少定期，如一个月审核一次所有账号与权限，并在审核发现账号与权限存在偏差时，于规定期限内完成整改。	检查是否有维护所有账号与权限的清单。 检查维护清单的记录，是否至少定期审核一次所有账号与权限，并在审核发现账号与权限存在偏差时，于规定期限内完成整改。

## NIST SP 800-53-风险评估

表 7-51 风险评估风险项检查项目

检查项目	检查内容
您是否已识别您范围内的资产（物理设备、系统、虚拟设备、软件和数据流等），根据资产的关键性、威胁影响和可能性来确定相关的风险。	检查资产风险威胁报告，是否识别出范围内的资产，根据资产的关键性、威胁影响和可能性来确定相关的风险，其中资产包括： <ul style="list-style-type: none"> <li>● 物理设备</li> <li>● 系统</li> <li>● 虚拟设备</li> <li>● 软件</li> <li>● 数据流等</li> </ul>
您是否制定漏洞扫描计划，并有专人负责通过手动检测或自动的漏洞扫描工具，定期（至少每季度一次）对网络环境进行漏洞扫描。	<ul style="list-style-type: none"> <li>● 检查漏洞扫描计划文档。</li> <li>● 检查是否由具有经验和资质的专人使用漏洞扫描工具，并在发生重大变更后重新执行内部和外部扫描（重大变更：例如数据访问权限被修改或数据环境安全受到影响）。</li> <li>● 检查漏洞扫描工具是否具备以下能力： <ul style="list-style-type: none"> <li>- 实时更新漏洞库。</li> <li>- 发现系统漏洞缺陷和不安全配置。</li> <li>- 支持标准化的漏洞检查表和扫描流程。</li> <li>- 对漏洞进行影响评估。</li> <li>- 展示已扫描的信息系统组件和已核查过的漏洞。</li> <li>- 需从正规渠道获取，商业工具要具备合法授权。</li> <li>- 不影响业务的运行。</li> </ul> </li> <li>● 检查是否对漏洞扫描中涉及的资料严格保密，不得向未经授权的非相关人员和组织公开披露。</li> </ul>

## NIST SP 800-53-配置管理

表 7-52 配置管理风险项检查项目

检查项目	检查内容
您是否建立和维护资产清单，内容需覆盖您拥有的所有组件，且资产清单包括资产重要性、责任人、位置、状态和资产关联关系等内容。	<p>检查是否制定与维护资产清单。</p> <p>检查是否将拥有的所有组件均列入清单。</p> <p>检查资产清单是否包括资产重要性、责任人、位置、状态和资产关联关系等内容。</p>
您是否至少每年一次或在重大变更时对资产进行盘点。	<p>询问资产管理人員是否至少每年一次，对资产进行盘点。</p> <p>询问资产管理人員否在重大变更时，对资产进行盘点。</p>
您是否维护数据流图和数据清单，对数据存储、处理和传输的过程、数据的位置进行记录。	<p>检查是否有制定和维护数据流和数据清单，记录数据的位置，内容参考如下：</p> <ul style="list-style-type: none"> <li>● 敏感数据</li> <li>● 网络架构层面的数据流</li> <li>● 数据的位置</li> </ul>
您是否已根据安全配置基线对所有软硬件资产进行了适当的加固处理。	<ul style="list-style-type: none"> <li>● 检查是否有正式的安全配置基线文档，该文档应详细列出针对不同类型的软硬件资产（如操作系统、数据库、网络设备等）的具体安全配置要求。</li> <li>● 通过自动化工具或手动方式审计现有的软硬件配置，确保它们符合既定的安全配置基线。这包括但不限于防火墙规则、用户权限设置、服务和端口的状态等。</li> <li>● 确认在部署新系统或更新现有系统时，是否遵循了基于安全配置基线的加固步骤，并且这些步骤被纳入到变更管理流程中。</li> </ul>
您是否提供自动化检查工具，集中管理安全配置基线，定期检测配置文件的更改、内容文件的完整性。	<p>检查是否有对安全配置基线的管理与验证部署自动化检查工具。</p> <p>检查自动化检查工具是否满足以下要求：</p> <ul style="list-style-type: none"> <li>● 定期检查配置的更改，如SAN、路由器配置。</li> <li>● 定期查检内容文件完整性，如关键系统文件、内容文件。</li> </ul>
您是否对变更进行记录，并进行风险评估和分类分级。	<ul style="list-style-type: none"> <li>● 检查是否有对变更进行风险评估与分级记录。</li> <li>● 检查变更风险评估分析维度是否包括如下内容： <ul style="list-style-type: none"> <li>- 受影响的设备或系统组件</li> <li>- 复杂度</li> <li>- 时间窗口</li> <li>- 对基础架构、网络及上下游系统的影响，如安全隐患、兼容性问题、隐私问题等</li> </ul> </li> </ul>

检查项目	检查内容
您是否有变更通知与实施策略，在变更实施后，对变更有效性进行验证，并同步更新配置库及适用的文件。	<p>检查是否有变更通知与实施策略等文件，包括以下要求：</p> <ul style="list-style-type: none"> <li>对变更后的有效性进行验证，同步更新配置库，有效性验证包括变更符合安全配置基线要求，以及对业务造成不利影响。</li> <li>对于未通过评审的变更，予以关闭，并保留相关文档记录。</li> </ul>

## NIST SP 800-53-意识与培训

表 7-53 意识与培训风险项检查项目

检查项目	检查内容
您是否根据持续监测和定期评估中获得的信息，至少每年一次审核并更新网络安全与隐私保护的管理策略、流程、标准及相关文件，并明确制定、分发和更新相关文档的人员	<p>检查是否有审核记录，每年审核网络安全与隐私保护管理策略、流程、标准及相关文件。</p> <p>检查网络安全与隐私保护的相关文件是否有指定的人员去制定、分发和更新。</p>
您是否针对不同岗位制定相应的安全意识培训和岗位技能培训计划，并定期刷新计划和培训内容。	<p>检查是否有根据不同岗位举行安全意识培训和岗位技能培训的记录。</p> <p>检查是否有对培训计划内容更新的记录。</p>
您是否定期对承担安全角色和关键职责的内外部员工开展岗位安全技能培训和考核，并检查对员工的绩效机制已包含信息安全的有关要求。	<p>检查是否有对担任安全角色和关键职责的人员进行岗位技能培训。</p> <p>检查员工的绩效考核机制是否有包括信息安全的要求。</p> <p>检查技术技能考核记录，包括对开发人员进行最新的安全编码技术进行培训和考核。</p>

## NIST SP 800-53-识别与认证

表 7-54 识别与认证风险项检查项目

检查项目	检查内容
您是否根据业务关键性、数据敏感性等要素对资产进行分级分类和标识。	<p>检查是否有资产分级分类记录，对资产进行分级分类和标识。</p> <p>检查是否有资产标识记录，记录对资产的保护需求。</p>

检查项目	检查内容
<p>您是否实施了适当的用户标识管理策略，包括为用户分配了唯一账号名、唯一身份鉴别码、设置有效期，并对跨组织的账号进行标识等。</p>	<ul style="list-style-type: none"> <li>● 检查用户账号管理系统配置，是否满足：               <ul style="list-style-type: none"> <li>- 为用户分配唯一账号名。</li> <li>- 禁止分配已失效或已过期的用户名。</li> <li>- 禁止使用组、共享或通用用户名。</li> <li>- 设置账号有效期。</li> </ul> </li> <li>● 检查是否有跨组织的账号区分机制。</li> </ul>
<p>您的密码策略是否遵循了行业标准，并禁止使用通用、共享、与账号一样的密码。</p>	<p>检查系统密码策略是否满足强度要求：</p> <ul style="list-style-type: none"> <li>● 密码长度至少为8个字符。</li> <li>● 密码至少包含（大写字母、小写字母、数字、特殊符号）中的三种的组合。</li> <li>● 密码历史为4个。</li> <li>● 密码最小有效期限为1天。</li> <li>● 密码最大有效期限为90天，至少每90天更改一次密码。</li> </ul>
<p>您是否建立了密码分配的策略。例如在首次登录时分配随机的初始密码，并在首次登录后强制要求更改密码且更改后的密码应满足公司的密码复杂度要求。</p>	<p>检查对密码是否有管理规范相关文档，包括但不限于以下内容：</p> <ul style="list-style-type: none"> <li>● 首次登录时分配随机的初始密码。</li> <li>● 首次登录后强制要求更改密码，且更改后的密码满足设置的密码复杂度要求。</li> </ul> <p>检查密码分配记录，是否对初始密码和密码复杂度有要求。</p>
<p>您在验证凭证（例如密码/口令）进行传输、存储时，是否对验证凭证使用AES、RSA、IDEA等加密算法进行加密，并在传输时使用加密通道。</p>	<ul style="list-style-type: none"> <li>● 检查密码传输和存储策略，是否对验证凭证（例如密码/口令）使用加密算法（例如AES、TDES/TDEA、RSA）等加密。</li> <li>● 检查密码传输时是否对传输通道进行加密。</li> <li>● 检查是否禁止未加密的静态鉴别凭证嵌入到应用、访问脚本中。</li> </ul>
<p>您实施多因素认证时，是否满足相应标准的要求，确保多因素认证是否绑定唯一的账号，禁止在多个账号之间共享；并且至少对其中一种鉴别技术使用密码技术来实现。</p>	<ul style="list-style-type: none"> <li>● 检查制定的权限管理规范中对于多因素认证鉴别因子的管理要求是否包括但不限于以下：               <ul style="list-style-type: none"> <li>- 多因素认证是否绑定唯一的账号，禁止在多个账号之间共享，且明确最小、最大有效期限，及再利用条件，当人员角色、属性发生变更时，应及时更新。</li> <li>- 是否至少对其中一种鉴别技术使用密码技术来实现</li> </ul> </li> </ul> <p>注：多因素认证的鉴别因子为采用口令、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。</p>

## NIST SP 800-53-个人信息处理和透明度

表 7-55 个人信息处理和透明度风险项检查项目

检查项目	检查内容
您是否在收集个人信息时遵循了最小化原则，仅收集与处理目的直接相关的必要信息。	<ul style="list-style-type: none"><li>● 检查是否有明确记录的数据收集目的，并评估这些目的是否具体、清晰。</li><li>● 确认所收集的个人信息类型是否与已定义的目的直接相关，并验证每类信息收集的必要性。</li><li>● 审查数据收集流程，以确定是否存在超出必要范围的信息收集行为。</li></ul>
您是否建立了有效的机制来响应个人信息主体关于访问、更正、删除其个人信息以及撤回同意等请求。	<ul style="list-style-type: none"><li>● 检查是否有明确记录的数据收集目的，并评估这些目的是否具体、清晰。</li><li>● 确认所收集的个人信息类型是否与已定义的目的直接相关，并验证每类信息收集的必要性。</li><li>● 审查数据收集流程，以确定是否存在超出必要范围的信息收集行为。</li><li>● 验证在处理个人信息主体请求时，是否采取了必要的验证步骤以确认请求者的身份，保护个人信息不被未授权访问。</li><li>● 检查是否有记录保存机制，用于记录收到的请求及其处理情况，以便审计和合规检查。</li><li>● 确认是否有针对复杂请求或特殊情况的额外处理程序或扩展时间框架的通知机制。</li></ul>

检查项目	检查内容
您是否已制定合适的个人信息保留期限或策略。	<ul style="list-style-type: none"><li>● 检查是否已制定个人信息保留期限或策略。</li><li>● 查制定的个人信息保留期限或策略是否合理，可参考以下方面：<ul style="list-style-type: none"><li>- 遵从当地适用的法律法规和行业规范。</li><li>- 考虑个人数据当前和未来价值，以及个人数据被用于或最初被收集的商业目的。</li><li>- 考虑留存个人数据的成本、风险和责任，包括为保障数据主体权利而做的努力(如访问权)。</li><li>- 确保个人数据“准确、最新”的难易程度。</li></ul></li></ul> <p>当个人信息已达到保留期限或策略时，是否对个人信息进行删除或去标识化处理，可参考以下情况：</p> <ul style="list-style-type: none"><li>● 当个人信息不再用于原有的目的，或已达到个人信息制定的保留期限或策略时，对此类个人信息进行删除或去标识化处理，包括因处理个人信息而生成的临时文件。 <b>注：</b>去标识化是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联数据主体的过程。</li><li>● 在没有其他适用法律要求组织继续保留个人信息时，当数据主体发出删除其个人信息请求后，立即删除个人信息。</li><li>● 在收集个人信息的方式或目的违反了法律法规要求或与数据主体的约定时，删除个人信息。</li></ul>
您是否确保在收集个人信息之前，以完整、透明、及时、清晰易懂且易于访问的方式告知个人信息主体，并定期审核这些告知内容以确保其符合法律法规及数据处理操作的要求。	<ul style="list-style-type: none"><li>● 检查是否有一个明确的隐私政策或通知，其中包含了个人信息被收集的原因、方式、使用范围以及共享情况等信息。</li><li>● 确认告知的信息是否足够透明，能够让个人信息主体充分理解数据将如何被使用。</li><li>● 评估告知过程是否及时，在个人信息收集之前完成，并且告知形式是否清晰易懂，避免使用过于技术性法律术语。</li><li>● 验证告知机制是否易于访问，例如通过网站、移动应用或其他直接沟通渠道提供给个人信息主体。</li><li>● 检查是否有定期审核告知内容的流程，以确保它们反映最新的数据处理活动并符合当前的法律法规要求。</li></ul>

检查项目	检查内容
您是否确保在收集个人信息时基于主体的同意、合同协议的履行或者其他法定事由，并提供了部分统一及撤销同意的机制。	<ul style="list-style-type: none"> <li>检查是否在收集个人信息前获得了个人信息主体明确的同意，且同意方式符合法律规定。</li> <li>确认是否存在允许个人信息主体对特定信息处理活动给予或拒绝部分同意的选项。</li> <li>评估是否有简单易行的方法供个人信息主体撤销其先前给予的同意，并记录撤销同意的过程。</li> <li>验证在个人信息收集过程中是否考虑了合同协议的履行或其他合法事由作为依据，并有相应的文档支持。</li> <li>检查是否有关于同意管理的内部政策或指南，以确保所有操作符合相关法律法规要求。</li> </ul>
您是否确保在进行个人信息活动时遵循了隐私保护的基本原则。	<ul style="list-style-type: none"> <li>检查是否有明确的隐私政策，该政策是否对个人信息的收集、使用、存储和共享进行了详细说明。</li> <li>确认是否获得了个人信息主体的同意，并记录同意的方式与时间。</li> <li>评估是否采取了适当的措施来确保个人信息的安全，包括但不限于加密、访问控制和定期安全审计。</li> <li>检查是否为个人信息主体提供了查询、更正或删除其个人信息的途径。</li> <li>确认是否遵守当地及国际上的隐私保护法律法规要求。</li> </ul>

## NIST SP 800-53-人员安全

表 7-56 人员安全风险项检查项目

检查项目	检查内容
您是否至少每年一次审核保密协议的内容，并及时通知所有利益相关方重新确认这些协议。	<ul style="list-style-type: none"> <li>检查是否有正式的文档记录了每年对保密协议内容的审核过程和结果。</li> <li>确认是否有详细的审核计划，涵盖所有关键的保密协议，并包括审查的具体标准和步骤。</li> <li>验证是否有系统用于跟踪所有保密协议的状态，包括签署日期、版本号以及最近一次审核的时间。</li> </ul>

检查项目	检查内容
您是否在人员终止任用时，将离职信息通知了所有相关的利益相关方，进行了离职面谈，并及时删除了该员工的访问权限以及确保其归还了名下的所有云服务提供商资产。	<ul style="list-style-type: none"><li>● 审查现有的离职管理政策或流程文档，确认其中是否明确规定了在员工离职时需要执行的所有步骤，如通知利益相关方、进行离职面谈、撤销访问权限及回收资产等。</li><li>● 查看历次员工离职的详细记录，确认每个离职案例中是否都包含了离职面谈记录、通知利益相关方的证据、访问权限撤销的操作记录以及归还资产的确认记录。</li><li>● 验证离职员工的所有系统和应用访问权限是否已被完全撤销。可以通过检查身份认证系统、目录服务（如Active Directory）和各类应用的日志来确认这一点。</li><li>● 确认离职员工名下的所有云服务提供商资产（如虚拟机、存储资源、API密钥等）是否已成功归还或停用。这通常涉及与云服务提供商的管理控制台进行核对。</li></ul>
您是否在人员岗位变更时，及时告知利益相关方，并评估及更新相关人员的逻辑和物理访问权限，确保在规定时间内完成所有必要的调整。	<ul style="list-style-type: none"><li>● 检查是否有正式的流程或政策文件，规定了人员岗位变更时如何通知利益相关方，并评估及更新其访问权限。</li><li>● 确认是否有明确的责任分配，指定负责通知利益相关方以及评估和更新访问权限的个人或团队。</li><li>● 评估是否有记录管理系统用于跟踪岗位变更及其相关的访问权限调整情况。</li><li>● 验证是否有标准操作程序（SOP），详细描述了从通知到权限更新的具体步骤和时间要求。</li></ul>
您是否在发现内外部员工存在违规行为时，进行了再次确认，并对违规行为的严重性和影响程度进行了评估。	<ul style="list-style-type: none"><li>● 检查是否有正式的流程或政策文件，规定了如何处理发现的违规行为，包括再次确认和评估其严重性及影响程度。</li><li>● 确认是否有专门的团队或人员负责调查和评估违规行为，并确保调查过程公正、透明。</li><li>● 评估是否有记录管理系统用于跟踪所有违规行为的调查结果及其处理情况。</li><li>● 验证是否有明确的标准来判断违规行为的严重性和影响程度，例如轻微、中等、严重等级别划分。</li></ul>

检查项目	检查内容
<p>您是否在雇佣员工前，对内外部所有可访问客户数据、交付网络或操作生产环境系统的员工进行背景调查，再由指定或授权的人员负责录用员工。</p>	<ul style="list-style-type: none"> <li>● 检查招聘管理流程规范是否包括对内外部人员进行背景调查。</li> <li>● 检查背景调查流程是否在以下节点开展背景调查：                             <ul style="list-style-type: none"> <li>- 雇用前</li> <li>- 担任对提供的服务有重大影响的角色时</li> </ul> </li> <li>● 检查背景调查模板是否包括但不限于以下内容：                             <ul style="list-style-type: none"> <li>- 身份信息</li> <li>- 学历背景</li> <li>- 工作经历</li> <li>- 资质证明</li> <li>- 信用记录</li> <li>- 无犯罪记录证明</li> <li>- 被勒索的风险</li> </ul> </li> </ul>
<p>您是否已经与内部人员和外部服务提供商签订了包含遵循网络安全规章制度的协议，并确认用户理解并同意这些条款。</p>	<ul style="list-style-type: none"> <li>● 检查是否有正式的协议文档，明确规定了所有内部人员和外部服务提供商必须遵守的网络安全规章制度。</li> <li>● 确认协议中是否详细列出了对各方的具体要求，如数据保护、访问控制、报告机制等。</li> <li>● 评估是否为内部人员和外部服务提供商提供了培训，确保其了解并能履行协议中的条款。</li> <li>● 验证是否有签署记录，证明所有相关人员和服务提供商已阅读并同意遵守协议内容。</li> </ul>
<p>您是否有专门的安全管理团队并明确定义其职责，职责可包括发布网络安全、隐私保护、信息安全相关管理策略，监督管理策略的落地执行，与内外部利益相关方进行沟通等。</p>	<p>检查是否制定网络安全与隐私保护的预算规划，预算规划包括人员、技术、环境、设施、信息和财务等，例如指定特定人员，每天 24 小时随时响应警报。</p>

## NIST SP 800-53-应急计划

表 7-57 应急计划风险项检查项目

检查项目	检查内容
您是否在员工上岗前以及至少每年一次定期对内外部员工进行安全意识培训。	<ul style="list-style-type: none"> <li>● 检查安全意识培训的记录，确认是否每年一次或者雇佣后进行意识培训，以及参与培训的人员理解培训内容。</li> <li>● 检查制定的安全意识培训资料的内容是否包括但不限于以下： <ul style="list-style-type: none"> <li>- 更新的安全政策和程序。</li> <li>- 安全责任与违规惩戒措施。</li> <li>- 普及安全意识，可参考当地法律法规、数据安全、隐私保护、社会工程学、终端使用、物理安全等相关内容。</li> <li>- 安全事件报告及应对流程。</li> <li>- 安全漏洞响应流程（针对负责安全漏洞响应责任的员工）。</li> </ul> </li> </ul>
您是否已经针对所识别的关键产品和服务及其面临的威胁场景制定了详细的业务连续性及灾难恢复计划。	<ul style="list-style-type: none"> <li>● 检查是否有正式的业务连续性计划（BCP）和灾难恢复计划（DRP）文档，详细描述了如何在各种威胁场景下维持关键业务功能并从灾难中恢复。</li> <li>● 确认计划中是否包含了对所有关键产品和服务的具体保护措施、恢复步骤及时间目标（如RTO，RPO）。</li> <li>● 评估是否有明确的角色与职责分配，确保每个团队成员都知道自己在应急响应中的角色和任务。</li> <li>● 验证是否有定期测试和演练机制，确保所有相关人员熟悉并能执行这些计划。</li> </ul>
您是否至少每年一次或在发生重大变更时进行了业务连续性测试和演练，并基于演练结果对业务连续性计划（BCP）和灾难恢复计划（DRP）进行了必要的调整。	<ul style="list-style-type: none"> <li>● 检查是否有正式的文档记录了业务连续性测试和演练的时间表及历史记录。</li> <li>● 确认是否有详细的测试和演练计划，涵盖所有关键业务功能、系统和服务，并包括不同类型的场景。</li> <li>● 评估是否有明确的角色与职责分配，确保每个团队成员都知道自己在演练中的角色和任务。</li> <li>● 验证是否有全面的演练报告，详细记录了演练过程、发现的问题及其解决方案。</li> </ul>

检查项目	检查内容
您是否已提供冗余的通信线路以确保云服务的高可用性。	<ul style="list-style-type: none"><li>● 检查是否部署了多条独立的通信线路，确保它们通过不同的地理位置或使用不同的传输介质连接至云服务提供商。</li><li>● 确认是否有自动故障转移机制，能够在主线路发生故障时无缝切换到备用线路。</li><li>● 评估是否定期对冗余通信线路进行测试，以验证其有效性和响应速度。</li><li>● 检查是否存在监控系统来实时监测通信线路的状态，并在出现问题时发出警报。</li></ul>
您是否对安全事件和应急演练进行了经验总结，包括进行了根本原因分析，并将这些分析结果纳入了事件响应、培训和演练计划中。	<ul style="list-style-type: none"><li>● 审查现有的安全事件报告和应急演练总结文档，确认其中是否包含了根本原因分析的内容，并检查是否有机制将分析结果反馈到事件响应、培训和演练计划中。</li><li>● 查看历次安全事件和应急演练后的根本原因分析报告，确保每次事件或演练后都进行了详细的分析，并记录了发现的问题及其根本原因。</li><li>● 审核针对根本原因分析提出的改进措施的实际执行情况，确认这些措施已被纳入事件响应流程、员工培训计划以及未来的应急演练安排中。</li></ul>
您是否已经建立了异地灾备中心，并实现了主站点和备站点之间的高可用性，确保关键业务能够进行异地实时备份与切换。	<ul style="list-style-type: none"><li>● 检查是否有详细的灾备计划文档，描述了异地灾备中心的设计、部署及管理策略。</li><li>● 确认是否已选择并配置了适当的硬件和软件资源，以支持主、备站点间的实时数据同步和高可用性。</li><li>● 评估是否实施了有效的数据复制技术，如同步或异步复制，以保证关键业务数据在主、备站点间的一致性和完整性。</li><li>● 验证是否有自动故障转移机制，能够在主站点发生故障时迅速将业务切换到备用站点。</li></ul>
您是否每年或发生重大变更时，对于安全事件响应计划、应急预案及流程指引进行审核并测试，根据审核和测试结果优化计划、预案及流程指引。	<ul style="list-style-type: none"><li>● 检查是否每年一次或重大变更时，审核事件流程机制、响应计划与应急预案。</li><li>● 检查是否有对审核和测试结果优化计划、预案及流程指引。</li></ul>

## NIST SP 800-53-供应链风险管理

表 7-58 供应链风险管理风险项检查项目

检查项目	检查内容
<p>您是否对供应商提供的服务进行定期审查或审核，并跟踪发现的问题。</p>	<ul style="list-style-type: none"> <li>● 检查供应商机制，是否对供应商有监视、评审和审核机制。</li> <li>● 检查是否至少每年对供应商进行监控与评估，包括但不限于以下内容：                             <ul style="list-style-type: none"> <li>- 供应商的业绩情况</li> <li>- 供应商的安全策略是否满足策略的要求</li> <li>- 供应商对于合同与协议的履行情况</li> <li>- 供应商违约的影响</li> <li>- 供应商灾难恢复和应急能力</li> <li>- 对供应商提供的服务或产品的依赖性</li> </ul> </li> <li>● 检查对于评估后发现的问题，若结果不可接受，是否有供应商替换或终止合作机制。</li> </ul>
<p>您是否在采购前对供应商进行风险评估，以确保其具备相应等级的安全保护能力。</p>	<ul style="list-style-type: none"> <li>● 检查是否有制定合格供应商的清单。</li> <li>● 检查合格供应商的清单内容是否包括：                             <ul style="list-style-type: none"> <li>- 供应商的详细信息</li> <li>- 产品或服务的描述</li> <li>- 风险评估的结果</li> <li>- 符合协定要求的资质证明</li> </ul> </li> </ul>
<p>您是否已与供应商签订了包含详细安全要求的合同协议，并明确了供应商的责任与义务。</p>	<ul style="list-style-type: none"> <li>● 检查是否有正式的合同或服务级别协议(SLA)，其中明确规定了供应商需要遵守的安全标准和要求。</li> <li>● 确认合同中是否包含了对供应商提供的产品或服务的具体安全要求，如数据保护、隐私保护、访问控制等。</li> <li>● 评估合同条款是否涵盖了供应商在发生安全事件时的责任，包括通知流程、补救措施及赔偿条款。</li> <li>● 验证是否有定期审核供应商安全实践的规定，以确保其持续符合组织的安全政策。</li> <li>● 检查合同中是否有关于终止合作的条款，特别是当供应商未能履行其安全责任时的情况。</li> <li>● 确保所有相关文档都经过法律审查，并且双方签字确认。</li> </ul>

检查项目	检查内容
您是否在采购过程中采取了适当的保护措施，以减少因供应链恶意利用而带来的安全风险。	<ul style="list-style-type: none"> <li>检查是否有正式的供应链风险管理策略或政策，明确如何识别和管理供应商带来的潜在风险。</li> <li>确认是否对供应商进行背景调查和安全评估，包括其财务健康状况、合规历史及安全实践。</li> <li>评估是否在合同中明确规定了供应商必须遵守的安全标准和要求，以及违反这些要求的后果。</li> <li>验证是否实施了多层次的安全审查机制，如产品来源验证、第三方审计等，确保采购的产品和服务未被篡改或植入恶意组件。</li> <li>检查是否有专门的团队或流程负责监控供应链中的潜在威胁，并能够快速响应任何可疑活动。</li> <li>确保所有采购的产品和服务都经过适当的安全测试和验证，特别是在关键领域如网络安全、数据保护等方面。</li> </ul>
您是否确保所采购的产品或服务符合相关的法律法规和行业标准认证要求，并对关键产品进行了专项测试。	<ul style="list-style-type: none"> <li>检查采购流程中是否有明确的步骤来验证产品或服务是否符合相关法律法规及行业标准认证的要求。</li> <li>确认供应商提供的产品或服务是否附带必要的合规性证书或声明，如ISO认证、CE标记等。</li> <li>评估在采购决策过程中是否考虑了产品的安全性、隐私保护能力及其对现有系统的兼容性。</li> <li>验证是否针对关键产品制定了专项测试计划，并且这些测试已经执行，结果记录完整。</li> <li>检查是否有专门的团队或第三方机构负责审核和评估产品或服务的安全性和合规性。</li> <li>确保所有采购的产品或服务都经过适当的审查和批准程序，以确保其符合组织的安全策略和标准。</li> </ul>

## NIST SP 800-53-维护与运维

表 7-59 维护与运维风险项检查项目

检查项目	检查内容
您是否建立管理机制来正确地维护数据中心设施和防护设备等，以保持设备持续的可用性和完整性。	<p>检查设备维护文档，是否建立机制正确地维护设备以保持持续的可用性和完整性。</p> <p>例如是否定期对于设施和设备进行巡检和维护（包括但不限于建筑结构、物理边界访问控制、巡检记录、防盗装置）、每年或发生重大变更时对设施和设备进行有效性和冗余功能检查等。</p>

## ISO/IEC 27002:2022-备份与恢复

表 7-60 备份与恢复风险项检查项目

检查项目	检查内容
TaurusDB实例应开启备份	创建TaurusDB数据库实例时，系统默认开启自动备份策略。实例创建成功后，您可根据业务需要设置自动备份策略。TaurusDB按照用户设置的自动备份策略对数据库进行备份。TaurusDB的备份操作是实例级的，而不是数据库级的。当数据库故障或数据损坏时，可以通过备份恢复数据库，从而保证数据可靠性。由于开启备份会损耗数据库读写性能，建议您选择业务低峰时间段启动自动备份。设置自动备份策略后，会按照策略中的备份时间段和备份周期进行全量备份。实例在执行备份时，按照策略中的保留天数进行存放，备份时长和实例的数据量有关。在进行全量备份的同时系统每5分钟会自动生成增量备份，用户不需要设置。生成的增量备份可以用来将库表数据恢复到指定时间点。
确保开启存储库中的备份策略	需要对备份对象执行自动备份操作时，可以设置备份策略。通过在策略中设置备份任务执行的时间、周期以及备份数据的保留规则，将备份存储库绑定备份策略，可以为存储库执行自动备份。备份策略需要绑定存储库才可以生效，若存储库未执行备份，确保绑定的备份策略状态为开启，防范数据丢失风险（如误删除、硬件故障）和业务中断风险，确保关键数据可恢复，满足合规性要求（如等保2.0）。若未开启备份策略，可能导致备份缺失，数据损坏或丢失后无法恢复，业务连续性受损，且可能违反数据保护法规。开启备份策略后： 1、存储成本增加：频繁备份可能占用更多存储空间，需合理规划保留周期。 2、资源占用：备份任务可能轻微影响I/O性能，但对业务运行无显著影响。
Workspace资源应开启备份存储库	云桌面支持备份存储库功能，当发生病毒入侵、人为误删除、软硬件故障等事件时，可通过CBR的备份服务将云桌面的数据恢复至任意备份点。备份恢复过程中，CBR会保障用户数据的安全性和正确性，确保业务安全。
确保SFS Turbo文件系统在备份存储库中	云备份（CBR）可以为SFS Turbo文件系统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。
启用备份功能并配置备份策略	SQLServer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。

检查项目	检查内容
GeminiDB实例开启备份	GeminiDB支持数据库实例的备份，以保证数据可靠性。实例删除后，手动备份数据保留。自动备份的数据和实例一起释放，备份的数据不支持下载导出。强烈建议您配置合适的自动备份策略，防止客户误操作或者服务异常的情况下，因没有开启备份而造成数据丢失的情况。
启跨区域复制功能	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。
确保ECS资源开启备份功能	ECS实例没有关联备份存储库，视为“不合规”。云备份（CBR）可以为云服务器、云硬盘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。详见云备份概述。相比数据丢失后的恢复，备份的成本更低。
Workspace应设置合理的备份周期	云桌面使用云备份服务中的“云桌面备份”功能进行桌面备份。保障用户数据的安全性和正确性，确保业务安全。当备份的时间间隔过大时，数据丢失风险增加：如果在两次备份之间发生了数据损坏或丢失的情况，那么从最近一次备份恢复时，会丢失这段时间内的所有更改和新增数据。这可能对业务造成严重影响。
建议CBR备份策略执行频率不低于最小频率	华为云CBR支持配置最小备份频率策略，通过策略引擎强制要求备份周期（如每天/每周），确保关键数据定期保护，避免备份遗漏。应对风险：防范因备份间隔过长导致的数据丢失风险（如系统故障时丢失过多增量数据），满足RPO（恢复点目标）要求，确保业务数据可回溯。若不满足：可能导致备份间隔超出安全阈值，故障时丢失大量未备份数据，延长恢复时间，违反行业合规性要求（如等保）。潜在影响： 1、资源消耗：高频备份增加存储和计算负载； 2、性能波动：备份时可能短暂影响业务I/O性能。
确保CBR存储库备份库有足够长的备份保留周期	确保备份保留时间足够长。防止需要使用备份进行业务恢复时，备份被过早清理，满足数据可恢复性和合规性要求。主要防范因备份保留周期过短导致数据无法恢复的风险，例如误删、恶意删除或自动化策略误清理关键备份，影响业务连续性。CBR备份保留日期过短可能导致备份被提前删除，灾难恢复时无可用备份，业务中断风险增加，且可能违反数据保留法规（如金融、医疗行业）。潜在影响： 1. 存储成本增加：长期保留备份会占用更多存储空间，需平衡成本与安全性； 2. 管理复杂度：需定期检查保留策略，避免因保留过多备份导致存储库容量不足。

检查项目	检查内容
确保ECS云服务器在指定周期内创建备份	ECS实例最近一次备份创建时间超过参数要求，视为“不合规”。云备份（CBR）可以为云服务器、云硬盘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。详见云备份概述。当备份的时间间隔过大时，数据丢失风险增加：如果在两次备份之间发生了数据损坏或丢失的情况，那么从最近一次备份恢复时，会丢失这段时间内的所有更改和新增数据，这可能对业务造成严重影响。
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。
确保SFS Turbo文件在最近一次备份距离现在不超过指定时间。	云备份（CBR）可以为SFS Turbo文件系统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。当备份的时间间隔过大时，数据丢失风险增加：如果在两次备份之间发生了数据损坏或丢失的情况，那么从最近一次备份恢复时，会丢失这段时间内的所有更改和新增数据。这可能对业务造成严重影响。
确保CSS集群多AZ部署	可用区（Availability Zone, AZ）指在同一区域（Region）下，电力、网络隔离的物理区域。同一地域内的可用区之间通过内网互通，但彼此在物理层面保持隔离，以降低单点故障风险。多可用区部署是CSS服务提供的高可用性解决方案。通过在同一地域内选择2个或3个不同的可用区部署集群，可有效防止数据丢失并降低服务中断风险。为防止数据丢失，并确保在服务中断情况下能降低集群的停机时间，从而增强集群的高可用性，CSS服务支持跨可用区（即多可用区）部署。创建集群时，如果选择多可用区部署，CSS服务会自动启用跨AZ高可用特性，确保节点在所选可用区中均匀分布（各AZ的节点数量差异不超过1）。多可用区部署时，建议优先选择3个可用区，而非2个可用区。当仅选择2个可用区时，如果其中一个可用区发生故障，可能导致无法选举Master节点，从而引发集群不可用风险。影响：在创建集群时，选择的任意类型的节点数需大于或等于所选AZ数，否则跨可用区部署会失败。当集群中数据节点数或冷数据节点数和可用区数不是整数倍关系时，集群的数据分布可能会不均匀，从而影响数据查询或写入业务。

检查项目	检查内容
建议CBR存储库开启多AZ备份	<p>CBR支持创建多AZ存储库，将备份数据存储到同区域的多个AZ。当某个AZ不可用时，仍然能够从其他AZ正常访问数据，适用于对可靠性要求较高的场景。主要防范单AZ故障（如硬件损坏、电力中断等）导致备份数据不可用，确保业务连续性，满足金融、医疗等行业的高可用性要求。若仅单AZ存储，一旦该AZ故障，可能导致备份数据无法访问，影响灾难恢复能力，增加业务中断风险。潜在影响：</p> <p>1、存储成本略增：多AZ存储会占用额外空间，但相比数据丢失风险可接受；</p> <p>2、备份/恢复延迟：跨AZ同步可能轻微增加备份时间，但对业务影响有限。约束限制：</p> <ul style="list-style-type: none"> <li>● 暂不支持更换已创建存储库的备份数据冗余策略。</li> <li>● 暂不支持将已创建的备份副本迁移至多AZ备份存储库中。</li> <li>● 复制存储库暂不支持多AZ备份冗余策略。</li> <li>● 启用后不支持修改。</li> </ul>

## ISO/IEC 27002:2022-身份与访问控制

表 7-61 身份与访问控制风险项检查项目

检查项目	检查内容
确保管理员账号禁用AK/SK	<p>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。</p>
确保IAM密码策略要求符合密码复杂度	<p>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）。</p>
应避免根用户以外的IAM用户加入admin用户组，防止授权过大	<p>根用户以外的IAM用户加入admin用户组，视为“不合规”。“admin”为缺省用户组，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。</p>

检查项目	检查内容
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。
确保创建的IAM策略已正确附加到IAM用户、用户组或委托	IAM策略未附加到IAM用户、用户组或委托，视为“不合规”。避免长期存在未绑定的IAM策略，防止因管理疏漏引发计划外授权，从而导致恶意操作。长期未绑定的IAM策略，建议删除处理。
应确保CSMS轮转凭据启用自动轮转	如果长时间不更新凭据，凭据内保护的重要信息（例如：重要密码、令牌、证书、SSH密钥、API密钥等）的泄露风险也会增加，定期轮换凭据会增加所保护的明文信息安全性。
应确保CSMS凭据在指定天数内轮转	CSMS凭据可以配置轮转，可以使用轮转来将长期机密信息替换为短期机密信息。如果长时间不更新凭据，凭据内保护的重要信息（例如：重要密码、令牌、证书、SSH密钥、API密钥等）的泄露风险也会增加，轮转机密信息可以增加所保护的明文信息安全性、限制非授权用户使用被泄露机密信息的时间。因此，应该定期轮转CSMS凭据。PCI DSS要求至少每90天更改一次用户密码或凭据轮转。
确保禁用ACL，并使用OBS存储桶策略实现更精细的访问控制。	OBS提供多种权限控制方式，包括IAM权限、桶策略、对象ACL、桶ACL。访问控制列表（Access Control List, ACL）用于资源拥有者给其他账号授予资源的访问权限。OBS ACL是基于账号级别的读写权限控制，且主要用于授予基本的读/写权限，权限控制细粒度不如桶策略和IAM权限。一般情况下，建议使用IAM权限和桶策略进行访问控制。否则会泄露权限配置规则及相应的domain id, domain name。在特定的权限配置场景下，攻击者可能会根据泄露的权限配置规则，构造请求非法操作桶内资源。
确保IAM用户组已添加权限	IAM用户组未添加任意权限，视为“不合规”。管理员可以创建用户组，并给用户组授予策略或角色，然后将用户加入用户组，使得用户组中的用户获得相应的权限。如果您的用户组没有配置任何授权，则不会带来任何有效授权行为，建议您定时检查并清理无效的IAM用户组，提升运行和管理效率。
应确保配置了自动轮转的CSMS凭据轮转成功	CSMS凭据轮转成功或不涉及轮转，视为合规。当您为凭据开启轮转后，您需要确保轮转执行是成功的。如果轮转失败，可能导致以下问题：凭据泄露风险：长期不轮转的凭据更容易被攻击者获取，增加数据泄露或服务滥用的可能性。服务中断风险：轮转失败可能导致凭据过期，引发服务中断或应用故障。约束：该合规规则只检查定时轮转是否成功，不检查立即轮转是否成功。该合规规则受制于Config收集资源的实时性，可能存在最多不超过24小时的滞后。

检查项目	检查内容
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）。
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。
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）。

## ISO/IEC 27002:2022-数据安全

表 7-62 数据安全风险项检查项目

检查项目	检查内容
启用KMS 密钥轮换	启用密码安全中心（Data Encryption Workshop, DEW）密钥轮换策略，定期更换原密钥的密钥材料，提升加密密钥的安全性。

## ISO/IEC 27002:2022-应用安全

表 7-63 应用安全风险项检查项目

检查项目	检查内容
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，以实现指定国家、地区的来源 IP 的自定义访问控制。
应确保CDN回源方式使用HTTPS	如果CDN节点没有缓存该资源，就会回源请求资源并缓存到CDN节点。回源协议也应当设置为HTTPS以确保数据传输的安全。
GeminiDB实例开启错误日志	GeminiDB实例的日志管理功能支持查看数据库级别的错误日志，包括数据库运行的Warning和Error级别的信息，有助于您分析系统中存在的问题。
应确保WAF防护策略配置防护规则	WAF防护策略可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。确保防护策略不是空置状态，而是根据自己网站防护的需要，灵活配置防护规则，才能更好的防护您的网站业务。

检查项目	检查内容
GaussDB实例应开启错误日志	租户开启GaussDB错误日志功能后，可以通过分析GaussDB错误日志来定位错误原因。当前错误日志功能默认开启。
CSS集群开启慢日志	Elasticsearch和OpenSearch集群备份的日志文件主要包括废弃操作日志、运行日志、慢索引日志、慢查询日志，用户可以使用日志定位问题。CSS集群默认记录慢日志，建议保持开启，并将其转储在OBS桶中进行备份。
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。
确保开启DWS数据库审计日志	<p>DWS（数据仓库服务）支持数据库审计日志功能，可以记录用户对数据库的访问行为、SQL操作、权限变更等关键事件。通过开启审计日志功能，可以有效追踪和分析数据库的操作历史，及时发现和应对潜在的安全威胁。该规则旨在应对以下风险：未开启审计日志功能可能会导致无法追踪和监控数据库的操作行为。攻击者可能利用未审计的环境进行未授权的访问或恶意操作，进而窃取敏感数据或破坏数据库的完整性。此外，内部人员的误操作或恶意行为也可能导致数据泄露或损坏，而无法追溯。</p> <p>如未开启审计日志功能，可能会导致以下影响：无法追踪和分析数据库的操作行为，增加数据泄露和篡改的风险。此外，无法及时发现和应对潜在的安全威胁，影响数据库的稳定性和数据的完整性。审计日志的生成和存储可能会占用额外的存储空间，增加存储成本。</p>

检查项目	检查内容
应确保ER服务启用安全审计日志	<p>用户可以通过开启CTS服务来记录对CC服务操作的审计日志，开启审计日志对于保护信息安全、确保合规性、提高系统稳定性和透明度等方面都具有重要意义。</p> <ul style="list-style-type: none"><li>● 增强安全性：审计日志记录了系统中发生的所有重要操作，包括登录尝试、文件访问、配置更改等。通过分析这些日志，安全团队可以及时发现异常行为，比如未授权的访问尝试或恶意活动，从而采取措施防止潜在的安全威胁。</li><li>● 满足合规要求：许多行业标准和法律法规（如GDPR、HIPAA、SOX等）要求组织必须记录和保留特定类型的活动日志。开启审计日志有助于满足这些合规性要求，避免因不合规而面临的罚款或其他法律后果。</li><li>● 追责：在多用户环境中，审计日志能够记录每个用户的具体操作，这对于明确责任、防止内部欺诈行为非常重要。一旦发生问题，可以通过日志追踪到具体的操作者，便于进行责任追究。</li><li>● 提高透明度：对于外部审计或监管机构来说，审计日志提供了透明度，证明了组织在数据处理、安全管理和合规性方面的努力。这有助于建立信任，增强组织的声誉。</li></ul>
确保ELB监听器绑定的安全策略中使用安全的TLS版本和加密套件	<p>ELB（弹性负载均衡）支持在HTTPS或TLS监听器中配置安全策略，允许用户选择安全的TLS版本和加密套件。通过选择最新的TLS版本（如TLS1.2或TLS1.3）和强加密套件，ELB可以确保客户端与服务器之间的通信安全，防止数据在传输过程中被窃听或篡改。使用安全的TLS版本和加密套件可以应对中间人攻击、降级攻击、数据泄露等风险。如果未配置，则可能导致因使用旧版本TLS协议或加密套件导致的数据泄露与篡改，并且可能面临中间人攻击的风险。使用安全的TLS版本和加密套件可能导致兼容性问题，旧版本浏览器或客户端可能不支持最新的TLS版本。</p>
GaussDB实例应开启慢日志	<p>租户在开启GaussDB实例慢日志功能后，租户可以通过GaussDB慢日志定位SQL语句执行慢的问题。当前慢日志功能默认开启。</p>
使用桶策略限制对OBS桶的访问必须使用HTTPS协议	<p>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。</p>
RDS实例不应使用数据库引擎默认端口	<p>使用默认SQLServer端口容易被监听，存在安全隐患，推荐使用非默认端口。</p>

检查项目	检查内容
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FuctionGraph函数日志功能	开启函数日志功能后，用户函数每次调用执行日志都会保存在LTS，方便用户定位问题和记录函数执行过程。
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。
确保对IAM服务的操作已记录审计日志	<p>用户可以通过开启CTS服务来记录对IAM服务操作的审计日志，开启审计日志对于保护信息安全、确保合规性、提高系统稳定性和透明度等方面都具有重要意义。</p> <ul style="list-style-type: none"><li>● 增强安全性：审计日志记录了系统中发生的所有重要操作，包括登录尝试、文件访问、配置更改等。通过分析这些日志，安全团队可以及时发现异常行为，比如未授权的访问尝试或恶意活动，从而采取措施防止潜在的安全威胁。</li><li>● 满足合规要求：许多行业标准和法律法规（如 GDPR、HIPAA、SOX等）要求组织必须记录和保留特定类型的活动日志。开启审计日志有助于满足这些合规性要求，避免因不合规而面临的罚款或其他法律后果。</li><li>● 追责：在多用户环境中，审计日志能够记录每个用户的具体操作，这对于明确责任、防止内部欺诈行为非常重要。一旦发生问题，可以通过日志追踪到具体的操作者，便于进行责任追究。</li><li>● 提高透明度：对于外部审计或监管机构来说，审计日志提供了透明度，证明了组织在数据处理、安全管理和合规性方面的努力。这有助于建立信任，增强组织的声誉。</li></ul>
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。

检查项目	检查内容
CSS集群应启用HTTPS	CSS集群的安全模式下可以选择使用HTTP协议或者HTTPS协议。安全模式+HTTP协议的集群采用HTTP协议明文传输数据，优点是安全认证提升了集群安全性。通过HTTP协议访问集群又能保留集群的高性能。支持用户权限隔离。缺点是不支持启用公网访问。适合对安全性有一定要求，但对性能要求较高的场景。安全模式+HTTPS协议的集群采用HTTPS协议进行通信加密，使数据更安全。优点是安全认证提升了集群安全性。HTTPS协议提升了集群公网访问的安全性。支持用户权限隔离。缺点是与HTTP协议相比，通过HTTPS协议访问集群会因加密和解密操作导致集群的读写性能有所下降。适合对安全性和数据传输加密要求较高、且需要公网访问的场景。在对性能要求不高、且需要公网访问的场景，建议使用安全模式+HTTPS模式协议。
确保弹性伸缩组使用弹性负载均衡健康检查	华为云弹性伸缩服务（Auto Scaling, AS）与弹性负载均衡（Elastic Load Balance, ELB）结合使用时，可以自动调整计算资源，以适应业务负载的变化。通过配置ELB健康检查，可以确保只有健康状态的实例参与负载均衡，从而提高服务的可用性和稳定性。健康检查功能会定期检查后端服务器的健康状态，一旦发现异常，会自动将流量重定向到其他健康的实例，避免了单点故障对业务的影响。不使用ELB健康检查可能会导致异常的实例继续接收流量，影响用户体验和业务连续性。在高并发场景下，异常实例可能会成为性能瓶颈，甚至导致整个服务不可用。此外，未及时发现和隔离故障实例，还可能增加安全风险，如被攻击者利用进行DDoS攻击等。若不使用健康检查，则异常实例可能继续接收流量，可导致用户请求失败或响应时间增加，并同时造成资源的浪费。同时，未及时隔离并清理故障实例，可导致实例被攻击者利用，增加安全风险。若健康检查频率设置不当，可能导致健康检查频率过高，增加负载并影响性能。
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。
RDS实例开启慢日志	查询慢日志用来记录执行时间超过当前慢日志阈值“long_query_time”（默认是1秒）的语句，您可以通过慢查询日志的日志明细，查找出执行效率低的语句，进行优化。您也可以下载慢查询日志进行业务分析。
应确保启用Web应用防火墙功能	Web应用防火墙（Web Application Firewall, WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

检查项目	检查内容
应确保配置安全的TLS版本	传输层安全性协议（TLS: Transport Layer Security），是一种安全协议，目的是为互联网通信提供安全及数据完整性保障，最典型的应用就是HTTPS。目前，有四个版本的TLS协议：TLS1.0/1.1/1.2/1.3，版本越高，安全性相对更高，但是对老版本的浏览器兼容性相对较差。
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。
GeminiDB实例开启慢查询日志	GeminiDB实例的日志管理功能支持查看数据库级别的慢日志，执行时间的单位为ms。通过该日志，可查找出执行效率低的语句，以便优化。
应确保WAF防护域名配置防护策略	WAF防护策略可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。确保防护策略不是空置状态，而是根据自己网站防护的需要，灵活配置防护规则，才能更好的防护您的网站业务。

## ISO/IEC 27002:2022-运维和运营安全

表 7-64 运维和运营安全风险项检查项目

检查项目	检查内容
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。
RDS数据库实例应将日志发布至日志跟踪服务（LTS）	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SQLServer日志数据，应在 LTS 中配置日志转储。

检查项目	检查内容
启用CES资源告警功能	云监控服务(CES)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。告警功能提供对监控指标的告警功能,用户对云服务的核心监控指标设置告警规则,当监控指标触发用户设置的告警条件时,支持以邮箱、短信、HTTP、HTTPS等方式通知用户,让用户在第一时间得知云服务发生异常,迅速处理故障,避免因资源问题造成业务损失。该服务应对的主要风险包括资源使用异常、业务性能下降及潜在故障风险。如果告警功能未能启用或配置不当,可能导致用户无法及时察觉资源问题,进而影响业务运行的稳定性,甚至可能造成业务停机、数据丢失或财务损失。因此,确保告警机制的正常运作对于云环境中的资源管理和故障响应至关重要。
PostgreSQL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。
配置监控KMS禁用或计划删除密钥的事件监控告警	CES配置监控KMS禁用或计划删除密钥的事件监控告警,旨在提供对关键云资源安全事件的实时监控与响应。通过事件监控功能,用户能够对云环境中重要的操作事件进行数据上报和查询,尤其是针对KMS密钥禁用或删除的高风险操作。一旦发生此类事件,系统将触发告警,并通过多种通知方式及时提醒用户,确保其能够迅速采取措施防止潜在的安全风险。此功能主要应对的风险是密钥管理不当带来的安全隐患,包括未经授权的密钥禁用、删除或其他操作,可能导致加密数据泄露、身份验证失败或数据完整性受损,请确保配置CES配置监控KMS禁用或计划删除密钥的事件监控告警。
TaurusDB实例开启慢日志	慢日志用来记录执行时间超过当前慢日志阈值“long_query_time”(默认是10秒)的语句,建议设置为1s,锁等待时间不计算在执行时间内。您可以通过查询慢日志的日志明细、统计分析情况,查找出执行效率低的语句,进行优化。
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。

检查项目	检查内容
确保APIG专享版实例配置访问日志	APIG提供了API的可视化分析和统计能力，支持查看API的调用日志。可以带来如下好处：异常检测：通过审计日志，识别异常访问行为，如频繁失败请求、异常IP等，及时发现潜在攻击；问题定位：通过日志快速定位API调用失败的原因，如参数错误、服务不可用等；用户行为分析：分析API调用模式，了解用户行为，支持产品优化；资源使用监控：监控API调用频率和资源消耗，防止资源浪费。
配置监控OBS桶策略变更的事件监控告警	CES配置监控OBS桶策略变更的事件监控告警，旨在帮助用户实时监控和响应对云存储资源的安全操作，特别是针对OBS桶策略变更的事件。通过事件监控功能，用户能够收集和上报业务中的关键事件及对云资源的操作记录，一旦发现OBS桶策略发生变更，系统会立即触发告警并通知用户，帮助用户及时进行干预，确保数据存储的安全性和合规性。该服务主要应对对象存储桶策略的误配置或恶意修改，可能导致数据泄露、权限滥用或资源滥用等风险。因此，应确保CES配置监控OBS桶策略变更的事件监控告警。
CES配置监控VPC变更的事件监控告警	CES配置监控VPC变更的事件监控告警，可以帮助用户实时监控和响应VPC中网络架构的关键变化。通过事件监控功能，用户能够对VPC相关的操作事件进行数据上报和查询，尤其是针对删除VPC、修改VPC等操作。一旦发生这些高风险的配置变更，系统将触发告警，及时通知用户，帮助其快速审查和采取必要的安全措施，确保网络架构的稳定和安全。如果未及时监控VPC的配置变更，可能会导致关键网络组件暴露或无法访问，进而影响云环境中的其他服务和资源。确保VPC变更事件得到及时监控和告警，对于防止不必要的网络安全漏洞和保障业务的正常运行至关重要。
确保已开启DWS数据库审计日志转储	DWS（数据仓库服务）具备审计日志转储功能，该功能能够记录用户对数据库的所有操作行为，包括查询、修改、删除等，并将这些日志转储到指定的存储系统（如OBS对象存储服务）。通过审计日志转储，可以有效应对未经授权的数据库访问、潜在的安全威胁以及内部人员的不当操作风险。如果不开启审计日志转储，将无法及时发现和追踪数据库的异常操作，可能导致数据泄露、篡改或删除等安全事件，影响业务的合规性和数据的完整性。在开启审计日志转储后，可能会对存储资源和网络带宽产生一定影响，因此建议根据实际需求合理配置日志转储策略。

检查项目	检查内容
TaurusDB实例开启审计日志	数据库审计日志是数据库安全管理和运维的重要工具，它能够提供全面的安全监控、满足合规性要求、辅助故障诊断、支持业务分析，并帮助实现有效的风险管控，虽然会带来一定的性能和存储成本，但对保障数据库安全和合规运营具有不可替代的价值。
GaussDB应开启数据库审计日志功能	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。
应确保DDoS原生基础防护开启LTS日志记录	启用Anti-DDoS防护功能后，您可以将攻击日志记录到云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的Anti-DDoS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。
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。

## ISO/IEC 27002:2022-治理和策略

表 7-65 治理和策略风险项检查项目

检查项目	检查内容
GaussDB应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。
CSS集群至少包含3个数据节点	为防止数据丢失，并确保在服务中断情况下能降低集群的停机时间，从而增强集群的高可用性，请确保CSS集群的实例个数大于2个。部署至少3个实例，可以确保当一个节点发生故障时，集群能够正常运行。

检查项目	检查内容
确保ELB实例多AZ部署	ELB（弹性负载均衡）支持多AZ（可用区）部署，允许用户将ELB实例部署在多个可用区。通过多AZ部署，ELB可以提高服务的可用性和容灾能力，确保在某个可用区发生故障时，服务仍可通过其他可用区继续提供。采用多AZ部署可以应对单点/区域故障、负载不均等风险。若未采用多AZ部署，则服务可能因可用区或可用区ELB实例发生故障而中断，并且可能会导致流量分布不均的问题。多AZ部署会导致网络流量经过更长的网络路径，可能增加数据传输的延迟，并导致云服务网络成本的上升。
CSS集群应启用快照	为避免数据丢失，您可以将集群的索引数据进行备份，当数据发生丢失或者想找回某一时间段数据时，您可以通过恢复索引操作快速获得数据。索引的备份是通过创建集群快照实现。第一次备份时，建议将所有索引数据进行备份。CSS服务的快照备份功能提供数据保护和恢复能力。通过快照备份，可以将集群的数据状态保存到OBS桶中，以便在需要进行恢复。CSS集群快照分为两种方式：自动创建快照和手动创建快照。影响：当使用快照备份功能时，备份的快照存储在OBS桶中需要额外收费。集群快照会导致CPU、磁盘IO上升等影响，建议在业务低峰期进行操作。
确保弹性伸缩组创建的ECS实例覆盖多AZ	华为云弹性伸缩组（AS）支持将新创建的ECS实例分布到多个可用区（AZ）。每个AZ是具备独立风火水电设施的物理数据中心隔离单元，同一Region内的多个AZ通过高速光纤互联，这是构建高可用应用架构的基础。配置伸缩组使用多AZ部署，核心目的是应对单AZ故障风险。如果所有ECS实例都集中在单个AZ内，一旦该AZ因基础设施故障（如断电、断网）或自然灾害发生中断，将导致整个伸缩组内的实例不可用，业务服务完全中断，丧失连续性。即使伸缩组状态正常，如果所选AZ不支持伸缩配置中指定的ECS实例类型，可能导致伸缩组无法使用或扩容活动异常，资源弹性扩展能力受限。此外，即使部分AZ支持所需实例类型，扩容时实例也无法均匀分布，削弱了跨AZ的高可用性。启用此规则（即配置多AZ）后，主要业务影响体现在跨AZ通信会引入轻微的网络时延增加（相比同AZ内通信），对于网络时延要求极高的业务（如毫秒级响应的金融交易系统）可能需注意。同时，配置时需确保所选的所有AZ都支持您需要的ECS实例类型，否则扩容仍可能集中在支持的AZ中，达不到理想的均匀分布效果。因此，建议在创建伸缩组时至少选择2个可用区，并优先采用“均衡分布”扩展策略，以实现最佳的高可用性。

检查项目	检查内容
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。
RDS数据库实例应配置多可用区部署	SQLServer实例部署在不同的可用区，可提高容灾能力。
RDS数据库集群应配置多可用区部署	SQLServer集群/主备节点部署在不同的可用区，可提高集群/主备实例的容灾能力。
确保DWS集群启用自动快照	华为云DWS服务支持自动快照功能，能够定期自动创建集群的数据备份。这些快照可以用于在集群发生故障或数据损坏时，快速恢复数据，确保业务的连续性。通过启用自动快照，用户可以有效保护数据，防止数据丢失。如果DWS集群没有启用自动快照，则DWS集群将无法自动创建数据备份。一旦发生硬件故障、人为错误或恶意攻击导致数据丢失，将无法快速恢复数据，导致业务中断和数据损失。此外，缺乏定期备份还可能导致数据无法恢复到最近的稳定状态，增加数据丢失的风险。虽然自动快照提供了数据保护，但频繁的快照创建可能会占用更多的存储空间，增加存储成本。

## 7.2 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 7-66 内置剧本

安全防线	剧本名	描述
主机安全	主机告警状态同步	自动同步主机告警状态
	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
	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
	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

安全防线	剧本名	描述
	HSS文件隔离查杀	自动隔离查杀恶意软件
	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
	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
	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
	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
	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，则通知客户并生成待办，如果人工审核通过则加入安全云脑VPC策略阻断
	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
	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
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
	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
	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
	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，生成拦截待办，待办人工审核通过后会该IP加入安全云脑WAF阻断策略中
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
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
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
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

安全防线	剧本名	描述
	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
	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
	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
	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
	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）
	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
	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
	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)
	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
	同步CFW黑IP到情报	将CFW的黑IP同步到云脑的情报管理中
	同步WAF黑IP到情报	将WAF的黑IP同步到云脑的情报管理中
其他/通用	凭据泄露响应	针对用户凭据（如账号密码、AK&SK、委托账号）泄露的场景，进行自动化停用AK&SK、停用IAM用户、修改Agency被委托账号为当前账号。
其他/通用	高危告警WAF自动处置	安全云脑提供的“高危告警WAF自动处置”剧本，剧本已匹配“高危告警WAF自动处置”流程。该剧本会自动获取CloudTIC（华为云平台侧情报中心）中WAF的IP情报，针对“威胁度”为“黑”且“置信度”大于70的IP情报（判定为有风险的IP情报）进行自动封堵IP并新增IP情报指标。针对“威胁度”为“白”或“置信度”小于30的IP情报（判定为低风险的IP情报）自动关闭告警并自动新增IP情报指标。
其他/通用	异常AccessKey泄露风险扫描	“异常AccessKey泄露风险扫描”剧本已关联“异常AccessKey泄露风险扫描”流程，剧本实现每天0点定时扫描GitHub是否存在泄露的AKSK，若存在泄露的AKSK则在安全云脑自动新增一条“AKSK风险类型”的攻击。

## 7.3 内置类型

本章节介绍安全云脑支持的内置告警类型、内置事件类型、内置威胁情报类型、内置漏洞类型。

### 内置告警类型

表 7-67 内置告警类型列表

类型名称	子类型/子类型标识	描述
DDoS攻击	DNS协议攻击 Tcp Dns	DNS协议攻击
	异常端口通信 Unusual Network Port	异常端口通信
	异常协议攻击 Unusual Protocol	异常协议攻击
	ACK Flood ACK Flood	ACK Flood
	BGP Flood攻击 BGP Flood Attack	BGP Flood攻击
	DNS IP TTL DNS IP TTL Check Fail	DNS IP TTL
	DNS Reply Flood 攻击 DNS Reply Flood	DNS Reply Flood 攻击
	DNS查询攻击 DNS Query Flood	DNS查询攻击
	DNS大小异常 DNS Size Abnormal	DNS大小异常
	DNS反射 DNS Reflection	DNS反射
	DNS返回域名流异常 DNS Reply Domain Flow Abnormal	DNS返回域名流异常
	DNS格式错误 DNS Format Error	DNS格式错误
DNS缓存匹配 DNS Cache Match	DNS缓存匹配	

类型名称	子类型/子类型标识	描述
	DNS缓存投毒 DNS Cache Poisoning	DNS缓存投毒
	DNS请求域名流异常 DNS Request Domain Flow Abnormal	DNS请求域名流异常
	DNS无效域名 DNS No Such Name	DNS无效域名
	FIN/RST Flood FIN/RST Flood	FIN/RST Flood
	HTTPS Flood HTTPS Flood	HTTPS Flood
	HTTP慢速攻击 HTTP Slow Attack	HTTP慢速攻击
	ICMP协议封禁 ICMP Protocol Block	ICMP协议封禁
	IP信誉 IP Reputation	IP信誉
	SIP Flood SIP Flood	SIP Flood
	SIP源速率异常 SIP Source Rate Abnormity	SIP源速率异常
	SYN Flood SYN Flood	SYN Flood
	SYN-ACK Flood SYN-ACK Flood	SYN-ACK Flood
	TCP带宽溢出 TCP Bandwidth Overflow	TCP带宽溢出
	TCP多连接攻击 TCP Connection Flood	TCP多连接攻击
	TCP分片带宽溢出 TCP Fragment Bandwidth Overflow	TCP分片带宽溢出
	TCP分片攻击 TCP Fragment Flood	TCP分片攻击

类型名称	子类型/子类型标识	描述
	TCP畸形报文 TCP Malformed	TCP畸形报文
	TCP认证UDP攻击 TCP-authenticated UDP Attack	TCP认证UDP攻击
	TCP协议封禁 TCP Protocol Block	TCP协议封禁
	UDP带宽溢出 UDP Bandwidth Overflow	UDP带宽溢出
	UDP分片 UDP Fragment Flood	UDP分片
	UDP分片带宽溢出 UDP Fragment Bandwidth Overflow	UDP分片带宽溢出
	UDP畸形报文 UDP Malformed	UDP畸形报文
	UDP协议封禁 UDP Protocol Block	UDP协议封禁
	URI监控 URI Monitor	URI监控
	暗网IP Dark IP	暗网IP
	单IP带宽溢出 Single IP Bandwidth Overflow	单IP带宽溢出
	当前连接耗尽攻击 Concurrent Connections Flood	当前连接耗尽攻击
	端口扫描攻击 Port Scanning Attack	端口扫描攻击
	恶意域名攻击 Malicious Domains Attack	恶意域名攻击
	反恶意软件 Anti-Malware	反恶意软件

类型名称	子类型/子类型标识	描述
	分布式拒绝服务攻击 DDoS	分布式拒绝服务攻击
	分区带宽溢出 Zone Bandwidth Overflow	分区带宽溢出
	过滤器攻击 Filter Attack	过滤器攻击
	黑名单 Blacklist	黑名单
	僵尸网络/特洛伊木马/蠕虫 Botnets/Trojan horses/ Worms Attack	僵尸网络/特洛伊木马/蠕虫
	目的IP新会话限速 Destination IP new session rate limiting	目的IP新会话限速
	其他Flood攻击 Other Flood	其他Flood攻击
	其他带宽溢出 Other Bandwidth Overflow	其他带宽溢出
	其他全局异常 Global Other Abnormal	其他全局异常
	其他协议封禁 Other Protocol Block	其他协议封禁
	全局ICMP异常 Global ICMP Abnormal	全局ICMP异常
	全局TCP分片异常 Global TCP Fragment Abnormal	全局TCP分片异常
	全局TCP异常 Global TCP Abnormal	全局TCP异常
	全局UDP分片异常 Global UDP Fragment Abnormal	全局UDP分片异常

类型名称	子类型/子类型标识	描述
	全局UDP异常 Global UDP Abnormal	全局UDP异常
	网页攻击 Web Attack	网页攻击
	位置攻击 Location Attack	位置攻击
	新连接耗尽攻击 New Connections Flood	新连接耗尽攻击
	域名劫持 Domain Hijacking	域名劫持
	源DNS返回流异常 Source DNS Reply Flow Abnormal	源DNS返回流异常
	源DNS请求流异常 Source DNS Request Flow Abnormal	源DNS请求流异常
	主机流量溢出 Host Traffic Over Flow	主机流量溢出
	HTTP Flood HTTP Flood	HTTP Flood
	ICMP Flood ICMP Flood	ICMP Flood
	SSL Flood SSL Flood	SSL Flood
	TCP Flood TCP Flood	TCP Flood
	UDP Flood UDP Flood	UDP Flood
	XML Flood XML Flood	XML Flood
	放大攻击 Amplification	放大攻击
Web恶意代码	网页暗链 Web Page Dark Link	网页暗链

类型名称	子类型/子类型标识	描述
	网页挂马 Web Page Trojan	网页挂马
Web攻击	Webshell Webshell	Webshell
	WAF机器人 WAF Robot	WAF机器人
	白名单IP White IP	白名单IP
	攻击惩罚 Known Attack Source	攻击惩罚
	黑名单IP Black IP	黑名单IP
	漏洞攻击 Vulnerability Attack	漏洞攻击
	命中隐私泄露规则 Leakage	命中隐私泄露规则
	默认 Default	默认
	扫描/爬虫 Scanner & Crawler	扫描/爬虫
	CC攻击 Challenge Collapsar	CC攻击
	IP信誉库 IP Reputation	IP信誉库
	SQL注入 SQL Injection	SQL注入
	XSS Cross-Site Scripting	XSS
	本地文件包含 Local Code Inclusion	本地文件包含
地理访问控制拦截 Geo IP	地理访问控制拦截	
恶意爬虫 Malicious Web Crawlers	恶意爬虫	

类型名称	子类型/子类型标识	描述
	反爬虫 Anticrawler	反爬虫
	防篡改 AntiTamper	防篡改
	非法请求 Illegal Access	非法请求
	黑白名单拦截 White or Black IP	黑白名单拦截
	精准防护 Custom Rule	精准防护
	命令注入 Command Injection	命令注入
	目录遍历 Path Traversal	目录遍历
	网站木马 Website Trojan	网站木马
	网站信息防泄露 Information Leakage	网站信息防泄露
	网站信息泄露 Web Service Exfiltration	网站信息泄露
	远程代码执行 Remote Code Execute	远程代码执行
	远程文件包含 Remote Code Inclusion	远程文件包含
恶意软件	加密货币挖矿 Cryptomining	加密货币挖矿
	Docker恶意程序 Docker Malware	Docker恶意程序
	钓鱼 Phishing	钓鱼
	恶意广告软件 Adware	恶意广告软件
	恶意软件 Malicious Software	恶意软件

类型名称	子类型/子类型标识	描述
	黑客工具 Hacktool	黑客工具
	灰色软件 Grayware	灰色软件
	间谍软件 Spyware	间谍软件
	垃圾邮件 Spam	垃圾邮件
	Rootkit Rootkit	Rootkit
	Webshell Webshell	Webshell
	病毒、蠕虫 Virus and Worm	病毒、蠕虫
	恶意文件 Malicious File	恶意文件
	反弹shell Reverse Shell	反弹shell
	后门木马 Backdoor Trojan	后门木马
	僵尸网络程序 Botnet Program	僵尸网络程序
	勒索软件 Ransomware	勒索软件
	挖矿程序 Bitcoin Miner	挖矿程序
	挖矿软件 Mining Software	挖矿软件
风险审计	Webcms漏洞 Webcms Vulnerability	Webcms漏洞
	Windows OS 漏洞 Windows Vulnerability	Windows OS 漏洞

类型名称	子类型/子类型标识	描述
	本地访问漏洞 Local Access Vulnerability	本地访问漏洞
	错误配置策略 Mis-Configured Policy	错误配置策略
	其它OS漏洞 Other OS Vulnerability	其它OS漏洞
	其它漏洞 Other Vulnerability	其它漏洞
	应用程序漏洞 Application Vulnerability	应用程序漏洞
	远程访问漏洞 Remote Access Vulnerability	远程访问漏洞
风险审计	弱口令 Weak Password	弱口令
	系统风险配置 System Risk Configuration	系统风险配置
攻击探测	钓鱼 Phishing	钓鱼
	网络拓扑构建 Map Network Topology	网络拓扑构建
	账户、组信息收集 Identify Groups/Roles	账户、组信息收集
	指纹扫描 Fingerprinting	指纹扫描
	主机发现 Determine IP Address	主机发现

类型名称	子类型/子类型标识	描述
漏洞利用	ActiveX漏洞利用 ActiveX Exploit	ActiveX漏洞利用
	CGI攻击 CGI Attack	CGI攻击
	DNS漏洞利用 DNS Exploit	DNS漏洞利用
	FTP漏洞利用 FTP Exploit	FTP漏洞利用
	Hadoop漏洞利用 Hadoop Vulnerability Exploit	Hadoop漏洞利用
	Hypervisor漏洞利用 Hypervisor Exploit	Hypervisor漏洞利用
	LDAP注入攻击 LDAP Injection Attack	LDAP注入攻击
	MacOS漏洞利用 MacOS Exploit	MacOS漏洞利用
	MySQL漏洞利用 MySQL Vulnerability Exploit	MySQL漏洞利用
	Office软件漏洞利用 Office Exploit	Office软件漏洞利用
	Redis漏洞利用 Redis Vulnerability Exploit	Redis漏洞利用
	RPC漏洞利用 RPC Exploit	RPC漏洞利用
	SQL注入 SQL Injection	SQL注入
	SSH漏洞利用 SSH Exploit	SSH漏洞利用
	SSI注入攻击 SSI Injection Attack	SSI注入攻击
Struts2 OGNL注入 Struts2 OGNL Injection	Struts2 OGNL注入	

类型名称	子类型/子类型标识	描述
	Telnet漏洞利用 TELNET Exploit	Telnet漏洞利用
	Unix漏洞利用 Unix Exploit	Unix漏洞利用
	Web漏洞利用 Web Exploit	Web漏洞利用
	XSS攻击 Cross-Site Scripting	XSS攻击
	本地文件包含 Local File Inclusion	本地文件包含
	恶意文件投递 Malicious File Delivery	恶意文件投递
	恶意文件执行 Malicious File Execution	恶意文件执行
	缓冲区溢出攻击 Buffer Overflow	缓冲区溢出攻击
	会话劫持 Session Hijack	会话劫持
	口令猜测 Password Cracking	口令猜测
	浏览器漏洞利用 Browser Exploit	浏览器漏洞利用
	弱口令访问 Weak Password Access	弱口令访问
	数据库漏洞利用 Database Exploit	数据库漏洞利用
	未知漏洞利用 Unknown Exploit	未知漏洞利用
	隐藏链接访问 Hide Link Access	隐藏链接访问
	邮件漏洞利用 Mail Exploit	邮件漏洞利用
	远程代码执行 Remote Code Execution	远程代码执行

类型名称	子类型/子类型标识	描述
	远程访问漏洞利用 Remote Access Exploit	远程访问漏洞利用
	远程文件包含攻击 Remote File Inclusion	远程文件包含攻击
	远程文件注入 Remote File Injection	远程文件注入
	组合漏洞利用 Misc Exploit	组合漏洞利用
	CMS漏洞 CMS Exploit	CMS漏洞
	CSRF攻击 CSRF Attack	CSRF攻击
	JNDI注入攻击 JNDI Injection Attack	JNDI注入攻击
	Linux漏洞 Linux Exploit	Linux漏洞
	SMB漏洞 SMB Exploit	SMB漏洞
	Windows漏洞 Windows Exploit	Windows漏洞
	XML注入 XML Injection	XML注入
	代码注入 Code Injection	代码注入
	漏洞逃逸攻击 Vulnerability Escape Attack	漏洞逃逸攻击
	命令执行 Command Execution	命令执行
	命令注入 Command Injection	命令注入
	文件逃逸攻击 File Escape Attack	文件逃逸攻击

类型名称	子类型/子类型标识	描述
	虚拟机逃逸攻击 VM Escape Attack	虚拟机逃逸攻击
	一般漏洞利用 General Exploit	一般漏洞利用
命令与控制	ECS存在当前IP被用于向高危网络发送消息 Command Control Activity	ECS存在当前IP被用于向高危网络发送消息
	可疑的域名、IP地址、端口动态生成访问 Dynamic Resolution	可疑的域名、IP地址、端口动态生成访问
	其他可疑连接 Abnormal Connection	其他可疑连接
	其他可疑行为 Abnormal Behavior	其他可疑行为
	外连恶意DNS Malicious Domain Query	外连恶意DNS
	外连恶意IP地址 Malicious Ip Address Query	外连恶意IP地址
	隐蔽隧道 Protocol Tunneling	隐蔽隧道
	与矿池地址通信 Mining Pool Communication	与矿池地址通信
其他	公共舆情 Public_Opinion	公共舆情
	云防火墙攻击 CFW_RISK	云防火墙攻击
数据泄露	数据窃取 Steal Data	数据窃取
	违规外传 Transfer Data Abnormal	违规外传

类型名称	子类型/子类型标识	描述
网络异常行为	IP访问频率异常 IP Access Frequency Abnormal	IP访问频率异常
	IP切换异常 IP Switch Abnormal	IP切换异常
	IP首次访问 IP First Access	IP首次访问
	Sinkhole攻击IP访问 Sink Hole	Sinkhole攻击IP访问
	代理IP访问 Proxy	代理IP访问
	恶意资源访问 Resource Permissions	恶意资源访问
	欺诈付款网站IP/域名访问 Payment	欺诈付款网站IP/域名访问
	洋葱网络IP访问 Tor	洋葱网络IP访问
	C&C异常通信 C&C Abnormal Communication	C&C异常通信
	IP黑名单访问 IP Blacklist Access	IP黑名单访问
	URL黑名单访问 URL Blacklist Access	URL黑名单访问
	恶意URL访问 Malicious URL Access	恶意URL访问
	恶意域名访问 Malicious Domain Name Access	恶意域名访问
	非授权访问企图 Unauthorized Access Attempt	非授权访问企图
可疑的网络流量 Suspicious Network Traffic	可疑的网络流量	

类型名称	子类型/子类型标识	描述
	容器网络外联 Container Network Connect	容器网络外联
	未知网络访问 Unknown Abnormal Network Access	未知网络访问
	文件MD5黑名单访问 File MD5 Blacklist Access	文件MD5黑名单访问
	异常外联行为 Abnormal External Behavior	异常外联行为
	域名黑名单访问 Domain Name Blacklist Access	域名黑名单访问
	周期外联通信 Periodic Outreach	周期外联通信
	可疑的端口转发 Suspicious Port Forward	可疑的端口转发
无文件攻击	VDSO劫持 VDSO Hijacking	VDSO劫持
	动态库注入进程 Dynamic Library Inject Process	动态库注入进程
	关键配置变更 Critical File Change	关键配置变更
	环境变量变更 Environment Change	环境变量变更
	进程注入 Process Inject	进程注入
	内存文件进程 Memfd Process	内存文件进程
	文件操纵 File Manipulation	文件操纵

类型名称	子类型/子类型标识	描述
系统行为异常	Crontab可疑任务 Crontab Suspicious Task	Crontab可疑任务
	Socket连接异常 Abnormal Socket Connection	Socket连接异常
	备份删除 Backup Deletion	备份删除
	非法数据库访问 Unauthorized Database Access	非法数据库访问
	权限异常访问 Privilege Abnormal Access	权限异常访问
	日志异常变化 Unexpected Log Change	日志异常变化
	容器进程退出 Container Process Exist	容器进程退出
	未知主机异常行为 Unknown Host Abnormal Activity	未知主机异常行为
	文件黑名单访问 File blacklist access	文件黑名单访问
	文件权限异常改变 Unexpected File Permission Change	文件权限异常改变
	系统安全防护被禁用 System Security Protection disabled	系统安全防护被禁用
	系统账号变更 System Account Change	系统账号变更
	异常注册表操作 Abnormal Registry Operation	异常注册表操作
	Crontab脚本提权 Crontab Script Privilege Escalation	Crontab脚本提权

类型名称	子类型/子类型标识	描述
	Crontab脚本修改 Crontab Script Change	Crontab脚本修改
	高危命令执行 High-risk Command Execution	高危命令执行
	高危系统调用 High-Risk Syscall	高危系统调用
	关键文件/目录变更 File/Directory Change	关键文件/目录变更
	关键文件变更 Key File Change	关键文件变更
	进程提权 Process Privilege Escalation	进程提权
	进程异常行为 Process Abnormal Activity	进程异常行为
	敏感文件访问 Sensitive File Access	敏感文件访问
	容器进程异常 Container Abnormal Process	容器进程异常
	容器异常启动 Container Abnormal Start	容器异常启动
	数据库连接异常 Abnormal Database Connection	数据库连接异常
	网卡混杂模式 Network Adapter Promiscuous Mode	网卡混杂模式
	文件提权 File Privilege Escalation	文件提权
	文件异常删除 File Abnormal Delete	文件异常删除

类型名称	子类型/子类型标识	描述
	系统启动脚本改变 System Start Script Change	系统启动脚本改变
	异常shell Abnormal Shell	异常shell
	异常命令执行 Abnormal Command Execution	异常命令执行
信息破坏	信息篡改 Information Tampering	信息篡改
	信息丢失 Information Loss	信息丢失
	信息假冒 Information Masquerading	信息假冒
	信息窃取 Information Interception	信息窃取
	信息泄露 Information Disclosure	信息泄露
	Linux网页篡改 Linux Web Page Tampering	Linux网页篡改
	Windows网页篡改 Windows Web Page Tampering	Windows网页篡改
	目录遍历 Directory Traversal	目录遍历
用户行为异常	Token恶意利用 Token Leakage	Token恶意利用
	Token恶意利用成功 Token Leakage Success	Token恶意利用成功
	异常用户首次访问 User First Cross Domain Access	异常用户首次访问

类型名称	子类型/子类型标识	描述
	用户访问频率异常 User Access Frequency Abnormal	用户访问频率异常
	用户访问时段异常 User Hour Level Access Abnormal	用户访问时段异常
	用户使用特定IP下载行为异常 User IP Download Abnormal	用户使用特定IP下载行为异常
	用户首次访问桶对象 Client First Access	用户首次访问桶对象
	用户下载行为异常 User Download Abnormal	用户下载行为异常
	暴力破解 Brute Force Cracking	暴力破解
	违规登录 Illegal Login	违规登录
	未知用户异常行为 Unknown User Abnormal Activity	未知用户异常行为
	异常登录 Abnormal Login	异常登录
	用户登录尝试 User Login Attempt	用户登录尝试
	用户密码窃取 User Password Theft	用户密码窃取
	用户权限提升成功 User Privilege Escalation Succeeded	用户权限提升成功
	用户权限提升失败 User Privilege Escalation Failed	用户权限提升失败
	用户首次登录 User First login	用户首次登录

类型名称	子类型/子类型标识	描述
	用户账号删除 User Account Removed	用户账号删除
	用户账号添加 User Account Added	用户账号添加
	用户组变更 User Group Changed	用户组变更
	用户组删除 User Group Removed	用户组删除
	用户组添加 User Group Added	用户组添加
	账号伪造 Account Forgery	账号伪造
	ECS可疑账号创建 Suspicious Ecs User Create	ECS可疑账号创建
	ECS账号权限修改 ECS User Escalate Privilege	ECS账号权限修改
	IAM可疑账号创建 Suspicious IAM Account Create	IAM可疑账号创建
	IAM账号权限修改 IAM Permissions Escalation	IAM账号权限修改
	暴力破解登录ECS ECS BruteForce Login	暴力破解登录ECS
	暴力破解登录IAM IAM BruteForce Login	暴力破解登录IAM
	非法系统账号 Invalid System Account	非法系统账号
	风险账号 Risky Account	风险账号
	可疑IP登录ECS Suspicious IP Address Login	可疑IP登录ECS

类型名称	子类型/子类型标识	描述
	可疑IP登录IAM Suspicious IP Address Login	可疑IP登录IAM
	异常登录IAM IAM Abnormal Login	异常登录IAM
	异地登录ECS Instance Credential Exfiltration	异地登录ECS
	用户登录成功 User Login Success	用户登录成功
	用户登录拒绝 User Login Denied	用户登录拒绝
	用户账号变更 User Account Changed	用户账号变更
资源操控	恶意逻辑插入 Malicious Logic Insertion	恶意逻辑插入
	基础设施操纵 Infrastructure Manipulation	基础设施操纵
	配置/环境操纵 Configuration/ Environment Manipulation	配置/环境操纵
	容器逃逸 Container Escape	容器逃逸
	容器资源操纵 Container Resource Manipulation	容器资源操纵
	软件完整性 Software Integrity Attack	软件完整性
资源侦查	端口探测数量异常 Port Detection	端口探测数量异常
	ARP 扫描 ARP Scan	ARP 扫描

类型名称	子类型/子类型标识	描述
	DNS探测 DNS Recon	DNS探测
	Hypervisor探测 Hypervisor Recon	Hypervisor探测
	ICMP探测 ICMP Recon	ICMP探测
	Linux探测 Linux Recon	Linux探测
	MacOS探测 MacOS Recon	MacOS探测
	NMAP扫描 NMAP Scan	NMAP扫描
	RPC请求探测 RPC Recon	RPC请求探测
	SNMP扫描 SNMP Recon	SNMP扫描
	TCP扫描 TCP Recon	TCP扫描
	UDP扫描 UDP Recon	UDP扫描
	Unix探测 Unix Recon	Unix探测
	WEB探测 Web Recon	WEB探测
	Windows探测 Windows Recon	Windows探测
	加密渗透扫描 Encrypted Penetration Scan	加密渗透扫描
	普通扫描事件 General Scanner	普通扫描事件
	数据库探测 Database Recon	数据库探测

类型名称	子类型/子类型标识	描述
	邮件探测 Mail Recon	邮件探测
	主机扫描 Host Scan	主机扫描
	组合探测 Misc Recon	组合探测
	端口扫描 Port Scan	端口扫描

## 告警类型相关操作

- 告警的基本概念请参见[运营对象管理概述](#)。
- 告警类型支持查看、新增、编辑、启用、禁用、删除操作，详细操作指导请参见[管理告警类型](#)。

## 内置事件类型

表 7-68 内置事件类型列表

类型名称	子类型/子类型标识	描述
DDoS攻击	DNS协议攻击 Tcp Dns	DNS协议攻击
	异常端口通信 Unusual Network Port	异常端口通信
	异常协议攻击 Unusual Protocol	异常协议攻击
	ACK Flood ACK Flood	ACK Flood
	BGP Flood攻击 BGP Flood Attack	BGP Flood攻击
	DNS IP TTL DNS IP TTL Check Fail	DNS IP TTL
	DNS Reply Flood 攻击 DNS Reply Flood	DNS Reply Flood 攻击
	DNS查询攻击 DNS Query Flood	DNS查询攻击

类型名称	子类型/子类型标识	描述
	DNS大小异常 DNS Size Abnormal	DNS大小异常
	DNS反射 DNS Reflection	DNS反射
	DNS返回域名流异常 DNS Reply Domain Flow Abnormal	DNS返回域名流异常
	DNS格式错误 DNS Format Error	DNS格式错误
	DNS缓存匹配 DNS Cache Match	DNS缓存匹配
	DNS缓存投毒 DNS Cache Poisoning	DNS缓存投毒
	DNS请求域名流异常 DNS Request Domain Flow Abnormal	DNS请求域名流异常
	DNS无效域名 DNS No Such Name	DNS无效域名
	FIN/RST Flood FIN/RST Flood	FIN/RST Flood
	HTTPS Flood HTTPS Flood	HTTPS Flood
	HTTP慢速攻击 HTTP Slow Attack	HTTP慢速攻击
	ICMP协议封禁 ICMP Protocol Block	ICMP协议封禁
	IP信誉 IP Reputation	IP信誉
	SIP Flood SIP Flood	SIP Flood
	SIP源速率异常 SIP Source Rate Abnormity	SIP源速率异常
	SYN Flood SYN Flood	SYN Flood

类型名称	子类型/子类型标识	描述
	SYN-ACK Flood SYN-ACK Flood	SYN-ACK Flood
	TCP带宽溢出 TCP Bandwidth Overflow	TCP带宽溢出
	TCP多连接攻击 TCP Connection Flood	TCP多连接攻击
	TCP分片带宽溢出 TCP Fragment Bandwidth Overflow	TCP分片带宽溢出
	TCP分片攻击 TCP Fragment Flood	TCP分片攻击
	TCP畸形报文 TCP Malformed	TCP畸形报文
	TCP认证UDP攻击 TCP-authenticated UDP Attack	TCP认证UDP攻击
	TCP协议封禁 TCP Protocol Block	TCP协议封禁
	UDP带宽溢出 UDP Bandwidth Overflow	UDP带宽溢出
	UDP分片 UDP Fragment Flood	UDP分片
	UDP分片带宽溢出 UDP Fragment Bandwidth Overflow	UDP分片带宽溢出
	UDP畸形报文 UDP Malformed	UDP畸形报文
	UDP协议封禁 UDP Protocol Block	UDP协议封禁
	URI监控 URI Monitor	URI监控
	暗网IP Dark IP	暗网IP

类型名称	子类型/子类型标识	描述
	单IP带宽溢出 Single IP Bandwidth Overflow	单IP带宽溢出
	当前连接耗尽攻击 Concurrent Connections Flood	当前连接耗尽攻击
	端口扫描攻击 Port Scanning Attack	端口扫描攻击
	恶意域名攻击 Malicious Domains Attack	恶意域名攻击
	反恶意软件 Anti-Malware	反恶意软件
	分布式拒绝服务攻击 DDoS	分布式拒绝服务攻击
	分区带宽溢出 Zone Bandwidth Overflow	分区带宽溢出
	过滤器攻击 Filter Attack	过滤器攻击
	黑名单 Blacklist	黑名单
	僵尸网络/特洛伊木马/蠕虫 Botnets/Trojan horses/Worms Attack	僵尸网络/特洛伊木马/蠕虫
	目的IP新会话限速 Destination IP new session rate limiting	目的IP新会话限速
	其他Flood攻击 Other Flood	其他Flood攻击
	其他带宽溢出 Other Bandwidth Overflow	其他带宽溢出
	其他全局异常 Global Other Abnormal	其他全局异常

类型名称	子类型/子类型标识	描述
	其他协议封禁 Other Protocol Block	其他协议封禁
	全局ICMP异常 Global ICMP Abnormal	全局ICMP异常
	全局TCP分片异常 Global TCP Fragment Abnormal	全局TCP分片异常
	全局TCP异常 Global TCP Abnormal	全局TCP异常
	全局UDP分片异常 Global UDP Fragment Abnormal	全局UDP分片异常
	全局UDP异常 Global UDP Abnormal	全局UDP异常
	网页攻击 Web Attack	网页攻击
	位置攻击 Location Attack	位置攻击
	新连接耗尽攻击 New Connections Flood	新连接耗尽攻击
	域名劫持 Domain Hijacking	域名劫持
	源DNS返回流异常 Source DNS Reply Flow Abnormal	源DNS返回流异常
	源DNS请求流异常 Source DNS Request Flow Abnormal	源DNS请求流异常
	主机流量溢出 Host Traffic Over Flow	主机流量溢出
	HTTP Flood HTTP Flood	HTTP Flood
	ICMP Flood ICMP Flood	ICMP Flood

类型名称	子类型/子类型标识	描述
	SSL Flood SSL Flood	SSL Flood
	TCP Flood TCP Flood	TCP Flood
	UDP Flood UDP Flood	UDP Flood
	XML Flood XML Flood	XML Flood
	放大攻击 Amplification	放大攻击
Web恶意代码	网页暗链 Web Page Dark Link	网页暗链
	网页挂马 Web Page Trojan	网页挂马
Web攻击	Webshell Webshell	Webshell
	WAF机器人 WAF Robot	WAF机器人
	白名单IP White IP	白名单IP
	攻击惩罚 Known Attack Source	攻击惩罚
	黑名单IP Black IP	黑名单IP
	漏洞攻击 Vulnerability Attack	漏洞攻击
	命中隐私泄露规则 Leakage	命中隐私泄露规则
	默认 Default	默认
	扫描/爬虫 Scanner & Crawler	扫描/爬虫
CC攻击 Challenge Collapsar	CC攻击	

类型名称	子类型/子类型标识	描述
	IP信誉库 IP Reputation	IP信誉库
	SQL注入 SQL Injection	SQL注入
	XSS Cross-Site Scripting	XSS
	本地文件包含 Local Code Inclusion	本地文件包含
	地理访问控制拦截 Geo IP	地理访问控制拦截
	恶意爬虫 Malicious Web Crawlers	恶意爬虫
	反爬虫 Anticrawler	反爬虫
	防篡改 AntiTamper	防篡改
	非法请求 Illegal Access	非法请求
	黑白名单拦截 White or Black IP	黑白名单拦截
	精准防护 Custom Rule	精准防护
	命令注入 Command Injection	命令注入
	目录遍历 Path Traversal	目录遍历
	网站木马 Website Trojan	网站木马
	网站信息防泄露 Information Leakage	网站信息防泄露
	网站信息泄露 Web Service Exfiltration	网站信息泄露
	远程代码执行 Remote Code Execute	远程代码执行

类型名称	子类型/子类型标识	描述
	远程文件包含 Remote Code Inclusion	远程文件包含
恶意软件	加密货币挖矿 Cryptomining	加密货币挖矿
	Docker恶意程序 Docker Malware	Docker恶意程序
	钓鱼 Phishing	钓鱼
	恶意广告软件 Adware	恶意广告软件
	恶意软件 Malicious Software	恶意软件
	黑客工具 Hacktool	黑客工具
	灰色软件 Grayware	灰色软件
	间谍软件 Spyware	间谍软件
	垃圾邮件 Spam	垃圾邮件
	Rootkit Rootkit	Rootkit
	Webshell Webshell	Webshell
	病毒、蠕虫 Virus and Worm	病毒、蠕虫
	恶意文件 Malicious File	恶意文件
	反弹shell Reverse Shell	反弹shell
后门木马 Backdoor Trojan	后门木马	
僵尸网络程序 Botnet Program	僵尸网络程序	

类型名称	子类型/子类型标识	描述
	勒索软件 Ransomware	勒索软件
	挖矿程序 Bitcoin Miner	挖矿程序
	挖矿软件 Mining Software	挖矿软件
风险审计	Webcms漏洞 Webcms Vulnerability	Webcms漏洞
	Windows OS 漏洞 Windows Vulnerability	Windows OS 漏洞
	本地访问漏洞 Local Access Vulnerability	本地访问漏洞
	错误配置策略 Mis-Configured Policy	错误配置策略
	其它OS漏洞 Other OS Vulnerability	其它OS漏洞
	其它漏洞 Other Vulnerability	其它漏洞
	应用程序漏洞 Application Vulnerability	应用程序漏洞
	远程访问漏洞 Remote Access Vulnerability	远程访问漏洞
风险审计	弱口令 Weak Password	弱口令
	系统风险配置 System Risk Configuration	系统风险配置
攻击探测	钓鱼 Phishing	钓鱼
	网络拓扑构建 Map Network Topology	网络拓扑构建
	账户、组信息收集 Identify Groups/Roles	账户、组信息收集

类型名称	子类型/子类型标识	描述
	指纹扫描 Fingerprinting	指纹扫描
	主机发现 Determine IP Address	主机发现
漏洞利用	ActiveX漏洞利用 ActiveX Exploit	ActiveX漏洞利用
	CGI攻击 CGI Attack	CGI攻击
	DNS漏洞利用 DNS Exploit	DNS漏洞利用
	FTP漏洞利用 FTP Exploit	FTP漏洞利用
	Hadoop漏洞利用 Hadoop Vulnerability Exploit	Hadoop漏洞利用
	Hypervisor漏洞利用 Hypervisor Exploit	Hypervisor漏洞利用
	LDAP注入攻击 LDAP Injection Attack	LDAP注入攻击
	MacOS漏洞利用 MacOS Exploit	MacOS漏洞利用
	MySQL漏洞利用 MySQL Vulnerability Exploit	MySQL漏洞利用
	Office软件漏洞利用 Office Exploit	Office软件漏洞利用
	Redis漏洞利用 Redis Vulnerability Exploit	Redis漏洞利用
	RPC漏洞利用 RPC Exploit	RPC漏洞利用
	SQL注入 SQL Injection	SQL注入
	SSH漏洞利用 SSH Exploit	SSH漏洞利用

类型名称	子类型/子类型标识	描述
	SSI注入攻击 SSI Injection Attack	SSI注入攻击
	Struts2 OGNL注入 Struts2 OGNL Injection	Struts2 OGNL注入
	Telnet漏洞利用 TELNET Exploit	Telnet漏洞利用
	Unix漏洞利用 Unix Exploit	Unix漏洞利用
	Web漏洞利用 Web Exploit	Web漏洞利用
	XSS攻击 Cross-Site Scripting	XSS攻击
	本地文件包含 Local File Inclusion	本地文件包含
	恶意文件投递 Malicious File Delivery	恶意文件投递
	恶意文件执行 Malicious File Execution	恶意文件执行
	缓冲区溢出攻击 Buffer Overflow	缓冲区溢出攻击
	会话劫持 Session Hijack	会话劫持
	口令猜测 Password Cracking	口令猜测
	浏览器漏洞利用 Browser Exploit	浏览器漏洞利用
	弱口令访问 Weak Password Access	弱口令访问
	数据库漏洞利用 Database Exploit	数据库漏洞利用
	未知漏洞利用 Unknown Exploit	未知漏洞利用
	隐藏链接访问 Hide Link Access	隐藏链接访问

类型名称	子类型/子类型标识	描述
	邮件漏洞利用 Mail Exploit	邮件漏洞利用
	远程代码执行 Remote Code Execution	远程代码执行
	远程访问漏洞利用 Remote Access Exploit	远程访问漏洞利用
	远程文件包含攻击 Remote File Inclusion	远程文件包含攻击
	远程文件注入 Remote File Injection	远程文件注入
	组合漏洞利用 Misc Exploit	组合漏洞利用
	CMS漏洞 CMS Exploit	CMS漏洞
	CSRF攻击 CSRF Attack	CSRF攻击
	JNDI注入攻击 JNDI Injection Attack	JNDI注入攻击
	Linux漏洞 Linux Exploit	Linux漏洞
	SMB漏洞 SMB Exploit	SMB漏洞
	Windows漏洞 Windows Exploit	Windows漏洞
	XML注入 XML Injection	XML注入
	代码注入 Code Injection	代码注入
	漏洞逃逸攻击 Vulnerability Escape Attack	漏洞逃逸攻击
	命令执行 Command Execution	命令执行

类型名称	子类型/子类型标识	描述
	命令注入 Command Injection	命令注入
	文件逃逸攻击 File Escape Attack	文件逃逸攻击
	虚拟机逃逸攻击 VM Escape Attack	虚拟机逃逸攻击
	一般漏洞利用 General Exploit	一般漏洞利用
命令与控制	ECS存在当前IP被用于向 高危网络发送消息 Command Control Activity	ECS存在当前IP被用于向高危网 络发送消息
	可疑的域名、IP地址、端 口动态生成访问 Dynamic Resolution	可疑的域名、IP地址、端口动 态生成访问
	其他可疑连接 Abnormal Connection	其他可疑连接
	其他可疑行为 Abnormal Behavior	其他可疑行为
	外连恶意DNS Malicious Domain Query	外连恶意DNS
	外连恶意IP地址 Malicious Ip Address Query	外连恶意IP地址
	隐蔽隧道 Protocol Tunneling	隐蔽隧道
	与矿池地址通信 Mining Pool Communication	与矿池地址通信
其他	公共輿情 Public_Opinion	公共輿情
	云防火墙攻击 CFW_RISK	云防火墙攻击
数据泄露	数据窃取 Steal Data	数据窃取

类型名称	子类型/子类型标识	描述
	违规外传 Transfer Data Abnormal	违规外传
网络异常行为	IP访问频率异常 IP Access Frequency Abnormal	IP访问频率异常
	IP切换异常 IP Switch Abnormal	IP切换异常
	IP首次访问 IP First Access	IP首次访问
	Sinkhole攻击IP访问 Sink Hole	Sinkhole攻击IP访问
	代理IP访问 Proxy	代理IP访问
	恶意资源访问 Resource Permissions	恶意资源访问
	欺诈付款网站IP/域名访问 Payment	欺诈付款网站IP/域名访问
	洋葱网络IP访问 Tor	洋葱网络IP访问
	C&C异常通信 C&C Abnormal Communication	C&C异常通信
	IP黑名单访问 IP Blacklist Access	IP黑名单访问
	URL黑名单访问 URL Blacklist Access	URL黑名单访问
	恶意URL访问 Malicious URL Access	恶意URL访问
	恶意域名访问 Malicious Domain Name Access	恶意域名访问
非授权访问企图 Unauthorized Access Attemp	非授权访问企图	

类型名称	子类型/子类型标识	描述
	可疑的网络流量 Suspicious Network Traffic	可疑的网络流量
	容器网络外联 Container Network Connect	容器网络外联
	未知网络访问 Unknown Abnormal Network Access	未知网络访问
	文件MD5黑名单访问 File MD5 Blacklist Access	文件MD5黑名单访问
	异常外联行为 Abnormal External Behavior	异常外联行为
	域名黑名单访问 Domain Name Blacklist Access	域名黑名单访问
	周期外联通信 Periodic Outreach	周期外联通信
	可疑的端口转发 Suspicious Port Forward	可疑的端口转发
无文件攻击	VDSO劫持 VDSO Hijacking	VDSO劫持
	动态库注入进程 Dynamic Library Inject Process	动态库注入进程
	关键配置变更 Critical File Change	关键配置变更
	环境变量变更 Environment Change	环境变量变更
	进程注入 Process Inject	进程注入
	内存文件进程 Memfd Process	内存文件进程
	文件操纵 File Manipulation	文件操纵

类型名称	子类型/子类型标识	描述
系统行为异常	Crontab可疑任务 Crontab Suspicious Task	Crontab可疑任务
	Socket连接异常 Abnormal Socket Connection	Socket连接异常
	备份删除 Backup Deletion	备份删除
	非法数据库访问 Unauthorized Database Access	非法数据库访问
	权限异常访问 Privilege Abnormal Access	权限异常访问
	日志异常变化 Unexpected Log Change	日志异常变化
	容器进程退出 Container Process Exist	容器进程退出
	未知主机异常行为 Unknown Host Abnormal Activity	未知主机异常行为
	文件黑名单访问 File blacklist access	文件黑名单访问
	文件权限异常改变 Unexpected File Permission Change	文件权限异常改变
	系统安全防护被禁用 System Security Protection disabled	系统安全防护被禁用
	系统账号变更 System Account Change	系统账号变更
	异常注册表操作 Abnormal Registry Operation	异常注册表操作
	Crontab脚本提权 Crontab Script Privilege Escalation	Crontab脚本提权

类型名称	子类型/子类型标识	描述
	Crontab脚本修改 Crontab Script Change	Crontab脚本修改
	高危命令执行 High-risk Command Execution	高危命令执行
	高危系统调用 High-Risk Syscall	高危系统调用
	关键文件/目录变更 File/Directory Change	关键文件/目录变更
	关键文件变更 Key File Change	关键文件变更
	进程提权 Process Privilege Escalation	进程提权
	进程异常行为 Process Abnormal Activity	进程异常行为
	敏感文件访问 Sensitive File Access	敏感文件访问
	容器进程异常 Container Abnormal Process	容器进程异常
	容器异常启动 Container Abnormal Start	容器异常启动
	数据库连接异常 Abnormal Database Connection	数据库连接异常
	网卡混杂模式 Network Adapter Promiscuous Mode	网卡混杂模式
	文件提权 File Privilege Escalation	文件提权
	文件异常删除 File Abnormal Delete	文件异常删除

类型名称	子类型/子类型标识	描述
	系统启动脚本改变 System Start Script Change	系统启动脚本改变
	异常shell Abnormal Shell	异常shell
	异常命令执行 Abnormal Command Execution	异常命令执行
信息破坏	信息篡改 Information Tampering	信息篡改
	信息丢失 Information Loss	信息丢失
	信息假冒 Information Masquerading	信息假冒
	信息窃取 Information Interception	信息窃取
	信息泄露 Information Disclosure	信息泄露
	Linux网页篡改 Linux Web Page Tampering	Linux网页篡改
	Windows网页篡改 Windows Web Page Tampering	Windows网页篡改
	目录遍历 Directory Traversal	目录遍历
用户行为异常	Token恶意利用 Token Leakage	Token恶意利用
	Token恶意利用成功 Token Leakage Success	Token恶意利用成功
	异常用户首次访问 User First Cross Domain Access	异常用户首次访问

类型名称	子类型/子类型标识	描述
	用户访问频率异常 User Access Frequency Abnormal	用户访问频率异常
	用户访问时段异常 User Hour Level Access Abnormal	用户访问时段异常
	用户使用特定IP下载行为异常 User IP Download Abnormal	用户使用特定IP下载行为异常
	用户首次访问桶对象 Client First Access	用户首次访问桶对象
	用户下载行为异常 User Download Abnormal	用户下载行为异常
	暴力破解 Brute Force Cracking	暴力破解
	违规登录 Illegal Login	违规登录
	未知用户异常行为 Unknown User Abnormal Activity	未知用户异常行为
	异常登录 Abnormal Login	异常登录
	用户登录尝试 User Login Attempt	用户登录尝试
	用户密码窃取 User Password Theft	用户密码窃取
	用户权限提升成功 User Privilege Escalation Succeeded	用户权限提升成功
	用户权限提升失败 User Privilege Escalation Failed	用户权限提升失败
	用户首次登录 User First login	用户首次登录

类型名称	子类型/子类型标识	描述
	用户账号删除 User Account Removed	用户账号删除
	用户账号添加 User Account Added	用户账号添加
	用户组变更 User Group Changed	用户组变更
	用户组删除 User Group Removed	用户组删除
	用户组添加 User Group Added	用户组添加
	账号伪造 Account Forgery	账号伪造
	ECS可疑账号创建 Suspicious Ecs User Create	ECS可疑账号创建
	ECS账号权限修改 ECS User Escalate Privilege	ECS账号权限修改
	IAM可疑账号创建 Suspicious IAM Account Create	IAM可疑账号创建
	IAM账号权限修改 IAM Permissions Escalation	IAM账号权限修改
	暴力破解登录ECS ECS BruteForce Login	暴力破解登录ECS
	暴力破解登录IAM IAM BruteForce Login	暴力破解登录IAM
	非法系统账号 Invalid System Account	非法系统账号
	风险账号 Risky Account	风险账号
	可疑IP登录ECS Suspicious IP Address Login	可疑IP登录ECS

类型名称	子类型/子类型标识	描述
	可疑IP登录IAM Suspicious IP Address Login	可疑IP登录IAM
	异常登录IAM IAM Abnormal Login	异常登录IAM
	异地登录ECS Instance Credential Exfiltration	异地登录ECS
	用户登录成功 User Login Success	用户登录成功
	用户登录拒绝 User Login Denied	用户登录拒绝
	用户账号变更 User Account Changed	用户账号变更
资源操控	恶意逻辑插入 Malicious Logic Insertion	恶意逻辑插入
	基础设施操纵 Infrastructure Manipulation	基础设施操纵
	配置/环境操纵 Configuration/ Environment Manipulation	配置/环境操纵
	容器逃逸 Container Escape	容器逃逸
	容器资源操纵 Container Resource Manipulation	容器资源操纵
	软件完整性 Software Integrity Attack	软件完整性
资源侦查	端口探测数量异常 Port Detection	端口探测数量异常
	ARP 扫描 ARP Scan	ARP 扫描

类型名称	子类型/子类型标识	描述
	DNS探测 DNS Recon	DNS探测
	Hypervisor探测 Hypervisor Recon	Hypervisor探测
	ICMP探测 ICMP Recon	ICMP探测
	Linux探测 Linux Recon	Linux探测
	MacOS探测 MacOS Recon	MacOS探测
	NMAP扫描 NMAP Scan	NMAP扫描
	RPC请求探测 RPC Recon	RPC请求探测
	SNMP扫描 SNMP Recon	SNMP扫描
	TCP扫描 TCP Recon	TCP扫描
	UDP扫描 UDP Recon	UDP扫描
	Unix探测 Unix Recon	Unix探测
	WEB探测 Web Recon	WEB探测
	Windows探测 Windows Recon	Windows探测
	加密渗透扫描 Encrypted Penetration Scan	加密渗透扫描
	普通扫描事件 General Scanner	普通扫描事件
	数据库探测 Database Recon	数据库探测

类型名称	子类型/子类型标识	描述
	邮件探测 Mail Recon	邮件探测
	主机扫描 Host Scan	主机扫描
	组合探测 Misc Recon	组合探测
	端口扫描 Port Scan	端口扫描

## 事件类型相关操作

- 事件的基本概念请参见[运营对象管理概述](#)。
- 事件类型支持查看、新增、编辑、启用、禁用、删除操作，详细操作指导请参见[管理事件类型](#)。

## 内置威胁情报类型

表 7-69 内置威胁情报类型列表

类型名称/类型标识	描述
IPv4 IPv4	IPv4
IPv6 IPv6	IPv6
邮件 Email	邮件
域名 domain	域名
URL URL	URL
其他 Unclassified	其他

## 威胁情报类型相关操作

- 查看威胁情报类型，详细操作指导请参见[查看威胁情报](#)。

## 内置漏洞类型

表 7-70 内置漏洞类型列表

类型名称/类型标识	描述
网站漏洞 Website Vulnerabilities	网站漏洞
Linux软件漏洞 Linux Vulnerabilities	Linux软件漏洞
Web-CMS漏洞 Web-CMS Vulnerabilities	Web-CMS漏洞
Windows系统漏洞 Windows Vulnerabilities	Windows系统漏洞
应用漏洞 Application Vulnerabilities	应用漏洞

### 漏洞类型相关操作

- 漏洞类型支持查看、新增、编辑、启用、禁用、删除操作，详细操作指导请参见[管理漏洞类型](#)。

# 8 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 8-1 购买

模块	约束与限制
配额数	<ul style="list-style-type: none"><li>• 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。</li><li>• 配额数最大限制为10000台。</li></ul>
增值包	<ul style="list-style-type: none"><li>• 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。</li><li>• 增值包不支持单独使用。<ul style="list-style-type: none"><li>- 如果需要购买增值包，请先购买标准版或专业版。</li><li>- 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。</li><li>- 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。</li></ul></li></ul>
标签	最多支持为安全云脑添加10个标签。

## 工作空间

表 8-2 工作空间

模块	约束与限制
工作空间 (Workspace)	<ul style="list-style-type: none"><li>● 付费版本安全云脑：单账号单Region内最多创建5个工作空间。</li><li>● 免费版本安全云脑：单账号单Region内最多创建1个工作空间。</li><li>● 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。</li></ul>
纳管环境	<ul style="list-style-type: none"><li>● 不支持纳管边缘环境：IEC、DEC、IES等边缘站点。</li><li>● 仅支持纳管Default项目，不支持纳管子项目。</li><li>● 不支持按EPS粒度纳管资源。</li></ul>
空间托管	<ul style="list-style-type: none"><li>● 单账号单Region内最多创建1个空间托管视图。</li><li>● 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。</li><li>● 单账号最多创建10个账号委托。</li></ul>

## 安全报告

表 8-3 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 8-4 告警模型

模块	约束与限制
告警模型	<ul style="list-style-type: none"><li>● 单账号单Region单workspace最多创建100个告警模型。</li><li>● 一个告警模型的运行时间间隔须 <math>\geq 5</math> 分钟，查询数据的时间范围 <math>\leq 14</math> 天。</li></ul>

## 安全分析

表 8-5 安全分析

模块	约束与限制
查询与分析	<ul style="list-style-type: none"><li>● 单次查询分析最多支持返回500条结果。</li><li>● 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。</li><li>● 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。</li><li>● 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。</li><li>● 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。</li></ul>
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 8-6 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	<ul style="list-style-type: none"><li>● 单账号单Workspace内，每天最多新增100个告警。</li><li>● 单账号单Workspace内，每天最多可以告警转事件100个。</li></ul>
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 8-7 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	<p>单账号单workspace内一天内的重试次数限制如下：</p> <ul style="list-style-type: none"><li>● 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。</li><li>● 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。</li></ul>
分类&映射	<ul style="list-style-type: none"><li>● 单账号单workspace内，分类&amp;映射模板 ≤ 50个。</li><li>● 单账号单workspace内，分类和映射的映射关系规格为 1:100。</li><li>● 单账号单workspace内，最多可新增分类&amp;映射100个。</li></ul>

# 9 安全

## 9.1 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，并用策略来控制用户对SecMaster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。

## 9.2 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 9-1 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。

数据保护手段	简要说明
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](#)。

## 9.3 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9-1](#)所示。

图 9-1 查询日志

事件名称	资源类型	事件来源	资源ID	资源名称	事件级别
creationFlow	workflow	CSB	50515885-c81317b488	my-test	normal
recollectServiceStatistics	workspace	CSB	5698146-3628	-	normal
recollectServiceStatistics	workspace	CSB	4862969-3c7b8	-	normal
recollectServiceStatistics	workspace	CSB	cc0652-3ade	-	normal
recollectServiceStatistics	workspace	CSB	417293-2a4d	-	normal
recollectServiceStatistics	workspace	CSB	49546d-03dc	-	normal
updatePlaybookVersion	playbook	CSB	232a4f-85	-	normal
updatePlaybook	playbook	CSB	44703-1c	-	normal

## 9.4 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，若某一地区出现故障，系统将在符合合规政策的前提下自动将客户的应用和数据迁移至未受影响的区域，确保业务连续性。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。

### 五级可靠性架构



## 9.5 监控安全风险

SecMaster已对接云监控服务（Cloud Eye，CES），可以通过CES管理控制台，查看SecMaster的相关事件和监控指标，及时了解SecMaster运行状况。

- 事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。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。
- 指标监控提供了指标数据上报、查询和告警的功能。用户可以通过云监控服务提供的管理控制台或API接口来检索安全云脑产生的监控指标和告警信息。

更多详细内容请参见[使用CES监控SecMaster](#)。

## 9.6 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 9-2 合规证书下载

## 合规证书下载

请输入关键词搜索

 <b>BS 10012:2017</b> BS 10012为个人信息管理体系提供了一个符合欧盟GDPR原则的最佳实践框架。它概述了组织在收集、存储、处理、保留或处理与个人相关的个人记录时需要考虑的核心需求。保留或处理与个人相关的个人记录时需要考虑的核心需求。 <a href="#">下载</a>	 <b>CSA STAR认证</b> CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。 <a href="#">下载</a>	 <b>ISO 20000-1:2018</b> ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的IT服务来满足客户和业务的需求。 <a href="#">下载</a>
 <b>SOC 1 类型II 报告 2022.04.01-2023.03.31</b> 华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。 <a href="#">下载</a>	 <b>SOC 1 类型II 报告 2022.10.01-2023.09.30</b> 华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为 2022.10.01-2023.09.30。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。 <a href="#">下载</a>	 <b>SOC 2 类型II 报告 2022.04.01-2023.03.31</b> 华为云每年滚动发布两期SOC2报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 2报告着重于组织的内部运作与合规，包括安全性、可用性、进程完整性、保密性、隐私性五大控制属性。 <a href="#">下载</a>

## 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 9-3 资源中心

## 资源中心

### 白皮书资源

<a href="#">隐私遵从性白皮书</a>	<a href="#">行业规范遵从性白皮书</a>	<a href="#">指南和最佳实践</a>	
 <b>尼日利亚NDPR遵从性指南</b> 本白皮书基于尼日利亚NDPR合规要求，分享华为云隐私保护的经验和实践，以及如何助力您满足尼日利亚NDPR合规要求。	 <b>阿根廷PDPL遵从性指南</b> 本白皮书基于阿根廷PDPL及第47号决议的合规要求，分享华为云隐私保护的经验和实践，以及如何助力您满足PDPL和第47号决议的合规要求。	 <b>巴西LGPD遵从性指南</b> 本白皮书基于巴西LGPD合规要求，分享华为云在隐私保护领域的经验和实践，以及如何助力您满足巴西LGPD合规要求。	 <b>智利共和国PDPL遵从性指南</b> 本白皮书基于智利共和国PDPL合规要求，分享华为云隐私保护的经验和实践，以及如何助力客户满足智利共和国PDPL合规要求。

## 9.7 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 workflows 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](#)。

# 10 权限管理

如果您需要对华为云上购买的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。如果账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用SecMaster服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制用户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，您希望用户拥有SecMaster的使用权限，但是不希望用户拥有删除SecMaster等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用SecMaster，但是不允许删除SecMaster的权限，控制用户对SecMaster资源的使用范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 10-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	<ul style="list-style-type: none"><li>● 系统角色</li><li>● 系统策略</li><li>● 自定义策略</li></ul>	为主体授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	<ul style="list-style-type: none"> <li>系统策略</li> <li>自定义身份策略</li> </ul>	<ul style="list-style-type: none"> <li>为主体授予身份策略</li> <li>身份策略附加至主体</li> </ul>	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在身份策略中通过条件键“g:RequestedRegion”的配置即可达到身份策略对于授权区域的控制。将策略附加主体或为主体授予该身份策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。[角色与策略权限管理](#)和[身份策略权限管理](#)分别介绍两种模型的系统权限。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

## 角色与策略权限管理

SecMaster服务支持角色与策略授权。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，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，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。

如表10-2所示，包括了SecMaster的所有系统权限。角色与策略授权场景的系统策略与身份策略授权场景的并不互通。

表 10-2 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

系统角色/策略名称	描述	类别	依赖关系
SecMaster ReadOnly	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

表10-3列出了SecMaster常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 10-3 常用操作与系统权限的关系

操作	SecMaster FullAccess	SecMaster ReadOnly
创建按需订单	√	x
创建包周期订单	√	x
查看订购版本	√	x
查看指标结果	√	√
创建委托	√	x
导入资源	√	x
查看报告	√	√
导出应急漏洞	√	x
创建数据空间	√	x
创建数据管道	√	x
查询数据	√	√
执行分析	√	x
创建检索条件	√	x
创建告警模型	√	x
启用告警模型	√	x
查询告警模板	√	√
创建剧本	√	x
审核剧本	√	x
创建剧本版本	√	x
创建剧本版本规则	√	x
创建剧本版本动作	√	x
创建流程	√	x

操作	SecMaster FullAccess	SecMaster ReadOnly
创建流程版本	√	x
审核流程版本	√	x
查询资产连接列表	√	√
创建资产连接	√	x
创建工作空间	√	x
查询待办列表	√	√
绑定情报类型与布局关联	√	x
获取告警详情	√	√
告警转事件	√	x
查询告警类型列表	√	√
绑定告警类型与布局关联	√	x
获取事件详情	√	√
绑定事件类型与布局的关联	√	x
获取漏洞组详情	√	√
导出漏洞组列表	√	x
绑定漏洞类型与布局关联	√	x

## 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**指定区域项目资源**SecMaster FullAccess权限后，在安全云脑控制台使用服务委托授权操作时，还需要给予子账号授予IAM创建委托权限、委托授权策略权限，具体说明如下：

表 10-4 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 <b>指定区域项目资源</b> 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 <b>IAM子账号补充授权操作</b> 。

## 身份策略权限管理

SecMaster服务支持身份策略授权。如表10-5所示，包括了SecMaster身份策略中的所有系统身份策略。身份策略授权场景的系统身份策略与角色与策略授权场景的并不互通。

**表 10-5** SecMaster 系统身份策略

系统策略名称	描述	策略类别
SecMasterFullAccess	安全云脑的所有权限。	系统策略
SecMasterReadOnly	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

表10-6列出了SecMaster常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

**表 10-6** 常用操作与系统策略的关系

操作	SecMasterFullAccess	SecMasterReadOnly
创建按需订单	√	x
创建包周期订单	√	x
查看订购版本	√	x
查看指标结果	√	√
创建委托	√	x
导入资源	√	x
查看报告	√	√
导出应急漏洞	√	x
创建数据空间	√	x
创建数据管道	√	x
查询数据	√	√
执行分析	√	x
创建检索条件	√	x
创建告警模型	√	x
启用告警模型	√	x
查询告警模板	√	√

操作	SecMasterFullAccess	SecMasterReadOnly
创建剧本	√	x
审核剧本	√	x
创建剧本版本	√	x
创建剧本版本规则	√	x
创建剧本版本动作	√	x
创建流程	√	x
创建流程版本	√	x
审核流程版本	√	x
查询资产连接列表	√	√
创建资产连接	√	x
创建工作空间	√	x
查询待办列表	√	√
绑定情报类型与布局关联	√	x
获取告警详情	√	√
告警转事件	√	x
查询告警类型列表	√	√
绑定告警类型与布局关联	√	x
获取事件详情	√	√
绑定事件类型与布局的关联	√	x
获取漏洞组详情	√	√
导出漏洞组列表	√	x
绑定漏洞类型与布局关联	√	x

## SecMaster 控制台功能依赖的身份策略

IAM主账号给IAM子账号授予**指定区域项目资源**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 10-7 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 <b>指定区域项目资源</b> 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 <b>IAM子账号补充授权操作</b> 。

## 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“指定区域项目资源”，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": "5.0",
  "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。

## 相关链接

- [IAM产品介绍](#)
- [通过IAM角色或策略授予使用SecMaster的权限](#)
- [通过IAM身份策略授予使用SecMaster的权限](#)

# 11 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，全面呈现当前ECS安全风险态势，并提供相应防护建议。HSS是ECS的安全防护产品，安全云脑通过接入HSS的日志数据和基线检查结果，为ECS提供安全管理服务。

## 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 11-1 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。

# 12 基本概念

## 12.1 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，并在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。

- **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可以快速发现威胁，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，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产生的日志数据。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，直接切换到备份系统，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》。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。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、运营日常业务、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，安全分析师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严重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。威胁搜寻者识别和响应自动工具未检测到的高级威胁。该角色采取主动行动，旨在加深企业或组织对已知威胁的理解，并在攻击发生前揭示未知威胁。

- **取证分析师**

大型企业/组织可能还会聘用取证分析师，取证分析师负责在出现违规后收集情报来确定其根本原因。取证分析师会搜寻系统漏洞、违反安全策略的行为和网络攻击模式，这些信息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，如果没有威胁调查员，那么聘用第三方可能比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、政府和其他组织适应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。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，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，会隐藏起来、窃取大量数据，并在任何人注意到之前提升权限。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。还会部署可自动执行任务的技术，让较小的团队更加高效，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。与终端节点检测和响应 (EDR) 等系统相比, XDR扩大了安全范围, 从而跨产品集成了保护, 包括企业/组织的终端节点、服务器、云应用程序和电子邮件等。在此基础上, 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。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 团队负责根据需要进行威胁清除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。

## 12.2 总览和态势总览

### 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，包括资产的安全评估结果、安全监控和安全趋势等信息，可以全面了解资产的安全情况。总览页面实时呈现安全云脑所有工作空间的整体安全评估结果，查看方法请参见[查看总览](#)。

### 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，包括资产的安全评估结果、安全监控和安全趋势等信息，可以全面了解资产的安全情况。目标工作空间的“态势感知 > 态势总览”页面呈现当前单个工作空间的安全评估结果，查看方法请参见[查看态势总览](#)。

### 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。安全大屏中的[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。

### 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”。

- 新购云脑或者新创建工作空间场景，未在“总览”页触发安全评分检测，安全状态未知，则安全评分为0分。请触发安全评分检测后再次查看安全评分结果。
- 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 12-1 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。
未知	0分	评分状态未知：请检测空间是否创建成功或数据是否接入成功。

- 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 12-2 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

分类	扣分项	单项扣分值	处理建议	最高扣分上限
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		
	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		

## 12.3 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。

## 相关操作

- **新增工作空间**：工作空间（Workspace）属于安全云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和Region，可支撑不同场景下的工作空间运营模式。在使用安全云脑的基线检查、告警管理、安全分析、安全编排等功能前，需要先创建工作空间，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。
- **创建空间托管**：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。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。
- **管理托管**：空间托管页面中，可以管理托管视图、我纳管的和纳管我的。

## 12.4 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。

### 告警和事件关系说明

本部分介绍告警和事件的含义、区别，告警转事件的原因和告警关联事件的原因。

- **告警和事件的含义与区别**

表 12-3 告警和事件的含义与区别

类别	定义	处理流程	重要性和紧急程度
告警	<p>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。</p> <p>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。</p> <p>告警的目的是及时通知相关人员，以便能够迅速响应并采取措施解决问题。</p>	<p>告警的处理流程通常包括接收、确认、分析、响应和关闭等步骤。当监控系统发出告警时，运维人员首先需要确认告警的真实性，然后分析告警的原因和影响范围，最后采取相应的措施来解决问题，并关闭告警。</p>	<p>告警一般需要立即评估和响应。</p> <p>每条告警的紧急程度和重要性各不相同，取决于告警的类型、级别和影响的范围。一些告警可能只是简单的提醒或预警，而另一些告警则可能表示系统已经遭受严重攻击或面临重大故障风险。</p>
事件	<p>事件是一个更广泛的概念，可以包括告警，但不限于此。事件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。</p> <p>事件的目的更广泛，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。</p>	<p>事件的处理流程则更加复杂和全面。除了包含告警处理流程中的各个环节外，事件处理还需要进行事件调查、影响评估、风险分析、制定应急计划、执行应急响应、事后总结等步骤。事件处理的目标是彻底解决问题，防止类似事件再次发生，并减少事件对业务的影响。</p>	<p>事件可能需要记录、分析或在某些情况下采取行动，但不一定需要立即响应。</p> <p>事件通常比告警具有更高的重要性和紧急程度。因为事件已经发生并产生了实际的影响，需要立即采取措施来应对和解决问题。如果事件得不到及时处理，可能会给组织带来重大的经济损失或声誉损害。</p>

- **告警转事件或关联事件的原因**

告警通常是在系统或服务出现异常或潜在故障时产生的通知。这些异常可能会直接影响业务的正常运行，因此告警需要被及时处理，以防止业务异常。告警通常需要采取相应的措施来清除故障，否则可能会因为这些异常或故障引起业务的异常。

事件则是在系统或服务在正常运行状态下产生的通知，它可能涉及到一些重要的状态变化，但不一定会引起业务异常。因此，事件一般不需要进行处理，主要用于帮助分析、定位问题。

表 12-4 告警转事件或关联事件的原因

类别	说明
告警转事件原因	<p>当告警的严重性达到一定程度，或者持续出现，或者其影响范围广泛时，它可能不再仅仅是一个需要关注的信号，也可能表明系统或网络中存在一个持续性的问题，此时，它已经演变成了一个需要立即处理的事件，这种情况下，可以将告警转化为事件来处理，以便深入调查问题的根源，并采取相应的措施来彻底解决。通常告警转事件的原因有以下几个方面：</p> <ul style="list-style-type: none"><li>● 信息聚合与分类 告警通常是对某个特定条件或阈值被违反的即时响应。随着时间的推移，大量的告警可能会被触发，如果直接处理这些独立的告警，可能会变得非常混乱和低效。将这些告警聚合成事件，可以帮助相关人员根据告警的类型、来源、影响等维度进行分类，从而更有效地处理它们。</li><li>● 简化工作流程 告警到事件的转换过程，通常伴随着对告警的过滤、去重、聚合等处理。这些处理使得可能触发多个相似告警的情况，被整合为一个更具代表性的事件。这样不仅减少了处理单个告警的工作量，也使得处理过程更加条理清晰，便于跟踪和记录。</li><li>● 提升问题解决效率 将告警转换为事件后，由于事件通常提供了比单个告警更全面的上下文信息，因此相关人员可以更容易地识别出问题的根本原因，有助于更快地定位问题，并采取有效的解决措施。</li><li>● 便于历史回顾与趋势分析 事件记录了问题的发生、发展、解决的全过程，这为后续的问题预防、系统优化等提供了宝贵的历史数据。通过对事件进行趋势分析，可以发现系统中潜在的薄弱环节，提前采取措施进行改进。</li><li>● 增强跨部门协作 在大型组织中，不同的部门可能需要共同参与问题的处理。将告警转换为事件后，可以更容易地在不同部门之间共享相关信息，促进跨部门协作，提高问题解决的效率。</li></ul> <p>总而言之，将告警转换为事件助于简化工作流程、提升问题解决效率、便于历史回顾与趋势分析。</p>

类别	说明
告警关联事件原因	<p>告警关联事件是监控和故障管理中的一个重要环节，它涉及到将多个独立但可能相互关联的事件或告警组合起来，以便更好地理解问题的根源和范围，从而更有效地进行故障排查和响应。通常告警关联事件的原因有以下几个方面：</p> <ul style="list-style-type: none"><li>● 依赖关系 在复杂的系统中，各个组件之间往往存在复杂的依赖关系。当一个组件出现故障时，可能会影响依赖它的其他组件的正常工作，进而引发一系列告警。例如，在微服务架构中，一个服务的崩溃可能导致调用该服务的其他服务也出现问题。</li><li>● 资源共享 当多个系统或服务共享同一资源（如服务器、数据库、网络设备等）时，该资源的问题可能导致多个系统或服务同时发出告警。例如，共享数据库服务器的性能下降可能会触发多个依赖该数据库的应用程序的性能告警。</li><li>● 连锁反应 某些情况下，一个初始的故障可能触发一系列连锁反应，导致更多的组件或系统受到影响。这种连锁反应可能由于系统设计不当、错误处理机制不完善或资源限制（如内存泄露导致的性能下降）等原因引起。</li><li>● 配置错误 配置错误或不一致的配置可能导致系统行为异常，进而触发多个看似不相关的告警。例如，错误的路由配置可能导致流量被错误地路由到不稳定的服务器，从而引发多个与性能相关的告警。</li><li>● 软件缺陷 软件中的缺陷（如bug）可能导致程序在特定条件下表现异常，并触发告警。如果这些缺陷影响了多个组件或系统，则可能引发多个关联告警。</li><li>● 外部因素 外部因素如自然灾害（如地震、洪水）、网络攻击、基础设施故障（如电力中断、网络中断）等也可能导致多个系统或组件同时出现问题，并触发大量告警。</li></ul>

## 相关操作

- 事件管理
  - 查看事件信息：详细操作请参见[查看事件信息](#)。
  - 新增或编辑事件：详细操作请参见[新增或编辑事件](#)。
  - 导入或导出事件：详细操作请参见[导入或导出事件](#)。
  - 关闭或删除事件：详细操作请参见[关闭或删除事件](#)。
- 告警管理
  - 查看告警信息：详细操作请参见[查看告警信息](#)。
  - 常见告警处置建议：详细操作请参见[常见告警处置建议](#)。

- 告警转事件或关联事件：详细操作请参见[告警转事件或关联事件](#)。
- 一键阻断或解封：详细操作请参见[一键阻断或解封](#)。
- 关闭或删除告警：详细操作请参见[关闭或删除告警](#)。
- 新增或编辑告警：详细操作请参见[新增或编辑告警](#)。
- 导入或导出告警：详细操作请参见[导入或导出告警](#)。

## 12.5 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。

## 操作连接

操作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。

## 操作连接与插件的关系

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）。操作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操作连接，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。

## 相关操作

- 启用流程：详细操作请参见[启用流程](#)。
- 启用剧本：详细操作请参见[启用剧本](#)。
- 管理操作连接：详细操作请参见[管理操作连接](#)。
- 查看插件详情：详细操作请参见[查看插件详情](#)。
- 查看实例监控：详细操作请参见[查看实例监控](#)。

# 12.6 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。

## 相关操作

- 安全分析使用流程：详细操作请参见[安全分析概述](#)。