## 态势感知

# 用户指南

文档版本54发布日期2022-11-24





### 版权所有 © 华为云计算技术有限公司 2024。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

### 注意

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

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

目录

1 权限管理	1
1.1 创建用户并授权使用 SA	
1.2 SA 自定义策略	
1.3 SA 权限及授权项	
	c
	0
2.1 选择计费模式	
2.1.1 包周期计费	
2.1.2 投需计费	
2.1.3 按需转包周期	6
2.2 购买标准版	
2.3 购买专业版	
2.4 升通综合大屏	17
2.5 增加资产配额	
2.6 续费	
2.7 退订	21
2.8 态势感知升级至安全云脑	24
3 安全概览	26
3.1 总览	
3.2 安全评分	
4 资源管理	34
5 业务分析	
6 综合大屏	40
6.1 综合态势感知	
6.2 主机安全态势	
7 威胁告警	51
7.1 威胁告警简介	
7.2 查看告警列表	54
7.3 威胁分析	
	•••
7.4 告警事件处理	
7.4 告警事件处理 7.4.1 DDoS	
7.4 告警事件处理 7.4.1 DDoS 7.4.2 暴力破解	

7.4.3 Web 攻击	
7.4.4 后门木马	59
7.4.5 漏洞攻击	59
7.4.6 僵尸主机	60
7.4.7 命令与控制	61
7.4.8 异常行为	61
8 漏洞管理	63
8.1 漏洞管理简介	63
8.2 查看应急漏洞公告列表	
8.3 查看主机漏洞扫描详情	
8.4 查看网站漏洞扫描详情	68
9 基线检查	70
9.1 云服务基线简介	
9.2 基线检查项目	70
9.3 配置基线检查功能所需的权限	
9.4 设置基线检查计划	107
9.5 执行基线检查计划	109
9.6 执行手动检查	
9.7 查看基线检查结果	113
9.8 处理基线检查结果	118
10 检测结果	
10.1 查看全部检测结果	
10.2 处理检测结果	126
10.3 导出检测结果	127
10.4 自定义结果列表	128
10.5 管理筛选条件	129
11 分析报告	
11.1 创建安全报告	132
11.2 发送安全报告	135
11.3 查看报告详情	138
11.4 下载历史报告	139
11.5 查看安全报告	141
11.6 编辑安全报告	143
11.7 删除报告	144
12 日志管理	
13 产品集成	
13.1 管理产品集成	
13.2 查看产品集成	
13.3 查看探测状态	
14 设置	

14.1 告警设置	155
14.1.1 设置告警通知	155
14.1.2 设置告警监控	156
14.2 授权设置	159
14.2.1 主机授权	. 159
14.3 启动主机扫描任务	. 164
14.4 检测设置	165



## 1.1 创建用户并授权使用 SA

如果您需要对您所拥有的态势感知(Situation Awareness,SA)进行精细的权限管理,您可以使用<mark>统一身份认证服务</mark>(Identity and Access Management,IAM),通 过IAM,您可以:

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

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

本章节为您介绍对用户授权的方法,操作流程如图1-1所示。

## 前提条件

给用户组授权之前,请您了解用户组可以添加的SA权限,并结合实际需求进行选择, SA支持的系统权限,请参见SA系统权限。若您需要对除SA之外的其它服务授权,IAM 支持服务的所有权限请参见<mark>系统权限</mark>。

如<mark>表1-1</mark>所示,包括了SA的所有系统权限。

#### 表 1-1 SA 系统权限

策略名称	描述	类别	依赖关系
SA FullAccess	态势感知的所有权限。	系统策略	无
SA ReadOnlyAcce ss	态势感知只读权限,拥有该权 限的用户仅能查看态势感知数 据,不具备态势感知配置权 限。	系统策略	无

#### 🗀 说明

目前,"SA FullAccess"或"SA ReadOnlyAccess"权限需要配合"Tenant Guest"权限才能使用。具体说明如下:

• 配置SA所有权限: "SA FullAccess"和"Tenant Guest"权限。

其中,如果需要使用SA的资源管理和基线检查功能需要配置以下权限:

- 资源管理: "SA FullAccess"和"Tenant Administrator"权限,详细操作请参见配置 相关功能所需的权限。
- **基线检查**: "SA FullAccess"、"Tenant Administrator"和IAM相关权限,详细操作 请参见配置相关功能所需的权限。
- 配置SA只读权限: "SA ReadOnlyAccess"和"Tenant Guest"权限。

## 示例流程





#### 1. 创建用户组并授权

在IAM控制台创建用户组,并授予态势感知的权限"SA FullAccess"和"Tenant Guest"。

2. 创建用户并加入用户组

在IAM控制台创建用户,并将其加入1中创建的用户组。

3. 用户登录并验证权限

新创建的用户登录控制台,切换至授权区域,验证权限: 在服务列表中选择除态势感知外(假设当前策略仅包含"SA FullAccess")的任 一服务,若提示权限不足,表示"SA FullAccess"已生效。

4. 配置委托。

其中,如果需要使用SA的资源管理和基线检查功能需要配置以下权限:

 资源管理: "SA FullAccess"和"Tenant Administrator"权限,详细操作请 参见配置相关功能所需的权限。  基线检查: "SA FullAccess"、"Tenant Administrator"和IAM相关权限, 详细操作请参见配置相关功能所需的权限。

## 1.2 SA 自定义策略

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

目前华为云支持以下两种方式创建自定义策略:

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

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

## SA 自定义策略样例

```
示例1:授权用户获取告警列表、获取威胁分析结果
{
 "Version": "1.1",
 "Statement": [
  Ł
    "Effect": "Allow",
    "Action": [
     "sa:threatevent:getList",
     "sa:threatevent:getAnalyze"
    1
  }
 ]
3
示例2: 拒绝用户修改告警配置信息
拒绝策略需要同时配合其他策略使用,否则没有实际作用。用户被授予的策略
中,一个授权项的作用如果同时存在Allow和Deny,则遵循Deny优先原则。
如果您给用户授予"SA FullAccess"的系统策略,但不希望用户拥有"SA
FullAccess"中定义的修改告警配置的权限,您可以创建一条拒绝修改告警配置的
自定义策略,然后同时将"SA FullAccess"和拒绝策略授予用户,根据Deny优先
原则,则用户可以对SA执行除了修改告警配置外的所有操作。拒绝策略示例如
下:
{
   "Version": "1.1",
   "Statement": [
     {
        "Action": [
           "sa:subscribe:operate"
        "Effect": "Deny"
     }
   ]
}
示例3: 多个授权项策略
一个自定义策略中可以包含多个授权项,且除了可以包含本服务的授权项外,还
可以包含其他服务的授权项,可以包含的其他服务必须跟本服务同属性,即都是
项目级服务或都是全局级服务。多个授权语句策略描述如下:
```

{

"Version": "1.1",

```
"Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "sa:cssb:operate",
         "sa:cssb:get"
     ]
   },
   {
      "Effect": "Allow",
      "Action": [
         "obs:bucket:GetReplicationConfiguration",
         "obs:bucket:PutReplicationConfiguration",
         "obs:bucket:DeleteReplicationConfiguration"
      ],
      "Resource": [
         "obs:*:*:bucket:*"
      1
  }
]
```

## 1.3 SA 权限及授权项

}

如果您需要对您所拥有的态势感知(Situation Awareness,SA)进行精细的权限管理,您可以使用统一身份认证服务(Identity and Access Management,IAM),如 果账号已经能满足您的要求,不需要创建独立的IAM用户,您可以跳过本章节,不影 响您使用SA服务的其它功能。

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

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

## 支持的授权项

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

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

#### 表 1-2 支持的授权项

权限	授权项
获取告警列表	sa:threatevent:getList
获取威胁分析结果	sa:threatevent:getAnalyze
获取主机列表	sa:threatevent:getAsset
查看综合态势感知大屏	sa:threatevent:getDashboard
查看主机安全态势大屏	sa:threatevent:getHostscreen

权限	授权项
获取租户控制台信息	sa:threatevent:getSafety
获取态势总览信息	sa:threatevent:getOverview
更新告警设置	sa:subscribe:operate
获取告警设置信息	sa:subscribe:getList
获取全局态势信息	sa:subscribe:get
获取编排信息	sa:service:get
设置服务状态	sa:service:operateSwitch
更新白名单信息	sa:service:operateWhiteList
获取订阅主题信息	sa:service:operateSubscribe
获取基线检查信息	sa:cssb:get
设置基线检查	sa:cssb:operate



## 2.1 选择计费模式

## 2.1.1 包周期计费

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

## 适用于包周期的资源

- SA资产配额,主要为主机配额。
- SA综合大屏功能,包括综合态势大屏和主机安全态势两个大屏。

若您需购买包年/包月的态势感知服务,可同时购买资产配额和综合大屏功能,配置费 用包括两种资源的费用之和;也可先购买资产配额,再开通综合大屏功能,配置费用 为分次计算,已购买资源不会重复计费,请放心购买。

您可以查看态势感知价格详情,快速了解态势感知的配置费用。

## 2.1.2 按需计费

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

## 适用于按需的资源

SA资产配额,主要为主机配额。

您可以查看态势感知价格详情,快速了解态势感知的配置费用。

## 2.1.3 按需转包周期

- 按需计费:按需计费是后付费模式,按态势感知服务的实际使用时长计费,可以 随时开通/取消。
- 包年/包月:包年/包月即包周期,是预付费模式,按订单的购买周期计费,适用于可预估资源使用周期的场景,价格比按需计费模式更优惠。

若您可预估使用态势感知服务的周期,并需要长期使用态势感知服务,可以将按需购 买的态势感知资源转为包周期计费模式,节省开支。

## 🛄 说明

- 资产配额与综合大屏功能需分别转包周期。
- 当资产配额被全部退订/取消后,即当前为基础版时。您需单击"综合大屏",进入大屏管理页面,在页面右上角再执行转包周期,将综合大屏功能从按需计费转为包周期。

### 前提条件

已购买按需计费的专业版服务,即已购买按需的资产配额或综合大屏。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制台。
- 步骤3 单击右上角"专业版",显示版本管理窗口。
- **步骤4**针对按需购买的资产配额或综合大屏,单击"转包周期",跳转到"按需转包年/包月"页面。
- 步骤5 确认资源信息,并选择购买时长。
- 步骤6 单击"去支付",完成订单支付。

----结束

## 2.2 购买标准版

## 背景信息

态势感知 SA服务<mark>即将下线</mark>,态势感知 SA的能力将由<mark>安全云脑 SecMaster</mark>服务提供。 为了避免影响您的业务,建议您使用安全云脑,购买安全云脑详细操作请参见<mark>购买安</mark> 全云脑。

态势感知提供基础版、标准版、专业版供您选择。

● 用户可免费体验**基础版**。

基础版仅提供检测部分威胁风险,呈现一定云上资产安全态势。

- 为及时和深入了解资产安全状况,确保云上资产安全,建议您升级为标准版或专业版。
  - 标准版提供一定种类的威胁检测和分析服务,包括威胁分析、告警设置、主机漏洞、安全日志管理等功能。若需要使用标准版,你需根据全局资产数购买配额,一个资产配额支持全方位防护一台资产。
  - 专业版提供更多种类的威胁检测和分析服务,包含威胁分析、告警设置、主机漏洞、网站漏洞、基线检查、安全日志管理及综合大屏等功能。若需使用 专业版服务,您需根据全局资产数购买配额,一个资产配额支持全方位防护 一台资产。

- 更多基础版、标准版、专业版功能差异,请参见<mark>服务版本差异</mark>。
- 综合大屏提供"综合态势感知大屏"和"主机安全态势大屏"两种大屏模式,集 中展示云上综合安全态势和主机安全状况。综合大屏功能为专业版额外选购付费 项目,您可以在购买资产配额后,参考开通综合大屏再购买。

#### 须知

- 基础版不支持退订。
- 标准版不支持直接升级到专业版,且专业版也不支持直接变更到标准版。如需使用 对应版本,需退订当前版本后再进行购买。
- 标准版仅支持通过包周期计费模式进行购买。
- 不支持部分配额购买标准版,部分配额购买专业版。
- 综合大屏为专业版额外选购付费项目,如需使用综合大屏,请先购买专业版。

#### 前提条件

• 已获取管理控制台的登录账号与密码。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。
- 步骤3 在页面右上角单击"升级"。
- **步骤4** (可选)选择使用角色。

默认可选IT运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO四类角色,不同 角色推荐配置不同 。

#### 图 2-1 选择使用角色

使用角色	IT运维人员 关主业务连续性 关主或物定位和消除	合規审计人员 共主合規风险   くの くにの (CISO   くの くにの くにの くにの くにの くにの くにの くにの くにの くにの	
	您可能担心业务中断 🥥 推荐配置 态势感知专业版		

步骤5选择计费模式,"计费模式"选择"包周期",按配置周期计费。

标准版仅支持"包周期"模式。

#### 图 2-2 选择包周期计费

计费模式	推荐包思期 按	蒂	
	📅 "包周期"比"按需"付書	费方式 <mark>优惠33.3%/月</mark> ,如果您长期使用,建议包周期购买。	

步骤6选择态势感知版本, "态势感知版本"选择"标准版"。

态势感知版本	基础版 企业掌握上云的安全合规态势(免费)	标准版 满足企业的云网络和主机的安全运营要求	专业版 满足企业的日常安全运营、合规检查的要求
	安全监控 • 集中呈现云上整体安全评估状况	安全监控 • 集中呈现云上整体安全评估状况	安全监控 <ul> <li>・集中呈现云上整体安全评估状况</li> <li>・联动其他云安全服务集中展示云上安全</li> </ul>
	威胁 • 集中呈现威胁告警事件统计信息	威胁 • 集中呈现威胁告警事件统计信息 • 提供 威胁分析和通知告警 功能	威胁 • 集中呈现威胁告警事件统计信息 • 提供 威胁分析、告警监控和通知告警 功 能
	漏詞管理 ・ 获取业界热点安全漏洞讯息	減同管理 ・ 获取业界热点安全漏洞讯息 ・ 呈现 主机漏洞 扫描結果并提供修复建议	漏洞管理 • 获取业界热点安全漏洞讯息 • 呈现 主机和网站漏洞 扫描结果并提供物 复建议
	基线检查 ・ 无	基线检查 • 检查基线配置风险状态 • 提示 存在安全额患的配置	基线检查 • 检查基线配置风险状态 • 提示存在安全隐患的配置并提供加固键 议
	资 <del>产安</del> 全 ・ 无	资产安全 •集中呈现云上 主机 实时安全状态	资产安全 • 集中呈现云上 主机和网站 实时安全状态
	安全报告 ・ 无	安全报告 • 无	安全报告 ・ 生成阶段性 安全概况、风险趋势报告
	根据云的责任共担模型,分析并评估华为 云租户的安全态势。	分析并评估租户的网络、端点,及使用过 程(权限、操作)的安全合规性、提供租户云 上主机等云资源的安全态势。	分析并评估租户边界、业务应用、虚拟网络、端点、使用过程(权限、操作、配置档查)、提供租户云上资源的安全态势。
	更多版本详情		没有我需要的场景?
主机配额	40 + (本次新増配額: 40) 您当前有40台主机,为防止未接权检测的主机被攻;	5后,您无法及时感知威胁,造成数据泄雷等风险,到	议您购买40台或40台以上的主机配额。
	(当前租户可购买的最大配额: 400 台)		

### **图 2-3** 选择版本

## 步骤7 配置资产配额,相关参数如表1 配置参数说明。

参数	说明
主机配额	主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数,可设置最大主机配 额需等于或大于当前账户下主机总数量,且不支持减少。 主机配额最大限制如下: ● 当前账户下主机总数量≤10台:主机配额最大限制为100台。
	<ul> <li>当前账户下主机总数量&gt;10台:主机配额最大限制=当前账户下主机总数量x10台</li> <li>示例:当前账户下主机总数量为20台,则主机配额最大限制为20x10=200台。</li> </ul>
	<b>说明</b> 为避免主机资产在防护份额外,不能及时感知攻击威胁,而造成数据泄露等安 全风险。当主机资产数量增加后,请及时增加配额数。

#### 表 2-1 配置参数说明

步骤8 选择态势感知使用时长。

## **图 2-4** 选择购买时长

购买时长	1	2	3	4	5	6	7	8	9个月	<mark>8.3折</mark> 1 年	<mark>7折</mark> 2 年	<mark>5折</mark> 3 年
	自动	续费 ⑦										

配置资产配额的使用时长。

计费模式选择"包周期"后,必须配置"购买时长"。

- 可按月(选择1/2/3/4/5/6/7/8/9个月)或按年(选择1/2/3年)购买。
- 在配置总价的基础上,购买1年享受8.3折优惠,购买2年享受7折优惠,购买3
   年享受5折优惠。
- 勾选"自动续费"。在账户余额充足前提下,当购买的版本即将到期时,自动续费,不影响使用。

#### 表 2-2 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1年	1年

🛄 说明

- 若需对不同资产配置不同使用时长,请参考增加资产配额。
- 更多关于自动续费修改、取消等操作说明,请参见自动续费规则说明。
- 步骤9 配置完成后,单击"立即购买"。
- **步骤10** 进入"订单详情"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"去支付"。
- 步骤11 在支付页面,选择付款方式完成付款。
- 步骤12 成功付款后,返回态势感知控制台页面,确认已生效和到期时间。

----结束

## 后续管理

图 2-5 版本管理窗口

标准版			
·计费方式	包周期	续费 退订	
	1台主机2021/12/6到期		
·主机配额	1台	增加配额	

- 若需变更资产配额,可单击"增加配额",添加资产配额购买,详细说明请参见 增加资产配额。
- 若购买的包周期版本即将到期或已经到期,可单击"续费",延长当前包周期资源的使用期限,详细说明请参见续费。
- 若不再使用资产配额功能,可单击"退订"或"取消",退订相应态势感知服务,详细说明请参见退订。

## 2.3 购买专业版

## 背景信息

态势感知 SA服务<mark>即将下线</mark>,态势感知 SA的能力将由<mark>安全云脑 SecMaster</mark>服务提供。 为了避免影响您的业务,建议您使用安全云脑,购买安全云脑详细操作请参见<mark>购买安</mark> 全云脑。

态势感知提供基础版、标准版、专业版供您选择。

- 用户可免费体验基础版。
   基础版仅提供检测部分威胁风险,呈现一定云上资产安全态势。
- 为及时和深入了解资产安全状况,确保云上资产安全,建议您升级为标准版或专业版。
  - 标准版提供一定种类的威胁检测和分析服务,包括威胁分析、告警设置、主机漏洞、安全日志管理等功能。若需要使用标准版,你需根据全局资产数购买配额,一个资产配额支持全方位防护一台资产。
  - 专业版提供更多种类的威胁检测和分析服务,包含威胁分析、告警设置、主机漏洞、网站漏洞、基线检查、安全日志管理及综合大屏等功能。若需使用 专业版服务,您需根据全局资产数购买配额,一个资产配额支持全方位防护 一台资产。
  - 更多基础版、标准版、专业版功能差异,请参见<mark>服务版本差异</mark>。
- 综合大屏提供"综合态势感知大屏"和"主机安全态势大屏"两种大屏模式,集 中展示云上综合安全态势和主机安全状况。综合大屏功能为专业版额外选购付费 项目,您可以在购买资产配额后,参考开通综合大屏再购买。

#### 须知

- 基础版不支持退订。
- 标准版不支持直接升级到专业版,且专业版也不支持直接变更到标准版。如需使用 对应版本,需退订当前版本后再进行购买。
- 标准版仅支持通过包周期计费模式进行购买。
- 不支持部分配额购买标准版,部分配额购买专业版。
- 综合大屏为专业版额外选购付费项目,如需使用综合大屏,请先购买专业版。

### 前提条件

• 已获取管理控制台的登录账号与密码。

## 包周期方式

步骤1 登录管理控制台。

**步骤2** 在页面左上角单击 — ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。

- 步骤3 在页面右上角单击"升级"。
- **步骤4** (可选)选择使用角色。

默认可选IT运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO四类角色,不同 角色推荐配置不同。

图 2-6 选择使用角色

使用角色	○ IT运進人员 关注或务理操性	A 合規审计人员 关注合规风险 CSO/CIO/CISO 关注合规风险 CSO/CIO/CISO	
	您可能担心业务中断 🔘 推荐配置 态势感知专业版		_

步骤5选择计费模式,"计费模式"选择"包周期",按配置周期计费。

图 2-7 选择包周期计费

计费模式	包周期 按需
	台 "包周期"比"按焉"付费方式代事33.3%/月,如果您长期使用,建议包周期购买。

步骤6选择态势感知版本。

当前默认选择"专业版",由基础版功能升级为专业版功能。

**图 2-8** 选择版本

态势感知版本	😔 基础版	◎ 标准版	◎ 专业版
	企业掌握上云的安全合规态势 (免费)	满足企业的云网络和主机的安全运营要求	满足企业的日常安全运营、合规检查的要求
	安全监控 <ul> <li>集中呈现云上整体安全评估状况</li> </ul>	安全监控 <ul> <li>集中呈现云上整体安全评估状况</li> </ul>	安全监控 • 集中呈现 <u>云上整</u> 体安全评估状况 • <b>联动其他云安全服务</b> 集中展示云上安全
	威胁 • 集中呈现威胁告警事件统计信息	威胁 • 集中呈现威胁告警事件统计信息 • 提供 威胁分析和通知告警 功能	威胁 • 集中呈现威胁告警事件统计信息 • 提供 威胁分析、告警监控和通知告警 功 能
	漏洞管理 • 获取业界热点安全漏洞讯息	漏同管理 • 获取业界热点安全漏洞讯息 • 呈现 主机漏洞 扫描结果并提供修复建议	漏洞管理 • 获取业界热点安全漏洞讯息 • 呈现 主机和网站漏洞 扫描结果并提供修 复建议
	基地合 ・ 无	基线检查 • 检查基线配置风险状态 • 提示存在安全稳定的配置	基线检查 • 检查基线配置风险状态 • 提示存在安全隐患的配置并提供加固建 议
	资 <del>产安</del> 全 ・ 无	资产安全 • 集中呈现云上 主机 实时安全状态	资产安全 • 集中呈现云上 主机和网站 实时安全状态
	安全报告 ・ 无	安全报告 ・ 无	安全报告 ・ 生成阶段性 <b>安全概况、风险趋势报告</b>
	根据云的责任共担横型,分析并评估华为 云租户的安全态势。	分析并评估租户的网络、谎点,及使用过 程(权限、操作)的安全合规性、提供租户云 上主机等云资源的安全态势。	分析并评估租户边界、业务应用、虚拟网络、端点、使用过程(权限、操作、配置检查)、提供租户云上资源的安全态势。
	更多版本详情		没有我需要的场景? 补充
主机配额	12 + (本次新増配額: 11)     悠当前有12台主机,为防止未抵权检测的主机被双击     (当前租户可购买的最大配额: 120 台)	后,您无法及时感知威胁,造成数据泄露等风险,建	议您购买12台或12台以上的主机配额。

步骤7 配置资产配额,相关参数如表1 配置参数说明。

#### 表 2-3 配置参数说明

参数	说明
主机配额	主机资产支持防护的最大主机数量。
	请根据当前账户下所有主机资产总数设置配额数,可设置最大主机配 额需等于或大于当前账户下主机总数量,且不支持减少。
	主机配额最大限制如下:
	● 当前账户下主机总数量≤10台: 主机配额最大限制为100台。
	<ul> <li>当前账户下主机总数量&gt;10台:主机配额最大限制=当前账户下主机总数量x10台</li> <li>示例:当前账户下主机总数量为20台,则主机配额最大限制为20x10=200台。</li> </ul>
	<b>说明</b> 为避免主机资产在防护份额外,不能及时感知攻击威胁,而造成数据泄露等安 全风险。当主机资产数量增加后,请及时增加配额数。

### 步骤8 (可选)开通综合大屏功能。

#### 图 2-9 选择安全大屏

19958.85	([ and access ( ) ] )	VALUE AN
i		
and the second s		0000 💳
	~ *° 🚞 🖵	
综合态势感知	预览 主机安全态势	预览

- **综合大屏**功能为增值付费项。
- 在勾选购买"安全大屏"时,可与资产配额一起购买,或在购买资产配额后再补充购买。

### 🛄 说明

"安全大屏"必须与资产配额搭配购买,不能单独购买,因在检测到资产的威胁攻击后,才能通过分析分类呈现安全态势大屏。

步骤9 选择态势感知使用时长。

### **图 2-10** 选择购买时长

胸決时长 1 2 3 4 5 6 7 8 9个月 1年 2年 3年 自动検費 ⑦

- 配置资产配额的使用时长。
  - 计费模式选择"包周期"后,必须配置"购买时长"。
  - 可按月(选择1/2/3/4/5/6/7/8/9个月)或按年(选择1/2/3年)购买。

- 在配置总价的基础上,购买1年享受8.3折优惠,购买2年享受7折优惠,购买3
   年享受5折优惠。
- 勾选"自动续费"。在账户余额充足前提下,当购买的版本即将到期时,自动续费,不影响使用。

表 2-4 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1年	1年

🛄 说明

- 若需对不同资产配置不同使用时长,请参考增加资产配额。
- 更多关于自动续费修改、取消等操作说明,请参见**自动续费规则说明**。
- 步骤10 配置完成后,单击"立即购买"。
- **步骤11** 进入"订单详情"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"去支付"。
- 步骤12 在支付页面,选择付款方式完成付款。
- 步骤13 成功付款后,返回态势感知控制台页面,确认已生效和到期时间。

----结束

按需方式

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制台。
- 步骤3 在页面右上角单击"升级"。
- 步骤4 (可选)选择使用角色。

默认可选IT运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO四类角色,不同 角色推荐配置不同。

图 2-11 选择使用角色

使用角色	○ IT运维人员 关注业务连续性	安全运维人员 关注威胁定位和消除	名规审计人员 关注合规风险	CSO/CIO/CISO 关注整体安全态势	
	您可能担心业务中断 🕚 推荐配置	态势感知专业版			

**步骤5**选择计费模式,"计费模式"选择"按需",按小时计费。

从开通开始到取消结束,按实际防护时长(小时)计费。

图 2-12 选择按需计费

计费模式		推 包周期	3	按需			
	Ħ	"包周期" 比	"按焉"	付费方式 <mark>优</mark>	憲33.3%/月,	如果您长期使用,	建议包周期购买。

### 步骤6选择态势感知版本。

当前默认选择"专业版",由基础版功能升级为专业版功能。

态势感知版本		◎ 标准版 诺尼公业的于网络和主机的安全运费要求	
		★ 集中呈现 <u>元上整</u> 体安全评估状况	<ul> <li>→ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>
	威胁 • 集中呈现威胁告警事件统计信息	成動 <ul> <li>集中呈现或動告警事件統計信息</li> <li>提供 或動分析和通知信誉 功能</li> </ul>	威胁 • 集中呈现威胁告警事件统计信息 • 提供 威胁分析、告警监控和通知告警 功 能
	漏洞管理 • 获取业界热点安全漏洞讯息	漏洞管理 ・ 获取业界热点安全漏洞讯息 ・ 呈现 主机漏洞 扫描结果并提供修复建议	漏洞管理 • 获取业界热点安全漏洞讯息 • 呈现主机和网站漏洞 扫描结果并提供修 复建议
	基地检查 ・ 无	基线检查 · 检查基线配置风险状态 · 提示存在安全隐患的配置	基线检查 • 检查基线配置风险状态 • 提示存在安全隐患的配置并提供加固建 议
	<u>済~安</u> 全 ・无	资产安全 • 集中呈现云上 主机 实时安全状态	资 <del>产安全</del> • 集中呈现云上 <b>主机和网站</b> 实时安全状态
	安全振告 ・ 无	安全振告 ・ 无	安全报告 • 生成阶段性 安全概况、风险趋势报告
	根据云的责任共相模型,分析并评估华为 云租户的安全态势。	分析并评估租户的网络、端点,及使用过 程(权限、操作)的安全合规性、提供租户云 上主们等云资源的安全态势。	分析并评估租户边界、业务应用、虚拟网络、 謊点、使用过程(权限、操作、配置检查)、提供租户云上资源的安全态势。
	更多版本详情		没有我需要的场景? 补充
主机配额	12 + (本次新措配额: 11)     您当前有12台主机,为防止未授权检测的主机核攻击     (当前租户可购买的最大配额: 120台)	后,您无法及时想知威胁,造成数据世最等风险,建	议您购买12台或12台以上的主机配额。

**图 2-13** 选择版本

## 步骤7 配置资产配额,相关参数如表1 配置参数说明。

### 表 2-5 配置参数说明

参数	说明
主机配额	主机资产支持防护的最大主机数量。
	请根据当前账户下所有主机资产总数设置配额数,可设置最大主机配 额需等于或大于当前账户下主机总数量,且不支持减少。
	主机配额最大限制如下:
	● 当前账户下主机总数量≤10台: 主机配额最大限制为100台。
	<ul> <li>当前账户下主机总数量&gt;10台:主机配额最大限制=当前账户下主机总数量x10台</li> <li>示例:当前账户下主机总数量为20台,则主机配额最大限制为20x10=200台。</li> </ul>
	<b>说明</b> 为避免主机资产在防护份额外,不能及时感知攻击威胁,而造成数据泄露等安 全风险。当主机资产数量增加后,请及时增加配额数。

步骤8 (可选)开通综合大屏功能。

#### **图 2-14** 选择安全大屏

2012/08/08/09/09/09/09/09/09/09/09/09/09/09/09/09/	-	( Anno According and ) VIIIIII	n
0			
			00
	•- • • •		
综合态势感知	预览	主机安全态势	预览

- **综合大屏**功能为增值付费项。
- 在勾选购买"安全大屏"时,可与资产配额一起购买,或在购买资产配额后再补充购买。

#### 🛄 说明

"安全大屏"必须与资产配额搭配购买,不能单独购买,因在检测到资产的威胁攻击后,才能通过分析分类呈现安全态势大屏。

- 步骤9 配置完成后,单击"立即购买"。
- **步骤10** 进入"订单详情"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"确认开通"。
- 步骤11 返回态势感知控制台页面,确认按需版本已生效。

----结束

## 后续管理

图 2-15 版本管理窗口

专业版		
·计费方式	包周期	续费 退订
	1台主机2022/6/	21到期
·主机配额	1台	增加配额
安全大屏 (未开通	)	立即开通
·综合态势大屏		了解更多
·主机安全大屏		了解更多

- 若需变更资产配额,可单击"增加配额",添加资产配额购买,详细说明请参见 增加资产配额。
- 若未同时开通综合大屏功能,可单击"立即开通",开通大屏功能,详细说明请参见开通综合大屏。

- 若购买的按需资源后,需长期使用态势感知服务,可单击"转包周期",将资源 计费模式转为包年/包月,详细说明请参见按需转包周期。
- 若购买的包周期版本即将到期或已经到期,可单击"续费",延长当前包周期资源的使用期限,详细说明请参见续费。
- 若不再使用资产配额或综合大屏功能,可单击"退订"或"取消",退订相应态 势感知服务,详细说明请参见退订。

## 2.4 开通综合大屏

综合大屏根据检测数据,资产安全数据可视化,集中呈现综合安全态势和主机全局安 全。为充分呈现云上安全态势,建议您在购买态势感知资产配额后,再开通综合大屏 功能。

## 包周期方式

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制台。
- 步骤3 单击"增加配额",跳转到态势感知购买页面。
- 步骤4 查看当前配置。

图 2-16 查看当前配置

当前配置 专业版定题 主机函数 4台 (包周期: 0台; 按署4台) 网站配数 1个 安全大屏 已开通 (按署付赛)

步骤5选择计费模式,"计费模式"选择"包年/包月",按配置周期计费。

图 2-17 选择包周期计费

计表统式
 包閣期
 「
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*
 \*\*

步骤6 勾选"安全大屏"。

图 2-18 选择安全大屏

manager and Barbar	IK	( term assessment press ) VALETTER	*EN
	see 199		۵ 🎓
		artostatum	

步骤7选择"购买时长"。

#### **图 2-19** 选择购买时长

□ 自动续费 ⑦	购买时长	1	2	3	4	5	6	7	8	9个月	<mark>8.3折</mark> 1 年	<mark>7折</mark> 2 年	<mark>5折</mark> 3 年
		自动	续费(?	)									

#### 🛄 说明

综合大屏的"配置费用"根据大屏的使用时长计算。已有资产配额不会重复计费,请放心购买。

- 步骤8 配置完成后,单击"立即购买"。
- **步骤9** 进入"订单确认"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"去支付"。
- **步骤10** 在支付页面完成付款后,返回态势感知控制台页面,即可查看综合态势感知和主机安全态势两个大屏。

----结束

### 按需方式

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。
- 步骤3 单击"增加配额",跳转到态势感知购买页面。
- 步骤4 查看当前配置。

图 2-20 查看当前配置

当前配置		
专业版配额	主机配额 4台(包周期:0台,按需4台)	网站配额 1个
安全大屏	已开通 (按需付费)	

**步骤5**选择计费模式,"计费模式"选择"按需计费",按小时计费。 从开通开始到取消结束,按实际防护时长(小时)计费。

#### 图 2-21 选择按需计费

计费模式	<u>推訪</u> 包現現 <u>比素</u>	
	"包周期"比"按秦"付舞方式优=33.3%/月,如果您长期使用,建议包周期购买。	

步骤6 勾选"安全大屏"。

#### **图 2-22** 选择安全大屏

安全大屏	□ 开通 安全态势大屏让您的	攻防态势尽收眼底,	了解更多			
	综合态势感知	预览 主持	几安全态势	预览		

步骤7 配置完成后,单击"立即购买"。

- **步骤8** 进入"订单确认"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"确认开通"。
- 步骤9 返回态势感知控制台页面,即可查看综合态势感知和主机安全态势两个大屏。

----结束

## 后续管理

- 若购买的按需资源后,需长期使用综合大屏功能,可在综合大屏管理页面,单击 "转包周期",将资源计费模式转为包年/包月,详细说明请参见按需转包周期。
- 若购买的包周期综合大屏即将到期或已经到期,可在综合大屏管理页面,单击 "续费",延长当前包周期资源的使用期限,详细说明请参见续费。
- 若不再使用综合大屏功能,可在综合大屏管理页面,单击"退订"或"取消", 退订相应态势感知服务,详细说明请参见退订。

## 2.5 增加资产配额

购买态势感知资产配额完成后,当用户资产数量增加,或需对不同资产有不同使用时 长需求,可参考本小节扩充"主机配额",并配置使用时长。

### 约束限制

• 主机配额是授权检测主机的数量。主机配额最大限制如下:

#### 表 2-6 主机配额最大限制

当前账户下主机总数量/台	主机最大配额/台
当前账户下主机总数量≤10	100
当前账户下主机总数量>10	当前账户下主机总数量x10 示例:已有20台主机,则主机最大配额为 20x10=200。

 在购买态势感知时,选择的最大配额需等于或大于当前账户下主机总数量,且不 支持减少。若购买的最大配额小于主机数量,可能会造成如下影响:
 未授权检测的主机被攻击后,不能及时感知威胁,造成数据泄露等风险。

## 包周期方式

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制台。
- 步骤3 单击右上角"增加配额",跳转到态势感知购买页面。

步骤4 查看当前配置。

步骤5选择计费模式,"计费模式"选择"包周期",按配置周期计费。

步骤6 配置"主机配额",在原有配额数基础上,增加的资产配额数。

步骤7选择"购买时长"。

🛄 说明

- 选择的"购买时长"为新增配额的使用时长,不影响已购买配额的使用时长。
- 增加配额的"配置费用"根据新增资产的配额数和使用时长计算。已有资产配额不会重复计费,请放心购买。
- 若需延长已购买配额的使用时间,请参见续费为目标配额延长使用时间。
- 步骤8 配置完成后,单击"立即购买"。
- **步骤9** 进入"订单确认"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"去支付"。
- **步骤10** 在支付页面完成付款后,返回态势感知控制台页面,即可对相应配额数的主机进行安全防护。

----结束

### 按需方式

步骤1 登录管理控制台。

- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制台。
- 步骤3 单击"增加配额",跳转到态势感知购买页面。
- 步骤4 查看当前配置。
- 步骤5选择计费模式,"计费模式"选择"按需",按小时计费。

从开通开始到取消结束,按实际防护时长(小时)计费。

- 步骤6 配置"主机配额",在原有配额数基础上,增加的资产配额数。
- 步骤7 配置完成后,单击"立即购买"。
- **步骤8** 进入"订单确认"页面,确认订单无误并阅读《态势感知服务免责声明》后,勾选 "我已阅读并同意《态势感知服务(SA)免责声明》",单击"确认开通"。
- 步骤9 返回态势感知控制台页面,即可对相应配额数的主机进行安全防护。

----结束

## 2.6 续费

态势感知续费是在原已购买的版本规格的基础上,延长使用时间。续费操作不可变更版本规格,即不能改变"主机配额"和"综合大屏"选择。

续费操作仅针对包周期版本规格。

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

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

#### 🛄 说明

资产配额与综合大屏功能需分别续费。

#### 手动续费

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。
- 步骤3 单击右上角"标准版"或"专业版",显示版本管理窗口。
- 步骤4 单击"续费",系统跳转至费用中心"续费管理"页面。
- 步骤5 在态势感知专业版实例所在行,单击"续费",跳转至"续费"页面。
- 步骤6 配置"选择续费时长",如选择"一年"。
- 步骤7 单击"去支付",跳转至支付页面,完成付款。
- 步骤8 返回续费管理页面,可查看态势感知已续费成功。

----结束

#### 开通自动续费

在账户余额充足前提下,已配置"自动续费"后,包周期版本的资产配额和综合大屏 将自动续费,延长使用周期。

自动续费的相关注意事项,请参见自动续费规则说明。

- 步骤1 登录管理控制台。
- 步骤2 单击"费用 > 续费管理",跳转至费用中心"续费管理"页面。
- **步骤3** 在"手动续费项"页签,选择态势感知专业版实例,单击"开通自动续费",跳转至自动续费配置页面。
- 步骤4 选择配置"自动续费周期"和勾选"预设自动续费次数"。
- 步骤5 单击"开通",完成自动续费配置。
- **步骤6** 返回续费管理页面,在"自动续费项"页签,可查看态势感知已开通自动续费。 后续将根据配置,自动续费延长使用期。

----结束

## 2.7 退订

若用户不再使用态势感知防护功能或综合大屏,可执行退订或一键取消操作。

 包周期(包年/包月)计费模式:预付费方式。新购5天内的资源,支持每年10次5 天无理由"退订";使用超过5天的资源,"退订"需要收取手续费。

- 按需计费模式:按小时计费方式。资源即开即停,支持一键"取消"释放资源。
   **〕说明**
  - 免费版不支持退订。
  - 资产配额与综合大屏功能需分别退订/取消。
  - 当资产配额被全部退订/取消后,即当前为基础版时。您需单击"综合大屏",进入大屏管理页面,在页面右上角再执行退订或取消综合大屏功能。

更多费用和订单说明信息,请参见<mark>费用中心</mark>。

## 退订包周期计费

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。
- 步骤3 单击右上角"标准版"或"专业版",显示版本管理窗口。
- **步骤4**针对包周期购买的资产配额或综合大屏,单击"退订",进入"退订管理"列表页面。

图 2-23 退订包周期计费

专业版				
·计费方式	包周期		续费	退订
	1台主机2022/6/2	1到期		
·主机配额	1台		増加	旧配额
安全大屏 (未开通)			立日	卯开通
·综合态势大屏		了解更	8	
·主机安全大屏		了解更	3	

- **步骤5** 在需要退订的实例所在行,单击"操作"列中的"退订资源",进入"退订资源"页面。
- 步骤6 确认待退订资源信息,选择退订原因,并勾选退订确认。
- 步骤7 单击"退订",在退订管理页面确认退订。

退订成功后,返回版本管理窗口,包年/包月计费的资产配额已取消。

----结束

#### 取消按需计费

步骤1 登录管理控制台。

文档版本 54 (2022-11-24)

- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。
- 步骤3 单击右上角"专业版",显示版本管理窗口。
- 步骤4 针对按需购买的版本或综合大屏,单击"取消",一键释放按需计费的资产配额。

图 2-24 取消按需计费

专业版			
·计费方式	按需	🏙 转包周期	取消
·主机配额	4台	増加	加配额
安全大屏			
·计费方式	按需	🛍 转包周期	取消
·综合态势大屏			查看
·主机安全大屏			查看

返回版本管理窗口,按需计费的资产配额资源已取消。

----结束

## 退订综合大屏

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理控制 台。
- 步骤3 在左侧导航栏中选择"综合大屏",进入态势感知综合大屏页面。
- **步骤4** 单击右上角"取消按需"或"取消包周期",并在弹出的确认框中单击"是",取消按需或包年/包月计费的综合大屏。

#### 图 2-25 退订综合大屏

态势感知	综合大屏	计表模式 按聲 🗂 转包周期 取消按器
安全甄远 史證整理 业务分析 • 【400大屏 重於法母 周所愿理 基成位量 台別成果 公共的母		
分析报告 日志管理		
安全产品集成 设置 <b>*</b>		

系统返回态势感知综合大屏页面,并显示为待开通状态,按需或包年/包月计费的综合 大屏已取消。

----结束

## 2.8 态势感知升级至安全云脑

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。

安全云脑是态势感知的升级版本,后续功能变更、版本迭代也将在安全云脑中进行。 因此,建议您升级至安全云脑。

## 升级说明

- 升级只支持从态势感知升级至安全云脑,不支持从安全云脑变更至态势感知。
- 升级时,需要将态势感知配额分配到不同区域,以及后续会关闭态势感知购买通 道,请提前做好配合规划。
- 升级后,态势感知和安全云脑的生命周期共享,如果订单为按需类型,则仍需在 原态势感知页面处理。
- 升级完成后,不支持在安全云脑中进行变更操作,如果需要执行版本升级或配额 增加等操作,请在原态势感知中进行处理。

### 将态势感知升级至安全云脑

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",默认进入态势感知安全概 览页面。
- 步骤3 在页面右上角,单击"升级到安全云脑"。

#### 图 2-26 升级至安全云脑



步骤4 在升级至安全云脑页面中, 配置参数信息。

- 版本关系:系统已自动同步SA的版本关系(版本、计费模式和安全大屏),无需 手动配置。
- 配额分配:将态势感知全部额分配至安全云脑,在安全云脑配额中填写配额数。

步骤5 单击"立即升级"。

升级完成后,请在页面左上角单击——,	选择"安全与合规 > 安全云	这
SecMaster",进入安全云脑管理页面,	使用安全云脑管理云上资源,	详细介绍和操作
指导请参见 <mark>安全云脑介绍文档</mark> 。		

----结束



## 3.1 总览

SA的"安全概览"页面实时呈现云上整体安全评估状况,并联动其他云安全服务,集 中展示云上安全。在"安全概览"查看安全概览信息和相关一键操作,实现云上安全 态势一览和风险统一管控。

您可以在"安全概览"页面查看您的资产安全总览情况,并进行相关操作。"安全概 览"分为以下几个板块:

- 安全评分
- 安全监控
- 安全趋势
- 威胁检测

## 安全评分

"安全评分"板块根据不同版本的威胁检测能力,评估整体资产安全健康得分,可快速了解未处理风险对资产的整体威胁状况,如<mark>图3-1</mark>。

#### **图 3-1** 安全评分



- 分值范围为0~100,分值越大表示风险越小,资产更安全,安全分值详细说明请参见安全评分。
- 分值环形图不同颜色表示不同威胁等级。例如,黄色对应"中危"。
- 单击"立即处理",系统右侧弹出"安全风险处理"页面,您可根据该页面的提示,参考对应的帮助文档或直接对风险进行处理。

- 安全风险处理页面中包含所有需要您尽快处理的安全风险和威胁,分为"威胁告警"、"漏洞"、"合规检查"三大类别。
- "安全风险处理"页面中显示的数据为最近/最新检测后的数据结果,"检测结果"页面(单击"前往处理",进入该页面)显示的是所有检测时间的各类数据详情,因此,安全风险处理页面的数据总数≤检测结果页面的数据总数。
- 处理安全风险:
  - 在"安全评分"栏中,单击"立即处理",系统右侧弹出"安全风险处 理"页面。
  - ii. 在"安全风险处理"页面中,单击"前往处理",进入检测结果页面。
  - iii. 选择一个或多个"未处理"状态的结果,单击"忽略"或"标记为线下 处理",对不同检测结果批量执行相应的处理操作。
    - 忽略:如果确认该检测结果不会造成危害,在"忽略风险项"窗口 记录"处理人"、"忽略理由",可标记为"已忽略"状态。
    - 标记为线下处理:如果该检测结果已在线下处理,在"标记为线下处理"窗口记录"处理人"、"处理时间"和"处理结果",可标记为"已线下处理"状态。
- 资产风险修复,并手动刷新告警事件状态后,安全评分实时更新。资产安全风险 修复后,也可以直接单击"重新检测",重新检测资产并进行评分。

🛄 说明

- 由于检测需要一定的时间,请您在单击"重新检测"按钮5分钟后,再刷新页面,查看 最新检测的安全评分。
- 资产安全风险修复后,为降低安全评分的风险等级,需手动忽略或处理告警事件,刷新告警列表中告警事件状态。
- 安全评分显示为历史扫描结果,非实时数据,如需获取最新数据及评分,可单击 "重新检测",获取最近的数据。

## 安全监控

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

#### **图 3-2** 安全监控

安全监持	Ŷ								
威胁	) <b>告警</b> [近7天]		<b>12</b> 页	漏洞		<b>46</b> 页	合规检查		<b>144</b> 页
致命	0	高危 1	其他 11	致命 4	高危 22	其他 20	致命 1	高危 58	其他 85

## 表 3-1 安全监控参数说明

参数名称	参数说明						
威胁告警	呈现最 <b>近7天内</b> 未处理威胁告警,可快速了解资产遭受的威胁告 类型和数量,呈现威胁告警的统计结果。						
	• 此处严重等级含义如下:						
	<ul> <li>- 致命:即致命风险,表示您的资产中检测到了入侵事件, 议您立即查看告警事件的详情并及时进行处理。</li> </ul>						
	<ul> <li>高危:即高危风险,表示资产中检测到了可疑的异常事件, 建议您立即查看告警事件的详情并及时进行处理。</li> <li>其他:即其他类型(中危、低危、提示)风险,表示服务器 中检测到了有风险的异常事件,建议您及时查看该告警事件 的详情。</li> <li>单击威胁告警模块,系统将列表实时呈现近7天内TOP5的威胁 告警事件,可快速查看威胁告警详情,监控威胁告警状况,如 图3-3所示。</li> <li>列表呈现近7天TOP5的威胁告警事件的信息,包括威胁告警 名称、告警等级、资产名称、告警发现时间。</li> </ul>						
	- 若列表显示内容为空,表示近7天无威胁告警事件。						
	<ul> <li>单击"查看更多",可跳转到"检测结果"页面,查看更多的威胁告警信息,并可自定义过滤条件查询告警信息,查看威胁告警详细操作请参见告警列表。</li> <li>图 3-3 查看实时威胁告警</li> </ul>						
宋谢监控最新威胁伯管事件 Top5 🔮 实时绘制中 皇帝更多							
	标题 卷缀 第户名称 发现时间						
	SSH BruteForce • 20# ecs 9 2022-01-05T163230.019+08.00						
	SSH BruteForce         ● 高監         ecc         )         2022-01-0571-632-40.019+060.0						
	RDP BruteForce限就 ●中告 ecs-> 32 2022-01-11110-22:02.914-08:00						
	SSH BruteForce ●中意 ecc 9 2022-01-057163330.019+08:00						

参数名称	参数说明					
漏洞	展示您资产中TOP5漏洞类型,以及 <b>近24小时内</b> 还未修复的漏洞总 数和不同漏洞风险等级对应的数量。					
	• 此处严重等级含义如下:					
	- 致命:即致命风险,表示您的资产中检测 议您立即查看漏洞事件的详情并及时进行	到了漏洞事件,建 处理。				
	<ul> <li>高危:即高危风险,表示资产中检测到了可疑的异常事件,</li> <li>建议您立即查看漏洞事件的详情并及时进行处理。</li> </ul>					
	<ul> <li>- 其他:即其他类型(中危、低危、提示))</li> <li>中检测到了有风险的异常事件,建议您及</li> <li>情。</li> </ul>	风险,表示服务器 时查看该漏洞的详				
	<ul> <li>单击漏洞模块中的"漏洞类型Top5"栏,系约 TOP5(根据某个漏洞影响的主机数量进行排型。</li> </ul>	统将列表呈现 序)的漏洞类				
	<ul> <li>一 本。</li> <li>一 此处的TOP等级是根据某个漏洞影响的主机数量进行</li> <li>一 受影响主机数量越多排名越靠前。</li> </ul>					
	- 仅当主机中Agent版本为2.0时,才会在" 中显示对应数据。如未显示数据或需要查 型,请将主机将Agent1.0升级至Agent2.0	<sup>-</sup> 会在"漏洞类型Top5" 濡要查看TOP5漏洞类 gent2.0。				
图 3-4 漏洞类型 漏洞类型 Top5 实时监控最新漏洞风险事件 Top5 💊 实时检测中						
						漏洞编号
	CVE-2022- 56	1				
	CVE-2022 39	1				
	CVE-2021- 19	1				
	CVE-2021- ?	1				
	CVE-2022-7 0	1				
	<ul> <li>单击漏洞模块中的"实时监控最新漏洞风险事系统将列表实时呈现近24小时内TOP5的漏洞 看漏洞详情,如图3-5所示。</li> </ul>	事件 Top5 " 栏, ]事件,可快速查				
	– 列表呈现当日最新TOP5漏洞事件详情,包 洞等级、资产名称、漏洞发现时间。	2括漏洞名称、漏				
	– 若列表显示内容为空,表示当日无漏洞事	件。				
	<ul> <li>单击"查看更多",可跳转到"检查结果</li> <li>的漏洞信息,并可自定义过滤条件查询漏</li> <li>详细操作请参见漏洞列表。</li> </ul>	"页面,查看更多 洞信息,查看漏洞				

参数名称	参数	敗说明						
	图 3-5 查看实时漏洞							
		羅姆獎型 Top5 实时监控最新羅阿风能事件 Top5 📦 该时检测中						
		标题		等级	资产名称		发现时间	
		EulerOS-SA-20	(expat securit	● 致命	cnnorth	mgr-002	2022-07-01T05:25:11.176+08:00	
		EulerOS-SA-20	(hesiod securi	<ul> <li>政命</li> </ul>	cnnort	ngr-002	2022-07-01T05:25:11.176+08:00	
		EulerOS-SA-202	gnutls securi	<ul> <li>政命</li> </ul>	cnnorth	1gr-002	2022-07-01T05:25:11.176+08:00	
		EulerOS-SA-	· (lz4 security u	<ul> <li>設命</li> </ul>	cnnort	Ir-002	2022-07-01T05:25:11.176+08:00	
		EulerOS-SA-2	(libX11 securi	<ul> <li>● 数命</li> </ul>	cnnor	_ ∿002	2022-07-01T05:25:11.176+08:00	
合规检查	展示您资产中 <b>近30天内</b> 存在的合规风险总数量和不同危险等级的 合规检查风险对应的数量。 • 此处严重等级含义如下:						级的	
		- 玖ௗ 置,	建议您	立即查看合語	示您的资广 规异常事件	中位派	斯利丁尔吕规斯	的配 处理。
		- 高危 建议	5:即高 2您立即	危风险,表 查看合规异	示资产中检 常事件的详	浏到了 結件并及	了可疑的异常的。 时进行处理。	配置, 。
		- 其他 中枢 项目	b: 即其 逾测到了 目的详情	他类型(中) 有风险的异 。	仓、低危、 常配置,建	提示) 設您及	风险,表示度 数时查看该合规	服务器 见检查
	•	单击合 的合规 示。	规检查! 检查异?	异常模块,系 常事件,可惊	系统将列表 快速查看合:	实时呈 规检查	现 <b>近30天内</b> T 详情,如 <mark>图</mark> 3	OP5 - <mark>6</mark> 所
	<ul> <li>列表呈现最近一次合规检查中TOP的合规异常事件详情,包</li> <li>括合规检查项目名称、等级、资产名称、发现时间。</li> </ul>							
		- 若列	表显示	内容为空.	表示近30天	无合规	见异常事件。	
	<ul> <li>单击"查看更多",可跳转到"检查结果"页面,查看更多的合规异常信息,并可自定义过滤条件查询合规检查信息, 查看合规检查详细操作请参见基线检查列表。</li> </ul>							
	图 3-6 查看合规异常事件							
		实时监控最新基线异	🛱 Top5 🌖 实时检测	9 <b>中</b>			查看更多	
		标题 Septemble data - *	an result	等级	资产名称	*	現时间	
		EVS disk encryption	n	<ul> <li>= 1,4P</li> <li>● 高茂</li> </ul>	te 46	20	222-01-10715:27:13.156+08:00	
		EVS disk encryptio	n		test-6a !	20	022-01-10T15:27:13.156+08:00	
		EVS disk encryptio	n	<ul> <li>● 高色</li> </ul>	test-56	)2 20	022-01-10T15:27:13.156+08:00	
		EVS disk encryptio	n	<ul> <li>● 高冠</li> </ul>	test-56	00 20	022-01-10T15:27:13.156+08:00	

## 安全趋势

"安全趋势"板块展示近7天内您的整体资产安全健康得分的趋势图。

#### **图 3-7** 安全趋势



## 威胁检测

"威胁检测"板块展示近7天内您的资产中检测到的告警数量及类型。

威胁检测服务(Managed Threat Detection,MTD)持续监控恶意活动和未经授权的 行为,从而保护账户和工作负载。该服务通过集成AI智能引擎、威胁情报、规则基线 等检测模型,识别各类云服务日志中的潜在威胁并输出分析结果,从而提升用户告 警、事件检测准确性,提升运维运营效率。

开通威胁检测服务(MTD)后,才支持检测云服务日志数据中的访问行为,发现是否 存在潜在威胁,对可能存在威胁的访问行为生成告警信息,输出告警结果。如果未开 通,请单击"立即开通",购买威胁检测服务。

<b>图 3-8</b> 开诵威肋	1枪测服务
-------------------	-------

<b>威胁检测</b> [未开通]		华东-上海一	•
	为了保护您的云账号、网络. 能力,建议开启威胁检测服:	,存储等资源环境,提高 务。	与安全风险识别
	立即开通了解更	\$	

## 3.2 安全评分

态势感知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。

本章节将介绍在安全评分中,不同分值的含义以及扣分项的详细情况。

## 安全分值

SA根据不同版本的威胁检测能力,评估整体资产安全健康得分。

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

🛄 说明

- 由于检测需要一定的时间,请您在单击"重新检测"按钮5分钟后,再刷新页面,查看 最新检测的安全评分。
- 资产安全风险修复后,为降低安全评分的风险等级,需手动忽略或处理告警事件,刷新告警列表中告警事件状态。

#### **表 3-2** 安全分值表

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

# 安全评分扣分项

安全评分扣分项及其分值情况如表3-3所示。

#### 表 3-3 安全评分扣分项

分类	扣分项	单项扣 分项	处理建议	最高扣分 上限
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	20
	存在未处理的高危不合 规项	5	里新融友扫描任务,自动   刷新评分。 	
	存在未处理的中危不合 规项	2		

分类	扣分项	单项扣 分项	处理建议	最高扣分 上限
	存在未处理的低危不合 规项	0.1		
漏洞	存在未处理的致命漏洞	10	按照漏洞修复建议指导进	20
	存在未处理的高危漏洞	5	行漏洞修复,修复后里新   触发漏洞扫描任务,自动	
	存在未处理的中危漏洞	2	刷新评分。	
	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	30
	存在未处理的高危告警 事件	5	がりあり レモ ノフ 。	
	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		



态势感知提供资源管理功能。在"资源管理"页面,您可以查看当前账号中所有资源 的安全状态统计信息,包括资源的名称、所属服务、所属区域、安全状况等,帮助您 快速定位安全风险问题并提供解决方案。

目前,支持查看以下资源的安全状况:

弹性云服务器 ECS、虚拟私有云 VPC、对象存储服务 OBS、弹性公网IP EIP、云解析 服务 DNS、弹性负载均衡 ELB、云数据库 RDS、裸金属服务器 BMS、云容器引擎 CCE、云容器实例 CCI、Web应用防火墙 WAF、SSL证书管理 SCM、云硬盘 EVS

前提条件

- 已购买态势感知标准版或专业版,且在有效使用期内。
- 操作账号权限检查。使用资源管理功能时,除了需要"SA FullAccess"、"SA ReadOnlyAccess"策略权限,还需要"Tenant Administrator"权限,请提前授 予操作账号对应权限。

"Tenant Administrator"权限配置详细操作请参见如何配置资源管理功能所需的权限。

## 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"资源管理",进入资源管理页面。
- 步骤4 查看全部资源安全状态,相关说明如表4-1所示。

#### **图 4-1** 资源管理

资源管理						
服务	全部 (0)	弹性云服务器 ECS (0)	虚拟私有云 VPC (0)	对象存储服务 OBS (0)	弹性公网IP EIP (0)	
	云解析服务 DNS (0)	弹性负载均衡 ELB (0)	云数据库 RDS (0)	裸金屬服务器 BMS (0)	云容飜引擎 CCE (0)	
	云容器实例 CCI (0)	Web应用防火塘 WAF (0)	SSL证书管理 SCM (0)	云硬盘 EVS (0)		
区域	全部 (0)	非北北京 (0)	<b>华北-北京四 (0)</b>	华东-上海一 (0)	华东-上海二 (0)	
	华南-广州 (0)	华南·深圳 (0)	西南-婁阳— (0)	中国-香港 (0)		
安全状况	全部 (0) 🚺 数命	3 (0) 🚺 高性 (0) 🚺	中危 (0)	<ul> <li>揭示(0)</li> <li>无风险(</li> </ul>	(0)	
					弹性公网IP · 请输入	兴健学 Q C
名称 ↓Ξ	服务 ↓Ξ 区的	· □ □ 型类驱液 = 1 割	全状況 ▽ 1三 1P地址 1三	防护状态 🏹 📖	6 JE 86 JE 호 JE 6	2业项目 ↓Ξ 标签
tes 2	弹性云服务器 ECS cr	n-north-7 云服务器	] 低微	◎ 开启 0	0 2 0	default {"CCE-Dyn
te: 8	弹性云服务器 ECS cr	n-north-7 云服务酬	] 任徳	• 开启 0	0 1 0	default {"CCE-Dyn

# 表 4-1 资源安全状态参数说明

参数名称	参数说明
名称	呈现资源的名称。
服务	呈现资源所属的服务。
区域	呈现资源所属的区域。
资源类型	呈现资源所属的类型。例如:云服务器、磁盘、实例等。
安全状况	<ul> <li>呈现资源的安全风险等级。</li> <li>风险等级包括"致命"、"高危"、"中危"、"低危"、"提示"和"无风险"。</li> <li>呈现当前资源风险的最高等级。例如,ECS中有高危、低危和提示级别的风险,则此处取最高值,显示为高危。</li> </ul>
	● 甲击1=, 可按风险等级排序资源列表。
IP地址	呈现资源的IP地址。
防护状态	呈现资源是否开启安全防护。如果未开启防护,可单击 "去开启"进行设置。
威胁	呈现资源 <b>近7天内</b> 存在的威胁告警总数。 单击告警数量可跳转"检测结果"页面,查看更多的威胁 告警信息,并可自定义过滤条件查询告警信息。
漏洞	呈现资源 <b>近24小时内</b> 未修复的漏洞总数。
	<ul> <li>单击漏洞数量可跳转"检测结果"页面,查看更多的漏洞信息,并可自定义过滤条件查询漏洞信息。</li> <li>"资源管理"页面中显示的数据为最近/最新检测后的数据结果,"检测结果"页面显示的是所有检测时间的各类数据详情,因此,资源管理页面的数据总数≤检测结果页面的数据总数。</li> </ul>
基线	呈现资源 <b>近30天内</b> 存在的基线风险总数。
	<ul> <li>单击基线检查异常数量可跳转"检测结果"页面,查 看更多的基线异常信息,并可自定义过滤条件查询基 线检查信息。</li> <li>"资源管理"页面中显示的数据为最近/最新检测后的 数据结果,"检测结果"页面显示的是所有检测时间 的各类数据详情,因此,资源管理页面的数据总数&lt;检</li> </ul>
	测结果页面的数据总数。
企业项目	呈现资源所属的企业项目。
标签	呈现资源已有的标签。 如果资源当天添加了标签,则在SA资源管理中第二天才 会同步显示。

步骤5 根据资源信息,筛选查看相关资源安全状态。

单击"服务"、"区域"或"安全状况"后的选项,将呈现符合过滤条件的资源列 表。

- **服务**: 筛选资源所属的服务。选择服务后,还可以根据"资源类型"来查看选择 指定资源类型的安全状态。
- 区域:筛选资源所在的区域。
   可选择区域包括"华北-北京一"、"华北-北京四"、"华东-上海一"、"华东-上海二"、"华南-深圳"、"华南-广州"、"西南-贵阳一"或"中国-香港"。
- 安全状况: 筛选资源的安全风险等级。
   可选择风险等级包括"致命"、"高危"、"中危"、"低危"、"提示"或 "无风险"。
- 步骤6 当资源列表较多时,可以通过搜索功能,快速查询指定资源。

在搜索框中输入资源的"弹性公网IP"、"名称"或"私有IP",单击 Q,即可查 看目标资源的安全状态。

----结束



态势感知提供安全业务的专项分析能力,实时为您全面展示云上资产的安全状态和存在的安全风险,并联动其他云安全服务,集中展示云上安全。

## 背景信息

● HSS专项分析

主机安全服务(Host Security Service, HSS)是以工作负载为中心的安全产品, 集成了主机安全、容器安全和网页防篡改,旨在解决混合云、多云数据中心基础 架构中服务器工作负载的独特保护要求。HSS通过对主机、容器进行系统完整性 的保护、应用程序控制、行为监控和基于主机的入侵防御等,保护工作负载免受 攻击。

在SA中的HSS业务分析页面,您可以查看您所有资产的风险指数、风险趋势、 TOP5事件类型以及您开通的主机安全和容器安全服务数量,帮助您实时了解主机 和容器的安全状态和存在的安全风险。

#### WAF专项分析

Web应用防火墙(Web Application Firewall, WAF)对网站业务流量进行多维 度检测和防护,结合深度机器学习智能识别恶意请求特征和防御未知威胁,全面 避免网站被黑客恶意攻击和入侵。

在SA中的WAF业务分析页面,您可以查看昨天、今天、3天、7天或者30天内所有 防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类 型统计次数,QPS、响应码信息,以及事件分布、受攻击域名 Top10、攻击源IP Top10、受攻击URL Top10、攻击来源区域 Top10和业务异常监控 Top10等防护 数据。

安全总览页面统计数据每隔2分钟刷新一次。

DBSS专项分析

数据库安全服务(Database Security Service)是一个智能的数据库安全服务,基于机器学习机制和大数据分析技术,提供数据库审计,SQL注入攻击检测,风险操作识别等功能,保障云上数据库的安全。

在SA中的DBSS业务分析页面,您可以查看最近30分钟、最近1小时、最近24小 时、7天或者30天内数据库的总体审计情况、风险分布、会话统计以及SQL分布情 况。

### 前提条件

已开通对应区域的对应服务。例如,需要查看"华北-北京四"区域中云主机的分析情况,则需要在"华北-北京四"区域开通企业主机安全服务。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 根据待分析选择对应的服务。
  - HSS专项分析
     在左侧导航栏选择"业务分析 > HSS专项分析",进入"HSS专项分析"页面。

图 5-1 HSS 专项分析

志势感知(安全云脑)	业务分析			0	) ## 0 2536 (****	弁服
安全概况	· 清洁将区地企业项目 (					289.8-
1000年	云负赖总能					
HSSߠ	风脸细致	11:10.0510		容额防护		
D855975915		Elteren	来就护主机	Elterter	*8997#	
综合大算	40	2 18	○ 台 开展的1户	U r	U 个 开始的90	
资源管理	中台 以前分离 重新法律					
成物乐智	2023/01/06 15:04:59					
展明然現	GMT+00.00					
観点に立作						

WAF专项分析

在左侧导航栏选择"业务分析 > WAF专项分析",进入"WAF专项分析"页面。

#### 图 5-2 WAF 专项分析



DBSS专项分析

在左侧导航栏选择"业务分析 > DBSS专项分析",进入"DBSS专项分析"页面。

图 5-3 DBSS 专项分析

态势感知	业务分析
安全概况	法选择区域 操作北原因 *
资源管理 业务分析 ▲	1 当約回城福朱开通数編年設金編為, 遠开通信使用
Lussemore	
HODIENCON	数据库安全服务 DBSS
WAF专项分析	数据更安全报号(Database Security Service)是一个智能的数据用安全报答,基于印刷学习印刷用大数据分析技术,提供数据单审计,SQL注入攻击性测,风险媒作识别等功能,保障云上数据单约安全,
DBSS专项分析	與来 7個更多
综合大屏	

步骤4 查看分析情况。

HSS安全总览

在SA中的HSS业务分析页面,您可以查看您所有资产的风险指数、风险趋势、 TOP5事件类型以及您开通的主机安全和容器安全服务数量,帮助您实时了解主机 和容器的安全状态和存在的安全风险。

具体分析情况请参见HSS业务分析。

WAF安全总览

在SA中的WAF业务分析页面,您可以查看昨天、今天、3天、7天或者30天内所有 防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类 型统计次数,QPS、响应码信息,以及事件分布、受攻击域名 Top10、攻击源IP Top10、受攻击URL Top10、攻击来源区域 Top10和业务异常监控 Top10等防护 数据。

具体分析情况请参见WAF业务分析。

DBSS安全总览

在SA中的DBSS业务分析页面,您可以查看最近30分钟、最近1小时、最近24小时、7天或者30天内数据库的总体审计情况、风险分布、会话统计以及SQL分布情况。

具体分析情况请参见DBSS业务分析。

----结束



# 6.1 综合态势感知

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

# 前提条件

已开通安全大屏增值项,可查看综合态势感知大屏相关信息。

## 操作步骤

步骤1 登录管理控制台。

- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"综合大屏",进入"综合大屏"页面。

#### 图 6-1 查看综合大屏信息



**步骤4**单击"综合态势感知"图片,进入"综合态势感知"大屏信息页面,如图6-2。 页面中各个模块的功能介绍和使用方法详见下述内容。

#### 图 6-2 综合态势感知大屏



----结束

# 全网安全地图

如图6-3所示,全网安全地图以区域维度动态展示了客户所有资产近7天内受到的威胁 情况。通过将攻击源和攻击目标具象化,用户可以直观了解资产的安全状况。图中每 个圆圈代表一个华为云区域,每个华为云区域发生的告警来源通过攻击线在地图上表 示出来,最多显示20条告警。

#### 🛄 说明

- "综合态势感知"大屏全网安全示意地图,根据华为云部署区域概略展示,背景地图不能做高精确定位。
- "综合态势感知"大屏全网安全示意地图,仅用于演示与汇报,不是为了任何非法目的,也 不具有任何恶意。



图 6-3 全网安全地图

# 全网威胁度

如<mark>图6-4</mark>所示,全网威胁度体现了**近7天内**资产的整体安全状况。图中体现的信息主要 有威胁度、威胁总量和受威胁资产数。

其中,威胁度的取值范围是0~100,数值越大表示威胁越高。由于不包含无风险的资产,所以受威胁资产数小于等于总资产数。

**图 6-4** 全网威胁度



# 威胁事件趋势

如<mark>图6-5</mark>所示,展示**近7天内**每日所受威胁的数量,威胁事件趋势的横坐标表示时间, 纵坐标表示威胁事件的数量。将鼠标箭头置于某个日期上,可以看到该日发生的威胁 事件总数。

图 6-5 威胁事件趋势



# 威胁类型分布

如<mark>图6-6</mark>所示,威胁类型分布体现了**近7天内**受到威胁的类型及不同威胁类型所占的比例。





## 受威胁资产数量趋势

如<mark>图6-7</mark>所示,展示**近7天内**每日受到威胁的资产的数量,受威胁资产数量趋势的横坐 标表示时间,纵坐标表示受威胁资产的数量。将鼠标箭头置于某个日期上,可以看到 该日受威胁的资产总数。

图 6-7 受威胁资产数量趋势



# 今日威胁雷达图

如图6-8所示,今日威胁雷达图体现了今天发现的威胁数量。

#### 图 6-8 今日威胁雷达图



# 威胁源主机 TOP5

如<mark>图6-9</mark>所示,威胁源主机TOP5展示了**近7天内**产生威胁数最多的前5台主机的相关信息,包括主机的IP地址、所属国家/地区和攻击次数,并按照威胁数量从高到低的次序 进行排列。

图 6-9 威胁源主机 TOP5



# 受攻击资产区域分布

如<mark>图6-10</mark>所示,受攻击资产区域分布以区域为维度,体现了**近7天内**受攻击资产的比例。

#### 图 6-10 受攻击资产区域分布



# 6.2 主机安全态势

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

## 前提条件

已开通安全大屏增值项,可查看综合态势感知大屏相关信息。

## 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。 **步骤3** 在左侧导航栏选择 "综合大屏",进入 "综合大屏"页面。

## 图 6-11 查看综合大屏信息

安全低范 決定管理 立労分析 学会大部 高防容 展防理 基計合容 基計合容 基計合容 基合社室		计费模式	按索 🗂 转	包周期	取消按需
基後检查					
HF日10351874	主机安金态粉				

**步骤4** 单击"主机安全态势"图片,进入"华为云主机安全态势"信息页面,如<mark>图6-12</mark>。 界面中各个模块的功能介绍和使用方法详见下述内容。

## 图 6-12 主机安全态势大屏



----结束

# 风险主机地图

区域维度风险主机直观展示了**当天**不同华为云区域内是否有风险主机。没有风险主机 的区域,指示灯为绿色,有威胁主机的区域,指示灯为红色。当用鼠标单击亮灯的区 域时,则分别显示出该区域的主机总数、Windows系统主机台数、Linux系统主机台数 和该区域的风险主机台数。通过将风险主机具象化,用户可以直观的了解资产的安全 状况。

#### 🗀 说明

- "华为云主机安全态势"大屏风险主机示意地图,根据华为云部署区域概略展示,背景地图 不能做高精确定位。
- "华为云主机安全态势"大屏风险主机示意地图,仅用于演示与汇报,不是为了任何非法目的,也不具有任何恶意。

# 主机安全事件统计

如**图6-13**所示,主机安全事件详情展示了**当天**威胁主机安全的5种告警类型,分别是暴力破解、异地登录、恶意程序、网站后门、文件变更。一个环形图表示一种类型,每个环形图中间的数字表示当天此种威胁出现的次数。环形图下方的风险主机台数体现了当天遭受此种威胁的主机数,亮蓝色的环形占总环形的比例表示风险主机占总资产的比例,以暴力破解环形图为例,当天一共有2台主机遭受了1次暴力破解。

#### 图 6-13 主机安全事件详情



# 资产统计

如<mark>图6-14</mark>所示,资产统计展示了总资产的数量和类型,两类主机分为Windows系统主 机和Linux系统主机。中间的条形图直观显示了这两种主机占总资产的比例,下方则显 示了这两种主机的具体数量。





# 近7天风险主机趋势

如<mark>图6-15</mark>所示,风险主机趋势的横坐标表示具体日期,纵坐标表示风险主机数量。从 图中可看到**近7天内**每天的风险主机数量和风险主机趋势。



**图 6-15** 风险主机趋势

# TOP5 风险云主机

如<mark>图6-16</mark>所示,TOP5风险云主机按照安全风险等级由高到低展示了**当天**受威胁主机的 相关信息,包括主机名称、主机系统及受到的攻击程度。TOP5风险云主机最多展示5 条。安全风险等级由高到低分别是致命、高危、中危、低危和提示。 **图 6-16** 风险云主机



# 近7天暴力破解趋势

如<mark>图6-17</mark>所示,近7天暴力破解攻击趋势展示了**近7天内**每天的暴力破解次数,横坐标 表示时间,纵坐标表示暴力破解的次数。将鼠标悬停于某日期范围内,可以看到该日 暴力破解的次数。

图 6-17 近 7 天暴力破解攻击趋势



漏洞检测

如<mark>图6-18</mark>所示,漏洞检测的环形图展示了**当天**检测出的Window漏洞与Linux漏洞的比例。环形图下方显示两种漏洞的个数,右上角显示了检测出漏洞的风险主机的台数。

#### 图 6-18 漏洞检测



## 基线检测

如<mark>图6-19</mark>所示,您可以通过主机基线模块查看口令复杂度和配置检测这两方面的风险 及个数。

## 图 6-19 基线检测



# 暴力破解类型

如<mark>图6-20</mark>所示,暴力破解类型展示了**当天**暴力破解的类型及每种类型的攻击次数。暴力破解一共有5种类型,分别是SSH暴力破解、RDP暴力破解、WEB暴力破解、MsSQL暴力破解、SQLServer暴力破解。右上角展示了当天受到暴力破解威胁的全部风险主机的台数。

#### **图 6-20** 暴力破解类型





# 7.1 威胁告警简介

## 背景信息

态势感知威胁告警功能汇集了华为云多个安全服务的告警能力,按照告警类型和等级 统一维度呈现,可以准确实时监控云上威胁攻击、检测您资产中的安全告警事件。

同时,通过威胁分析,从攻击源和受攻击资产两个维度,帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

态势感知威胁告警支持以下功能项:

#### • 告警列表

通过"实时监控"云上威胁告警事件,并接入AntiDDos、HSS、WAF等服务上报 的告警事件,提供告警通知和监控,记录近180天告警事件详情。

• 威胁分析

从"攻击源"或"被攻击资产"查询威胁攻击,统计威胁攻击次数或资产被攻击 次数。

• 告警通知

自定义威胁告警通知,设置每日定时告警通知和实时告警通知,通过接收消息通 知及时了解威胁风险。

● 告警监控

自定义监控的威胁名单、告警类型、告警级别等,选择性呈现关注的威胁告警。

## 告警类型

目前SA支持检测8类威胁告警事件,共包括200+种子告警类型。

#### 🛄 说明

SA**基础版**支持检测部分威胁攻击事件。为全面快速地了解并处理资产遭受的威胁,确保云上资 产安全,建议您购买标准版或专业版。

## DDoS 事件

"实时检测"华为云、非华为云及IDC的互联网主机的DDoS攻击。

共支持检测100+种子类型的DDoS威胁。

- 网络层攻击 NTP Flood攻击、CC攻击等。
- 传输层攻击
   SYN Flood攻击、ACK Flood攻击等。
- 会话层攻击
   SSL连接攻击等。
- 应用层攻击
   HTTP Get Flood攻击、HTTP Post Flood攻击等。

## 暴力破解事件

"实时检测"入侵资产的行为和主机资产内部的风险,检测SSH、RDP、FTP、SQL Server、MySQL等账户是否遭受的口令破解攻击,以及检测资产账户是否被破解异常 登录。

共支持检测22种子类型的暴力破解威胁。

- 支持检测的暴力破解威胁
   包括SSH暴力破解(2种)、RDP暴力破解、MSSQL暴力破解、MySQL暴力破 解、FTP暴力破解、SMB暴力破解(3种)、HTTP暴力破解(4种)、Telnet暴力 破解。
- 接入的HSS服务上报的告警事件
   包括SSH暴力破解、RDP暴力破解、FTP暴力破解、MySQL暴力破解、IRC暴力破 解、Webmin暴力破解、其他端口被暴力破解、系统被成功爆破事件。

## Web 攻击事件

"实时检测"Web恶意扫描器、IP、网马等威胁。

共支持检测38种子类型的Web攻击威胁。

- 支持检测的Web攻击威胁
   包括Webshell攻击(3种)、跨站脚本攻击、代码注入攻击(7种)、SQL注入攻击(9种)、命令注入攻击。
- 接入的HSS服务上报的告警事件
   包括Webshell攻击、Linux网页篡改、Windows网页篡改。
- 接入的WAF服务上报的告警事件
   包括跨站脚本攻击、命令注入攻击、SQL注入攻击、目录遍历攻击、本地文件包含、远程文件包含、远程代码执行、网站后门、网站信息泄露、漏洞攻击、IP信
   誉库、恶意爬虫、网页防篡改、网页防爬虫。

后门木马事件

"实时检测"资产系统是否存在后门木马风险,以及被后门木马程序入侵后的恶意请求行为。

文档版本 54 (2022-11-24)

共支持检测5种子类型的后门木马威胁。

- 检测主机资产上Web目录中的PHP、JSP等后门木马文件类型。
- 检测资产被植入木马特性

检测内容包括资产系统存在win32/ramnit checkin木马、被入侵后执行wannacry 勒索病毒相关的DNS解析请求、被入侵后尝试下载木马程序,被入侵后访问HFS 下载服务器等。

# 僵尸主机事件

"实时检测"资产被入侵后对外发起攻击的威胁。共支持检测7种子类型的僵尸主机威胁。

- 对外发起SSH暴力破解
- 对外发起RDP暴力破解
- 对外发起Web暴力破解
- 对外发起MySQL暴力破解
- 对外发起SQLServer暴力破解
- 对外发起DDoS攻击
- 被入侵后安装挖矿程序

## 异常行为事件

"实时检测"资产系统异常变更和操作行为。共支持检测21种子类型的异常行为威胁。

共支持检测21种子类型的异常行为威胁。

- 支持检测的异常行为威胁
   包括文件系统被扫描、CMS V1.0漏洞、敏感文件被访问。
- 接入的HSS服务上报的告警事件

包括系统成功登录审计事件、文件目录变更监测事件、混杂模式网卡、异常权限 用户、反弹Shell、异常Shell、高危命令执行、异常自启动、文件提权、进程提 权、Rootkit程序。

- 接入的WAF服务上报的告警事件
   包括自定义规则、白名单、黑名单、地理访问控制、扫描器爬虫、IP黑白名单、 非法访问。
- 接入的MTD服务上报的告警事件
   包括暴力破解、恶意攻击、渗透、挖矿攻击等恶意活动和未经授权行为。

## 漏洞攻击事件

"实时检测"资产被尝试使用漏洞进行攻击。共支持检测2种子类型的漏洞攻击威胁。

- SMBv1漏洞攻击
- WebCMS漏洞攻击

# 命令控制事件

"实时检测"资产可能被命令与控制服务器(C&C,Command and Control Server)远程控制,访问与恶意软件或建立与恶意软件之间的链接。

共支持检测3种子类型的命令控制威胁。

- 监控主机存在访问DGA域名行为
- 监控主机存在访问恶意C&C域名行为
- 监控主机存在恶意C&C通道行为

# 7.2 查看告警列表

通过查看"告警列表",您可以了解近180天的告警威胁的统计信息列表,列表内容包 括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件,如告警名 称、告警等级和发生时间等,快速查询到相应告警事件的统计信息。

此外,您还可以通过及时处理告警事件,标记告警事件处理状态,并支持一键导出近 180天的告警事件。

# 约束限制

- 仅标准版和专业版支持忽略和标记告警事件,基础版不支持。
- 仅支持导出近180天的全部告警事件,暂不支持筛选导出告警事件信息。
- 按过滤场景筛选告警,最多可呈现10000条告警。

## 查看告警详情

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- **步骤3** 在态势感知管理页面选择"威胁告警 > 告警列表",进入态势感知告警列表管理页面。

#### 图 7-1 查看告警列表信息

志势想知	威胁告誓							I	TO BOOK
安全规范	0								
资源管理	告誓列表 成語分析								
11月分析 •	法要求称 全部 DDoS 暴	の破解 Web改善 県门木马	演奏の本 優戸主机 命やさ	控制 异核行为					
综合大算									
10000 (D	NAME TO O THE	2121 0 214 0 214 0	0 107						
湖市管理	15回秋志 <b>全部 未注理</b> E	日初編 日城下处理							
<b>基地位置</b>	2019月 今天 昨天 近1	庆 近7天 近10天 近年4	F						
检测结果									
分析服装	忽略 标记为线下处理	导出全部改藝						资产P · 请输入关键字进行检索	QC
日志管理	() 執管各称	1978 1978 1978	来源(闽家/地区)	主机D	367*1P (38111P)	秋生时间 17	\$62 ()	操作	
安全产品集成	□ 算單行为	Container Escape 0 中燈		d51159aa6093a6	10 · · ·	2022-10-27717:02:32.013+08:00	未经理	忽略 目标记为成下处理	
	■ 単規行为	Container Escape 0 中間		d51159aa6093a6	n	2022-10-27117:01:53:222+08:00	#15 <b>8</b>	忽略   杨迅大战下处理	
1182 ·	□ 异年行为	Abnormal Contain 0 提示		d51159aa6093a6	10	2022-10-27716:34:04:184+08:00	未经理	888   \$FE238FE43	
0.452 03072 *	□ 异年行为	Container Escape 0 中意		544a2591c0540ec	11 0	2022-10-27716:32:51.939+08:00	未经理	898 · 标记为线下处理	
7±22	□ 异株行为	Abnormal Contain 0 提示		19dfcea5b15432b	0	2022-10-27716:31:30.857+08:00	未达理	忽略   标记为线下处理	
	日 异年行为	Abnormal Contain 0 提示		687233722fc1170	n	2022-10-27716:31:30.857+08:00	未处理	8948   16123-0617-02-88	
	日 异年行为	Abnormal Contain 0 提示		79265f713cc0e54	n	2022-10-27716:31:30.750+08:00	未处理	1946   1912月19日下位日間	
	□ 异爆行为	Abnormal Contain 0 證示		5f19149ca4599d8	n	2022-10-27716:31:30.741+08:00	未经理	\$P\$ 1625357338	
	□ 异年行为	Abnormal Contain 0 提示		3c37ao4ed7a0228	n	2022-10-27716:31:30.736+08:00	未处理	844 HRIENHETHE	
	日 异年行为	Abnormal Contain 0 提示		90e08c0ca71d9fa	n	2022-10-27716:31:30.730+08:00	未处理	1946   47423-0477-048	
	10 · (3)8580: 10,000 ( 1	1 2 3 4 5 1000 ;							

**步骤4** 筛选"告警名称"、"告警等级"、"发生时间"和"处理状态"条件选项,在列表 栏查看显示符合过滤条件的告警事件列表。

- 告警名称:告警事件所属的分类。
- 告警等级:告警事件对应的等级,包括"致命"、"高危"、"中危"、"低危"、"提示"。
- 处理状态:用户对告警事件的处理标记,可选择"未处理"、"已忽略"、"已 线下处理"。
- 发生时间:告警事件发生的时间范围,可选择"今天"、"昨天"、"近3天"、 "近7天"、"近30天"和"近半年"。

步骤5 当过滤后的告警事件较多时,可以利用搜索功能快速找到指定告警事件。

在下拉框中选择"资产IP"、"来源IP"、"主机ID",在搜索框中输入相应IP或ID, 单击<sup>Q</sup>,即可查看到指定资产相关的告警信息。

步骤6 查看告警事件详情。

单击列表中告警的"告警名称",右侧滑出告警详情窗口,可查看与该告警相关的 "基本信息"、"数据来源"、"攻击信息"、受影响的用户等信息,以及该告警的 处理状态。

----结束

#### 标记告警事件

当SA检测出告警事件后,您可手动标记已处理的告警事件。

- 步骤1 在"告警列表"页面,标记告警事件的处理状态。
  - 忽略:如果确认该告警事件不会造成危害,可标记为"已忽略"状态。
  - 标记为线下处理:如果该告警事件已在线下处理,在"标记为线下处理"窗口记录"处理人"、"处理时间"和"处理结果",可标记为"已线下处理"状态。
- 步骤2 批量标记告警事件。

选择一个或多个"未处理"状态的告警,单击"忽略"或"标记为线下处理",对不同告警事件批量执行相应的处理操作。

步骤3 单个标记告警事件。

在告警列表对应"操作"列,单击"忽略"或"标记为线下处理",对单个告警事件 执行相应处理操作。

步骤4 取消告警事件标记。

告警处理状态标记后,可在告警事件对应"操作"列,单击"取消忽略"或"取消标记",恢复告警"未处理"状态,再修改告警状态。

----结束

# 导出告警事件

在"告警列表"页面,单击"导出全部告警",一键导出列表中全部告警事件,并以 excel文件形式保存在本地。导出完成后,即可离线查看告警事件列表。

文档版本 54 (2022-11-24)

#### 图 7-2 导出告警事件

态势感知	成約告答 ② +业版: 型加充制
安全概范	
资源管理	<u>告警列表</u> 威胁分析
业务分析 ▼	音音音称 金金 DO-G 最近破解 Web攻击 価戸主机 异常行为 形態软件
综合大屏	
威胁告誓	
漏洞管理	处理状态 全部 未处理 已錄時 已续下处理
基线检查	发生时间 今天 路天 近3天 近30天 近半年
检测结果	
分析报告	御略
日志管理	□ 告告名称 告告类型 告告等级 来逝(周_ 主机D 资产IP_ 发生时间 F 状态 操作
安全产品集成	□ 展力機解 SSH Br 0 中危 1 - 8332283 1: 2021-12-20T18:15:29.377+08:00 未处理 忽略 标记为终下处理
· (2프 -	
网络安全 🔻	Web攻击 XSS 0 中危 一 556a09 12 _ 2021-11-25T16:33:05:409+08:00 未处理 忽略 标记为线下处理

导出的excel文件中包含"事件标识"、"受影响资源"、"严重等级"和"发现时间"等信息。

#### 🛄 说明

目前仅支持导出近180天的全部告警事件。

# 7.3 威胁分析

当告警列表中积累了较多威胁告警信息时,您可以使用"威胁分析"功能,从"攻击 源"或"被攻击资产"的维度分析网络攻击情况。

## 前提条件

已购买态势感知标准版或专业版,且在有效使用期内。

## 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- **步骤3** 在态势感知管理页面选择"威胁告警 > 威胁分析",进入态势感知威胁分析管理页面。
- **步骤4** 在下拉框中选择条件"攻击源"或"被攻击资产"、"发生时间",并输入待查询的 IP地址,单击"开始分析"。

#### 🛄 说明

发生时间可选择"今天"、"昨天"、"近3天"、"近7天"、"近30天"、"近半年"。

**步骤5** 在列表栏查看符合过滤条件的威胁信息,可以直观看到该攻击源对哪些资产发起了何 种类型的攻击,或被攻击资产遭到了哪些攻击。

----结束

# 7.4 告警事件处理

文档版本 54 (2022-11-24)

# 7.4.1 DDoS

## 告警类型说明

分布式拒绝服务(Distributed Denial of Service,简称DDoS)攻击是指攻击者使用网 络上多个被攻陷的电脑作为攻击机器,向特定的目标发动DoS攻击。DoS(Denial of Service)攻击也称洪水攻击,是一种网络攻击手法,其目的在于使目标电脑的网络或 系统资源耗尽,服务暂时中断或停止,导致合法用户不能够访问正常网络服务的行 为。

DDoS威胁父类型约有100多种子类型,态势感知基础版、标准版和专业版支持全部 DDoS的子类型威胁告警。

## 处理建议

当检测到应用系统受到DDoS类威胁时,代表应用系统受到DDoS类攻击,属于"提示"告警级别威胁,建议用户直接购买DDoS高防服务防护。

# 7.4.2 暴力破解

## 告警类型说明

暴力破解法(BruteForce)是一种密码分析方法,基本原理是在一定条件范围内对所 有可能结果进行逐一验证,直到找出符合条件的结果为止。攻击者通常使用暴力破解 的方式猜测远程登录的用户名和密码,一旦破解成功,即可实施攻击和控制。

态势感知支持检测22种子类型的暴力破解威胁,基础版不支持检测暴力破解类威胁, 标准版支持检测8种子类型威胁,专业版支持检测全部子类型威胁(其中有8种类型需 要购买<mark>主机安全服务</mark>)。

## 处理建议

当检测到暴力破解类威胁时,各子类型威胁处理建议参见<mark>表7-1</mark>。

#### 表 7-1 部分暴力破解类威胁处理建议

威胁告警 名称	告警 等级	威胁说明	处理建议
SSH暴力 破解	中危	检测到ECS实例被不 断尝试SSH登录,代 表有攻击者正在尝试 对ECS实例做SSH暴 力破解攻击尝试。	攻击发生主要原因是SSH端口开放到公 网,因此建议按照如下方式处理: 1. 在安全组设置中限制外部SSH访问; 2. 在ECS操作系统中配置hosts.deny。
RDP暴力 破解	中危	检测到ECS实例被不 断尝试RDP登录,代 表有攻击者正在尝试 对ECS实例做RDP暴 力破解攻击尝试。	攻击发生的主要原因是RDP端口开放到 公网,因此建议按照如下方式处理: 1. 在安全组设置中限制外部RDP访问; 2. 在ECS操作系统中配置远程桌面访问 控制,如配置Windows防火墙等。

威胁告警 名称	告警 等级	威胁说明	处理建议
Web暴力 破解	中危	检测到Web服务 (如登录页面等)被 不断尝试登录,代表 有攻击者正在尝试对 Web应用登录页面 等做暴力破解攻击尝 试。	攻击发生的主要原因是将应用的后台管 理页面(如phpMyAdmin、tomcat管理 页面等)开放到公网;需要开放到公网 访问的业务,登录页面未做登录校验。 因此建议按照如下方式处理: 1.在安全组设置中限制外部访问后台管 理系统页面; 2.在Web应用中设置防爆破逻辑,如设 置登录短信验证码、图片验证码等;
MySQL 爆破	中危	检测到ECS实例上的 MySQL被不断尝试 登录,代表有攻击者 正在尝试对ECS实例 做MySQL暴力破解 攻击尝试。	攻击发生的主要原因是MySQL服务端口 开放到公网,因此建议按照如下方式处 理: 1. 在安全组中限制外部访问MySQL实 例; 2. 配置OS上的防火墙策略,限制外部访 问; 3. 解除安装MySQL实例的ECS与EIP的绑 定关系。
MS SQL 爆破	中危	检测到ECS实例上的 MS SQLServer被不 断尝试登录,代表有 攻击者正在尝试对 ECS实例做MS SQLServer暴力破解 攻击尝试。	攻击发生的主要原因是MS SQLServer服 务端口开放到公网,因此建议按照如下 方式处理: 1. 在安全组设置中限制外部访问MS SQLServer实例; 2. 配置OS上的防火墙策略,限制外部访 问; 3. 解除安装MS SQLServer实例的ECS与 EIP的绑定关系。
系统爆破 检测事件	中危	检测到ECS实例被暴 力破解攻击,不断被 尝试登录。	建议登录企业主机安全管理控制台处 理。
非法系统 账户	中危	检测到ECS实例被暴 力破解攻击,不断被 非法系统账户尝试登 录。	建议登录企业主机安全管理控制台处 理。
系统被成 功爆破事 件	高危	检测到用户ECS实例 被爆破成功。	建议登录企业主机安全管理控制台处 理。

# 7.4.3 Web 攻击

## 告警类型说明

Web攻击(WebAttack)是针对用户上网行为或网站服务器等设备进行攻击的行为。 常见的Web攻击方式包括SQL注入攻击、跨站脚本攻击、跨站请求伪造攻击等。

态势感知支持检测38种子类型的Web攻击威胁,基础版不支持检测Web攻击类威胁,标准版支持检测19种子类型威胁,专业版支持检测全部子类型威胁(其中有14种类型需要购买Web应用防火墙服务,3种类型需购买主机安全服务)。

## 处理建议

当检测到Web攻击类威胁时,代表有攻击者正在尝试对Web应用漏洞做攻击尝试,属于"中危"及以下告警级别威胁。因此建议按照如下方式处理:

- 1. 检查Web应用逻辑是否有相应漏洞;
- 2. 购买Web应用防火墙服务防护。

# 7.4.4 后门木马

## 告警类型说明

后门木马又称特洛伊木马(Trojan Horse),是一种后门程序。后门木马具有很高的伪装性,通常表现为一个正常的应用程序或文件,以获得广泛的传播和目标用户的信任。当目标用户执行后门木马程序后,攻击者即可对用户的主机进行破坏或盗取敏感数据,如各种账户、密码、保密文件等。在黑客进行的各种攻击行为中,后门木马基本上都起到了先导作用,为进一步的攻击打下基础。

态势感知支持检测5种子类型的后门木马威胁,基础版不支持检测后门木马类威胁,标 准版支持检测1种子类型威胁,专业版支持检测全部子类型威胁。

#### 处理建议

当检测到后门木马类威胁时,ECS实例存在木马程序网络请求,代表ECS实例已经存在 被植入木马的特征,如尝试做wannacry勒索病毒相关DNS解析请求、尝试下载exe类 木马程序等,属于"高危"告警级别威胁。因此建议按照如下方式处理:

- 1. 关闭被攻击ECS实例;
- 2. 检查实例所在子网的其他主机是否被入侵;
- 3. 购买企业主机安全服务防护。

# 7.4.5 漏洞攻击

#### 告警类型说明

漏洞是指计算机系统安全方面的缺陷,可导致系统或应用数据遭受保密性、完整性、可用性等方面的威胁。攻击者利用漏洞获取计算机权限、盗取敏感数据、破坏软硬件 系统等行为均可称为漏洞攻击。

态势感知支持检测2种子类型的漏洞攻击威胁,基础版不支持检测漏洞攻击类威胁,标 准版不支持检测漏洞攻击,专业版支持检测全部子类型威胁。

## 处理建议

当检测到漏洞攻击类威胁时,各子类型威胁处理建议参见<mark>表7-2</mark>。

威胁告警 名称	告警 等级	威胁说明	处理建议
MySQL 漏洞攻击	低危	检测到ECS实例被尝 试利用MySQL漏洞 攻击,代表ECS实例 被尝试使用MySQL 漏洞进行攻击。	攻击发生主要原因是ECS实例在公网上开 放了MySQL服务,因此建议按照如下方 式处理: 1. 配置安全组规则,限制MySQL服务公 网访问; 2. 解绑ELB,关闭MySQL服务公网访问 入口。
Redis漏 洞攻击	低危	检测到ECS实例被尝 试利用Redis漏洞攻 击,代表ECS实例被 尝试使用Redis漏洞 进行攻击。	攻击发生主要原因是ECS实例在公网上开 放了Redis服务,因此建议按照如下方式 处理: 1. 配置安全组规则,限制Redis服务公网 访问; 2. 解绑ELB,关闭Redis服务公网访问入 口。

表 7-2 漏洞攻击类威胁处理建议

# 7.4.6 僵尸主机

## 告警类型说明

僵尸主机亦称傀儡机,是由攻击者通过木马蠕虫感染的主机,大量僵尸主机可以组成 僵尸网络(Botnet )。攻击者通过控制信道向僵尸网络内的大量僵尸主机下达指令, 令其发送伪造包或垃圾数据包,使攻击目标瘫痪并"拒绝服务",这就是常见的DDoS 攻击。此外,随着虚拟货币(如比特币)价值的持续增长,以及挖矿成本的逐渐增 高,攻击者也开始利用僵尸主机进行挖矿和牟利。

态势感知支持检测7种子类型的僵尸主机威胁,基础版不支持检测僵尸主机类威胁,标 准版支持检测5种子类型威胁,专业版支持检测全部子类型威胁。

#### 处理建议

当检测到僵尸主机类威胁时,检测到ECS实例存在挖矿特性行为(如访问矿池地址 等)、对外发起DDoS攻击或暴力破解攻击,代表ECS实例可能已经被植入挖矿木马或 后门程序,可能变成僵尸网络,属于"高危"告警级别威胁。因此建议按照如下方式 处理:

- 1. 对ECS实例做病毒木马查杀,查杀失败则关闭该实例;
- 2. 检查实例所在子网的其他主机是否被入侵;
- 3. 购买企业主机安全服务防护。

# 7.4.7 命令与控制

# 告警类型说明

域名生成算法(Domain Generation Algorithm, DGA)是一种利用随机字符生成命 令与控制(Command and Control,C&C)域名的技术,常被用于逃避域名黑名单功 能的检测。攻击者利用DGA产生恶意域名后,选择部分域名进行注册并指向C&C服务 器。当受害者运行恶意程序后,主机将通过恶意域名连接至C&C服务器,攻击者即可 远程操控主机。

态势感知支持检测3种子类型的命令与控制类威胁,基础版和标准版不支持检测命令与控制类威胁,专业版支持检测全部子类型威胁。

#### 处理建议

当检测到命令与控制类威胁时,ECS实例存在访问DGA域名、访问远程C&C服务器或建 立了连接C&C的通道,一种恶意软件访问或连接行为,代表ECS实例可能正在被C&C远 程控制,可能变成僵尸网络,属于"高危"告警级别威胁。因此建议按照如下方式处 理:

- 1. 对ECS实例做病毒木马查杀,查杀失败则关闭该实例;
- 2. 检查实例所在子网的其他主机是否被入侵;
- 3. 购买企业主机安全服务防护。

# 7.4.8 异常行为

#### 告警类型说明

异常行为(Abnormal Behavior)主要指在主机中发生了一些不应当出现的事件。例 如,某用户在非正常时间成功登录了系统,一些文件目录发生了计划外的变更,进程 出现了非正常的行为等。这些异常的行为事件很多是有恶意程序在背后作乱。所以在 发生这类异常行为时,应当引起重视。态势感知中的异常行为数据主要来源于主机安 全服务和Web应用防火墙服务。

态势感知支持检测21种子类型的异常行为威胁,基础版不支持检测异常行为类威胁, 标准版支持检测7种子类型威胁,专业版支持检测全部子类型威胁(其中有7种类型需 要购买Web应用防火墙,11种类型需要购买**主机安全服务**)。

#### 处理建议

当检测到异常行为类威胁时,各子类型威胁处理建议参见<mark>表7-3</mark>。

#### 表 7-3 部分异常行为类威胁处理建议

威胁告警名称	告警 等级	威胁说明	处理建议
文件目录变更	提示	检测到ECS实例的关键文件	建议登录企业主机安全管理
监测事件		被更改。	控制台处理。
系统成功登录	提示	检测到ECS实例已异常成功	建议登录企业主机安全管理
审计事件		登录。	控制台处理。

威胁告警名称	告警 等级	威胁说明	处理建议
进程异常行为	低危	检测到ECS实例存在进程异 常行为,疑似恶意程序。	建议登录企业主机安全管理 控制台处理。



# 8.1 漏洞管理简介

# 背景介绍

态势感知通过集成华为云安全公告、漏洞扫描数据,以及实施扫描任务,集中呈现云 上资产漏洞风险,以及实时通报突发安全漏洞预警,帮助用户及时发现资产安全短 板,修复危险漏洞。

态势感知支持以下类型的漏洞:

• 应急漏洞公告

接入华为云安全公告数据信息,呈现业界近期广泛披露的热点安全漏洞。

- 主机漏洞
   包括Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞。
- 网站漏洞

包括Web常规漏洞、端口漏洞、弱密码、CVE漏洞、网页内容合规(图片、文字)、网站挂马、链接健康等共8大类漏洞的检测。

## 应急漏洞公告

态势感知通过采集华为云安全公告讯息,及时呈现业界近期广泛披露的安全漏洞,并 支持一键获取安全漏洞详情、影响范围和处置建议等信息,提供对资产风险的消减建 议。应急漏洞功能支持以下特性:

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

# 主机漏洞

态势感知通过<mark>授权主机</mark>,并一<mark>键扫描主机漏洞</mark>,呈现主机漏洞扫描检测信息,支持查 看漏洞详情,并提供相应漏洞修复建议。

主机漏洞共支持3大类漏洞项的检测,详情请参见<mark>表8-1</mark>说明。

表 8-1 主机漏洞检测项说明

检测项	说明
Linux软件漏洞检 测	通过与漏洞库进行比对,检测系统和软件(例如:SSH、 OpenSSL、Apache、MySQL等)是否存在的漏洞,呈现漏洞结 果,并提供修复建议。
Windows系统漏	通过订阅微软官方更新,判断服务器上的补丁是否已经更新,并
洞检测	推送微软官方补丁,呈现漏洞结果,并提供修复建议。
Web-CMS漏洞检	通过对Web目录和文件进行检测,识别出Web-CMS漏洞,呈现
测	漏洞结果。

# 网站漏洞

态势感知通过接入漏洞管理服务的扫描结果数据,集中呈现网站存在的漏洞,提供详细的漏洞分析结果,并针对不同类型的漏洞提供专业可靠的修复建议。

网站漏洞共支持8大类漏洞项的检测,详情扫描内容参见<mark>表8-2</mark>。

#### 表 8-2 网站漏洞检测项说明

检测项	说明
Web常规漏洞扫 描	默认必选扫描项。扫描常规的30+种Web漏洞,包括XSS、SQL 等网站漏洞。
端口扫描	(可选)扫描服务器端口的开放状态,检测出容易被黑客发现 的"入侵通道"。
弱密码扫描	(可选)扫描网站的弱密码漏洞。
	<ul> <li>全方位的OS连接,涵盖90%的中间件,支持标准Web业务弱 密码检测、操作系统、数据库等弱口令检测。</li> </ul>
	<ul> <li>丰富的弱密码匹配库,模拟黑客对各场景进行弱口令探测。</li> </ul>
CVE漏洞扫描	(可选)接入公共暴露漏洞库(Common Vulnerabilities and Exposures,CVE ),根据漏洞库快速更新漏洞规则,扫描CVE 最新漏洞。
网页内容合规检 测(文字)	(可选)检测网站文字的合规性。
网页内容合规检 测(图片)	(可选)检测网站图片的合规性。
网站挂马检测	(可选)检测网站的挂马漏洞风险。

检测项	说明
链接健康检测	(可选)检测网站的链接地址健康性,避免死链、暗链、恶意 链接。

# 8.2 查看应急漏洞公告列表

当业界有新安全漏洞披露时,您可以使用"应急漏洞公告"功能,获取业界近期披露的热点安全漏洞信息,助您及时确认资产是否有受到威胁,消减资产风险。

应急漏洞功能支持以下特性:

- 支持每5分钟抓取一次安全公告讯息,更新应急漏洞公告。
- 支持按披露时间排序应急漏洞公告。
- 支持按关键字查找应急漏洞公告。
- 支持导出全部应急漏洞公告列表。

# 约束限制

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

## 查看应急漏洞公告

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- **步骤3** 在态势感知管理页面选择"漏洞管理 > 应急漏洞公告",进入"应急漏洞公告"汇聚页面。

#### 图 8-1 应急漏洞公告

应	应急漏洞公告⑦ 主机漏洞 网站漏洞			
全	部 (315) ● 未读 (230)	已濃     全部时间     ▼       请输入关键字进行搜索     Q	更新时间: 2021/07/06 19:15:00 ⑦ []	
	披露时间 ↓=	公告名称		
•	2021/7/6 16:50:00	Kaseya VSA 远程代码执行漏洞预警(CVE-2021-30116)		
•	2021/7/2 16:02:00	Windows Print Spooler远程代码执行Oday漏洞预警 (CVE-2021-34527)		
•	2021/6/30 17:25:00	ForgeRock AM远程代码执行漏洞预警(CVE-2021-35464)		
•	2021/6/30 11:05:00	Windows Print Spooler远程代码执行漏洞预警 (CVE-2021-1675)		
	2021/6/24 18:12:00	Apache Dubbo多个远程代码执行漏洞		
	2021/6/23 20:08:00	VMware Carbon Black App Control(AppC)身份验证线过篇调预警(CVE-2021-21998)		
•	2021/6/16 15:50:00	Apache Shiro历史高危反序列化漏洞预警(shiro-550、shiro-721)		
•	2021/6/9 13:50:00	微软6月份月度安全漏洞预警		
•	2021/6/3 14:36:00	用友NC BeanShell远程代码执行漏洞预警(CNVD-2021-30167)		
•	2021/6/1 17:24:00	runc 符号钳姆挂载与容器逃逃漏洞预警(CVE-2021-30465)		
10	▼ 总条数: 315 〈	1 2 3 4 5 32 <b>&gt;</b>		

步骤4 查看应急漏洞公告列表刷新时间。

查看右上角"更新时间",即可获知列表刷新时间。

步骤5 查看应急漏洞公告详细信息。

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

步骤6 按时间查看应急漏洞公告。

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

步骤7 搜索历史应急漏洞公告。

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

#### ----结束

### 导出应急漏洞公告

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

导出的Excel文件中包含"公告名称"、"披露时间"、"链接"等信息。

# 8.3 查看主机漏洞扫描详情

执行完主机漏洞扫描任务后,可在主机漏洞页面查看扫描结果。

# 约束限制

受漏洞管理服务(CodeArts Inspector )调整影响,仅付费续存期用户可继续正常使用 主机漏洞功能。

新用户以及付费版本到期的用户,请先开启HSS产品集成(详情请参见<mark>启用产品集</mark> 成),通过查看全部检查结果,获取主机扫描结果。

#### 前提条件

- 已购买态势感知标准版或专业版,且在有效使用期内。
- 已完成主机漏洞扫描任务。

## 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。
- **步骤3** 在态势感知管理页面选择"漏洞管理 > 主机漏洞",进入"主机漏洞"页面。主机漏洞参数说明如表8-3。

#### 🛄 说明

在列表的右上角,用户可以根据漏洞IP、漏洞等级或者漏洞名称进行筛选查看目标类漏洞详情。

#### **图 8-2** 主机漏洞

应急漏洞公告 ② _ 主机漏洞 网站漏洞				
			▼         全部等级         ▼	名称 Q C
漏洞名称	IP	漏洞等级	修复建议	操作
CESA-2019:2829	192	🕗 高危	update kernel,kernel-devel,kernel-headers,kerne	查看忽略理由 取消忽略
CESA-2019:1880	192.	🕗 高危	update curl,libcurl to the latest version	查看忽略理由 取消忽略
CESA-2019:1873	192.	🕗 高危	update kernel, kernel-devel, kernel-headers, kerne	查看忽略理由 取消忽略
CESA-2019:1619	192	🕗 高危	update vim-common, vim-enhanced, vim-filesyst	忽略
CESA-2019:3055	192	🕗 高危	update kernel,kernel-devel,kernel-headers,kerne	忽略
CESA-2019:1884	192	🕗 高危	update libssh2 to the latest version	忽略
CESA-2019:3197	192	❶ 提示	update sudo to the latest version	忽略
CESA-2019:2964	192.	💧 高危	update patch to the latest version	忽略
CESA-2019:1587	192	🕗 高危	update python,python-libs to the latest version	忽略

### 表 8-3 主机漏洞参数说明

参数名称	参数说明		
漏洞名称	扫描出的漏洞名称。 单击漏洞名称,可查看该漏洞的简介、相关漏洞库信息。		
IP	主机的IP地址。		
参数名称	参数说明		
------	--		
漏洞等级	按照漏洞的危险程度分为:"高危"、"中危"、"低危"、"提示"。		
修复建议	根据修复建议,快速对漏洞做出响应处理。		
操作	<ul> <li>如果某一项漏洞您已经完成了修复,可以在目标漏洞的"操作" 列,单击"忽略"。</li> </ul>		
	<ul> <li>如果希望重新关注已经忽略的漏洞,可以在目标漏洞的"操作"</li> <li>列,单击"查看忽略理由"了解当时的处理原因,确认需要恢复风险项后,单击"取消忽略",恢复风险项检测。</li> </ul>		

----结束

# 8.4 查看网站漏洞扫描详情

执行完网站漏洞扫描任务后,可在网站漏洞页面查看扫描结果。

## 约束限制

受漏洞管理服务(CodeArts Inspector)调整影响,仅付费续存期用户可继续正常使用主机漏洞功能。
 新用户以及付费版本到期的用户,请先开启CodeArts Inspector产品集成(详情请参见启用产品集成),通过查看全部检查结果,获取网站扫描结果。

### 前提条件

- 已购买态势感知专业版,且在有效使用期内。
- 已完成网站扫描任务。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在态势感知管理页面选择"漏洞管理 > 网站漏洞",进入"网站漏洞"页面。

#### 图 8-3 查看网站漏洞信息

态势感知	漏洞管理		🔤 专业版 : 增加配級
安全看板			
综合大屏	应急漏洞公告 ⑦ 主机漏洞 网站漏洞		
资产管理			
威胁告答	漏洞名称	漏洞等级	
温洞管理			
基线检查		( • )	
检测结果	<u> </u>		
分析报告	暂无表格数据	暂无表格数据	24
日志管理			
安全产品集成			

### 步骤4 查看漏洞分布比例及漏洞等级分布比例,如图8-4。

### **图 8-4** 网站漏洞



### 步骤5 查看漏洞详情列表,网站漏洞参数说明如表8-4。

### 图 8-5 网站漏洞详情列表

标记	为忽略						所有状态 ▼ 高级搜索 ≫
	漏洞名称/漏洞ID	目标网址	发现时间	漏洞等级	检测项目	状态	操作
	内容安全策略 13e3ee431c1f8f94	http://	2019/01/03 22:02:37 GMT+08:00	〇 低危	Others	未修复	忽略取消忽略
	内容安全策略 ab5ee2a8ceea2c9	http://	2019/01/03 22:02:37 GMT+08:00	0 低危	Others	未修复	忽略 取消忽略

#### 表 8-4 网站漏洞参数说明

参数名称	参数说明
漏洞名称/漏洞 ID	扫描出的漏洞名称。 单去漏洞名称,可查看该漏洞的简介,相关漏洞库信息
	网站的IP地址。
发现时间	任务扫描出漏洞的时间。
漏洞等级	按照漏洞的危险程度分为:"高危"、"中危"、"低危"、"提示"。
检测项目	漏洞类型。
状态	<ul> <li>"未修复"</li> <li>"已修复"</li> <li>"已忽略"</li> </ul>
操作	<ul> <li>如果确认该风险类型不存在风险,在目标风险类型所在行的"操作"列,单击"忽略",忽略此风险项。</li> <li>如果想对已忽略的风险项恢复为风险类型,在目标风险类型所在行的"操作"列,单击"取消忽略",恢复检测此风险。</li> </ul>

----结束



# 9.1 云服务基线简介

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

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

## 约束与限制

- SA基础版暂不支持使用基线检查功能。标准版暂不支持云服务基线查看详情功能。为及时了解云服务配置状态,以及确保云服务的配置的合理性,建议您购买专业版。
- 操作账号权限检查。使用基线检查功能时,除了需要"SA FullAccess"、"SA ReadOnlyAccess"策略权限,还需要"Tenant Administrator"权限和IAM相关 权限,请提前授予操作账号对应权限。

"Tenant Administrator"权限和IAM相关权限配置详细操作请参见配置基线检查功能所需的权限。

• 基线检查功能为Region级别功能,具体上线region请以SA控制台显示为准。

# 9.2 基线检查项目

态势感知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<mark>查看基线检查项目详情</mark>。

本章节将介绍SA云服务基线检查支持的检查项目。

## 表 9-1 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	身份与访问管理		12
1.0	检测		7
	基础设施防护		24
	数据防护		22
	事件响应		13
护网检查	安全套件覆盖		12
	账号加固		5
	主机加固		4
	Sudo漏洞		1
	访问控制		1
	敏感信息排查		5
等保2.0三级要求	安全通用要求	安全物理环境	22
		安全通信网络	8
		安全区域边界	20
		安全计算环境	34
		安全管理中心	12
		安全管理制度	7
		安全管理机构	14
		安全管理人员	12
		安全建设管理	34
		安全运维管理	48
	云计算安全扩展要 求	安全物理环境	1
		安全通信网络	5
		安全区域边界	8
		安全计算环境	19
		安全管理中心	4
		安全建设管理	8
		安全运维管理	1
	安全运维管理		1

检查规范	检查类别	包含的检查项数量
	安全运维管理	1

# 安全上云合规检查一身份与访问管理

### 表 9-2 身份与访问管理风险项检查项目

检查项目	检查内容
IAM用户启用检查	启用统一身份认证(Identity and Access Management,IAM)服务后,系统默认用户组admin中 的IAM用户,可以使用华为云所有服务。 检查所有IAM用户列表,是否已启用至少两个IAM用户,
	以及IAM用户所属的用户组是否都为admin用户组。
IAM用户开启登录保护 检查	在IAM的安全设置中启用登录保护后,登录时还需要通过 虚拟MFA或短信或邮件验证,再次确认登录者身份,进一 步提高账号安全性,有效避免钓鱼式攻击或者用户密码意 外泄漏,保护您安全使用云产品。 检查在IAM的安全设置中是否开启登录保护。
IAM用户开启操作保护 检查	在IAM的安全设置中开启操作保护后,主账户及子用户在 控制台进行敏感操作(如:删除弹性云服务器、解绑弹性 IP等)时,将通过虚拟MFA、手机短信或邮件再次确认操 作者身份,进一步提高账号安全性,有效保护您安全使用 云产品。
 管理品账号AK/SK启田	位旦IAMI用广走百开后採IF体扩。   访问変钼(AK/SK、Access Key ID/Secret Access Key)
检查	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。

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

## 安全上云合规检查—检测

### 表 9-3 检测风险项检查项目

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

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

# 安全上云合规检查一基础设施防护

### 表 9-4 基础设施防护风险项检查项目

检查项目	检查内容
安全组入方向规则控制 检查	安全组入方向规则应满足最小化访问控制原则。 一般,在非业务需要的情况下,以下情况视为未按最小化 访问控制(风险由高到低):源地址为0.0.0/0;公网地 址的掩码小于32;内网地址的掩码小于24。
高危端口、远程管理端 口暴露检查	安全组是一个逻辑上的分组,为具有相同安全保护需求并 相互信任的云服务器提供访问策略。安全组创建后,可以 在安全组中设置出方向、入方向规则,这些规则会对安全 组内部的云服务器出入方向网络流量进行访问控制,当云 服务器加入该安全组后,即受到这些访问规则的保护。 安全组入方向规则中不应对外开放或未最小化开放高危端 口、远程管理端口。 高危端口如下:20,21,135,137,138,139,445, 389,593,1025 未最小化开放指的是:源地址为0.0.0/0;公网地址的掩 码小于32;内网地址的掩码小于24 检查安全组入方向规则中是否存在对外开放或未最小化开 放高危端口、远程管理端口。
绑定EIP的ECS配置密钥 对登录检查	当存在ECS对外暴露EIP的情况下,为安全起见,弹性云服 务器登录时应使用密钥方式进行身份验证。
日志指标过滤和告警事 件(VPC更改)检查	日志审计模块是信息安全审计功能的核心必备组件,是企 事业单位信息系统安全风险管控的重要组成部分。云审计 服务(Cloud Trace Service,以下简称CTS),是华为云 安全解决方案中专业的日志审计服务,提供对各种云资源 操作记录的收集、存储和查询功能,可用于支撑安全分 析、合规审计、资源跟踪和问题定位等常见应用场景。 检查CTS中是否存在因VPC更改而产生的日志和告警事 件。

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

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

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

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

## 安全上云合规检查——数据防护

表 9-5	数据防护风险项检查项目
-------	-------------

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

检查项目	检查内容
DCS数据库绑定EIP时的 安全设置检查	当分布式缓存服务(Distributed Cache Service,简称 DCS)配置公网连接时,业务数据会在公网上进行传输, 数据容易泄露,因此,需要最小化控制访问源以及开启 SSL通道、更改默认数据库端口。 检查当DCS数据库配置公网连接时,是否限制访问源以及 开启SSL、更改默认端口。
云数据库GaussDB绑定 EIP时的安全设置检查	当云数据库GaussDB配置公网连接时,业务数据会在公 网上进行传输,数据容易泄露,因此,需要最小化控制 访问源以及开启SSL通道、更改默认数据库端口。 检查当云数据库GaussDB配置公网连接时,是否限制访 问源以及开启SSL、更改默认端口。
RDS数据库绑定EIP检查	当云数据库RDS(Relational Database Service,简称 RDS)配置公网连接时,业务数据会在公网上进行传输, 数据容易泄露,因此,不建议数据库开通公网连接方 式。 检查当RDS数据库配置,是否开通公网连接方式。
DDS数据库绑定EIP检查	当文档数据库服务(Document Database Service)配置 公网连接时,业务数据会在公网上进行传输,数据容易 泄露,因此,不建议数据库开通公网连接方式。 检查当DDS数据库配置,是否开通公网连接方式。
DCS数据库绑定EIP检查	当分布式缓存服务(Distributed Cache Service,简称 DCS)配置公网连接时,业务数据会在公网上进行传输, 数据容易泄露,因此,不建议数据库开通公网连接方 式。 检查当DCS数据库配置,是否开通公网连接方式。
云数据库GaussDB绑定 EIP检查	当云数据库GaussDB配置公网连接时,业务数据会在公 网上进行传输,数据容易泄露,因此,不建议数据库开 通公网连接方式。 检查当云数据库GaussDB配置,是否开通公网连接方 式。
RDS数据库实例安全组 规则检查	检查关系型数据库(Relational Database Service, RDS)实例所关联的安全组规则是否存在不安全规则,即 检查安全组规则的允许范围是否超过使用范围。当源地 址为0.0.0/0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(所有地址), 端口为1~65535或者数据库业务端口,如3306。
GaussDB数据库实例安 全组规则检查	安全组入方向规则应满足最小化访问控制原则。 一般地,在非业务需要的情况下,以下情况视为未按最 小化访问控制(风险由高到低): IPv4:源地址为0.0.0.0/0;公网地址的掩码小于32;内网 地址的掩码小于24 IPv6:源地址为::/0

检查项目	检查内容
OBS桶服务端加密检查	OBS服务端加密是在上传对象到桶时,将数据在服务端加 密成密文后存储。再次下载加密对象时,存储的密文会 先在服务端解密为明文,再反馈给用户。将数据加密后 存储到OBS桶中,提高数据的安全性。
	检查所有OBS桶是否开启服务端加密。
OBS桶的ACL权限检查	OBS桶ACL是基于账号或用户组的桶级访问控制,桶的拥 有者可以通过桶ACL授予指定账号或用户组特定的访问权 限。
	匿名用户指未注册华为云的普通访客。如果OBS桶的ACL 赋予了匿名用户桶的访问权限或ACL访问权限,表示所有 人无需经过任何身份验证即可访问OBS桶。
	检查所有OBS桶,是否给匿名用户赋予桶访问权限或者 ACL访问权限。
MySQL数据库实例root 用户远程登录控制检查	MySQL数据库实例的root应做好远程登录的控制,限制 仅应用端、DAS管理网段等业务需要方可登录,防止root 账号被暴力破解。
RDS数据库实例安全组	安全组入方向规则应满足最小化访问控制原则。
入方向规则检查   	一般,在非业务需要的情况下,以下情况视为未按最小 化访问控制(风险由高到低 ):
	IPv4:源地址为0.0.0.0/0;公网地址的掩码小于32;内网 地址的掩码小于24
	IPv6:源地址为::/0
	检查云数据库(Relational Database Service,RDS)实 例所关联的安全组入方向规则是否按最小化访问控制。
DCS数据库实例安全组	安全组入方向规则应满足最小化访问控制原则。
入万回规则检查   	一般,在非业务需要的情况下,以下情况视为未按最小 化访问控制(风险由高到低 ):
	IPv4:源地址为0.0.0.0/0;公网地址的掩码小于32;内网 地址的掩码小于24
	IPv6:源地址为::/0
	检查分布式缓存服务(Distributed Cache Service, DCS)实例所关联的安全组入方向规则是否按最小化访问 控制。
DDS数据库实例安全组	安全组入方向规则应满足最小化访问控制原则。
入方向规则检查	一般,在非业务需要的情况下,以下情况视为未按最小 化访问控制(风险由高到低 ):
	IPv4:源地址为0.0.0.0/0;公网地址的掩码小于32;内网 地址的掩码小于24
	IPv6: 源地址为::/0
	检查文档数据库服务(Document Database Service, DDS)实例所关联的安全组入方向规则是否按最小化访问 控制。

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

# 安全上云合规检查——事件响应

### 表 9-6 事件响应风险项检查项目

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

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

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

## 护网检查一安全套件覆盖

表 9-7	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	企业主机安全服务(Host Security Service, HSS)是提 升主机整体安全性的服务,通过主机管理、风险预防、入 侵检测、高级防御、安全运营、网页防篡改功能,全面识 别并管理主机中的信息资产,实时监测主机中的风险并阻 止非法入侵行为,帮助企业构建服务器安全体系,降低当 前服务器面临的主要安全风险。 检查主机是否已开启防护。
主机Agent状态检查	企业主机安全服务(Host Security Service, HSS)是一 个用于全面保障主机整体安全的服务,能帮助您高效管理 主机的安全状态,并构建服务器安全体系,降低当前服务 器面临的主要安全风险。 在主机中安装Agent后,您的主机才能收到HSS的保护。 检查主机Agent是否为在线状态。
主机安全检测状态检查	企业主机安全服务(Host Security Service, HSS)将实 时检测主机中的风险和异常操作,在每日凌晨将对主机执 行全面扫描。执行配置检测后,您可以根据检测结果中的 相关信息,修复主机中含有风险的配置项或忽略可信任的 配置项。 检查主机的检测结果是否存在异常。
WAF(云模式)基础防 护配置检查	Web基础防护开启后,默认防范SQL注入、XSS跨站脚 本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令 执行、目录遍历、敏感文件访问、命令/代码注入等常规 的Web攻击。 检查WAF在云模式下是否已开启Web基础防护。

检查项目	检查内容
WAF(云模式)防护策 略配置检查	Web基础防护支持"拦截"(发现攻击行为后立即阻断并 记录)和"仅记录"(发现攻击行为后只记录不阻断攻 击)模式,检测版仅支持"仅记录"模式。
	WAF中所有待防护的域名应开启Web基础防护并设置为拦 截模式,开启后,默认防范SQL注入、XSS跨站脚本、远 程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、 目录遍历、敏感文件访问、命令/代码注入等常规的Web 攻击。
	检查WAF在云模式下是否已开启Web基础防护并设置为拦 截模式。
WAF(独享模式)基础 防护配置检查	Web基础防护开启后,默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。
	检查WAF在独享模式下是否已开启Web基础防护。
WAF(独享模式)防护 策略配置检查	Web基础防护支持"拦截"(发现攻击行为后立即阻断并 记录)和"仅记录"(发现攻击行为后只记录不阻断攻 击)模式,检测版仅支持"仅记录"模式。
	WAF中所有待防护的域名应开启Web基础防护并设置为拦 截模式,开启后,默认防范SQL注入、XSS跨站脚本、远 程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、 目录遍历、敏感文件访问、命令/代码注入等常规的Web 攻击。
	检查WAF在独享模式下是否已开启Web基础防护并设置为 拦截模式。
网站高危漏洞检查	漏洞管理服务(CodeArts Inspector )可以帮助您快速检 测出您的网站存在的漏洞,提供详细的漏洞分析报告,并 针对不同类型的漏洞提供专业可靠的修复建议。
	检查网站中是否存在高危漏洞。
网站中危漏洞检查	漏洞管理服务(CodeArts Inspector)可以帮助您快速检 测出您的网站存在的漏洞,提供详细的漏洞分析报告,并 针对不同类型的漏洞提供专业可靠的修复建议。 检查网站中是否存在中危漏洞。
扫描时间检查	漏洞管理服务(CodeArts Inspector)可以帮助您快速检 测出您的网站存在的漏洞,提供详细的漏洞分析报告,并 针对不同类型的漏洞提供专业可靠的修复建议。 检查扫描时间是否已超过一周。
SA专业版购买检查	态势感知提供基础版、标准版和专业版三个版本,不同版 本有不同功能使用范围。 专业版可以呈现全局安全态势。通过动态安全检测和威胁 分析,并提供安全加固建议。 检查是否已购买SA专业版。

检查项目	检查内容
主机Agent版本检查	在主机中安装Agent后,您的主机将受到HSS云端防护中 心全方位的安全保障,在安全控制台可视化界面上,您可 以统一查看并管理同一区域内所有主机的防护状态和主机 安全风险。
	企业主机安全服务有基础版、企业版、旗舰版和网页防篡 改版四个版本。
	基础版一般只用于测试、个人用户防护主机账户安全。建 议您选择企业版及以上版本。 检查所有主机Agent是否为企业版及以上版本。

# 护网检查——账号加固

表 9-8 账号加固风险项检查项目	目
-------------------	---

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

# 护网检查—主机加固

### 表 9-9 主机加固风险项检查项目

检查项目	检查内容
主机高危端口暴露检查	HSS提供资产管理功能,主动检测主机中的开放端口,及 时发现主机中含有风险的各项资产。
	如果检测到开放了危险端口或者开放了不必要的端口,需 要排查这些端口是否是正常业务使用,如果不是正常业务 端口,建议关闭端口。对于危险端口建议进一步检查程序 文件,如果存在风险建议删除或者隔离源文件。
	检查所有主机是否在对外开放或未最小化开放的高危端 口。
CCE集群Kubernetes版 本检查	云容器引擎(Cloud Container Engine,简称CCE)提供 高度可扩展的、高性能的企业级Kubernetes集群,支持 运行Docker容器。借助云容器引擎,您可以在华为云上 轻松部署、管理和扩展容器化应用程序。
	当CCE集群Kubernetes版本低于1.15,有安全漏洞风险, 建议您进行升级。
	检查CCE集群Kubernetes版本是否在1.15以下。
VPC配置(对等连接) 检查	对等连接是指两个VPC之间的网络连接。您可以使用私有 IP地址在两个VPC之间进行通信,就像两个VPC在同一个 网络中一样。您可以在自己的VPC之间创建对等连接,也 可以在自己的VPC与同一区域内其他的VPC之间创建对等 连接。
	检查VPC是否已经创建对等连接,如果已创建,则检查是 否开放或未最小化高危端口。
VPC配置(VPN网关) 检查	VPN网关是虚拟私有云中建立的出口网关设备,通过VPN 网关可建立虚拟私有云和企业数据中心或其它区域VPC之 间的安全可靠的加密通信。 检查VPC是否已经创建了VPN网关。

# 护网检查—Sudo 漏洞

## 表 9-10 Sudo 漏洞风险项检查项目

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

# 护网检查—访问控制

### 表 9-11 访问控制风险项检查项目

检查项目	检查内容
安全组入方向规则控制 检查	安全组入方向规则应满足最小化访问控制原则。 一般,在非业务需要的情况下,以下情况视为未按最小化 访问控制(风险由高到低):源地址为0.0.0/0;公网地 址的掩码小于32;内网地址的掩码小于24。 IPv4:源地址为0.0.0.0/0;公网地址的掩码小于32;内网 地址的掩码小于24。 IPv6:源地址为::/0。

## 护网检查—敏感信息排查

表 9-12 敏感信息排查风险坝检查坝
---------------------

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

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

# 等保 2.0 三级要求一安全物理环境

表 9-13 安全物理环境风险项检查项目

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

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

## 等保 2.0 三级要求一安全通信网络

表 9-14 安全通信网络风险项检查项目

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

## 等保 2.0 三级要求一安全区域边界

### 表 9-15 安全区域边界风险项检查项目

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

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

## 等保 2.0 三级要求一安全计算环境

### 表 9-16 安全计算环境风险项检查项目

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

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

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

# 等保 2.0 三级要求一安全管理中心

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

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

## 等保 2.0 三级要求一安全管理制度

表 9-18 安全管理制度风险项检查项目

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

## 等保 2.0 三级要求一安全管理机构

表 9-19 安全管理机构风险项检查项目

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

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

## 等保 2.0 三级要求一安全管理人员

表 9-20 安全管理人员风险项检查项目

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

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

# 等保 2.0 三级要求一安全建设管理

### 表 9-21 安全建设管理风险项检查项目

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

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

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

# 等保 2.0 三级要求一安全运维管理

### 表 9-22 安全运维管理风险项检查项目

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

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

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

## 等保 2.0 三级要求一安全物理环境

#### 表 9-23 安全物理环境风险项检查项目

检查子项目	检查项目
基础设施位置	应保证云计算基础设施位于中国境内。

## 等保 2.0 三级要求一安全通信网络

### 表 9-24 安全通信网络风险项检查项目

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

## 等保 2.0 三级要求一安全区域边界

表 9-25 安全区域边界风险项检查项目

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

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

# 等保 2.0 三级要求一安全计算环境

表 9-26 安全计算环境风险项检查项目

检查子项目	检查项目
身份鉴别	当远程管理云计算平台中设备时,管理终端和云计算平台 之间应建立双向身份验证机制。
访问控制	应保证当虚拟机迁移时,访问控制策略随其迁移。
	应允许云服务客户设置不同虚拟机之间的访问控制策略。
入侵防范	应能检测虚拟机之间的资源隔离失效,并进行告警。
	应能检测到非授权新建虚拟机或者重新启用虚拟机,并进 行告警。
	应能检测恶意代码感染及在虚拟机间蔓延情况,并进行告 警。
镜像和快照保护	应针对重要业务系统提供加固的操作系统镜像或操作系统 安全加固服务。
	应提供虚拟机镜像、快照完整性检验功能,防止虚拟机镜 像被恶意篡改。
	应采取密码技术或其他技术手段防止虚拟机镜像、快照中 可能存在的敏感资源被非法访问。
数据完整性和保密性	应确保云服务客户数据、用户个人信息等存储于中国境 内,如需出境应遵循国家相关规定。
	应确保只有在云服务客户授权下,云服务提供商或第三方 才具有云服务客户数据的管理权限。
	应确保虚拟机迁移过程中重要数据的完整性,并在检测到 完整性受到破坏时采取必要的恢复措施。
	应支持云服务客户部署密钥管理解决方案,保证云服务客 户自行实现数据的加解密过程。
数据备份恢复	云服务客户应在本地保存其业务数据的备份。
	应提供查询云服务客户数据及备份存储位置的能力。
检查子项目	检查项目
--------	---
	云服务提供商的云存储服务应保证云服务客户数据存在若 干个可用的副本,各副本之间的内容应保持一致。
	应为云服务客户将业务系统及数据迁移到其体云计算平台 和本地系统提供技术手段,并协助完成迁移过程。
剩余信息保护	应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

# 等保 2.0 三级要求一安全管理中心

表 9-27 安全管理中心风险项检	塗项目
-------------------	-----

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

# 等保 2.0 三级要求一安全建设管理

#### 表 9-28 安全建设管理风险项检查项目

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

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

# 等保 2.0 三级要求一安全运维管理

#### 表 9-29 安全运维管理风险项检查项目

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

# 等保 2.0 三级要求一安全运维管理

#### 表 9-30 安全运维管理风险项检查项目

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

# 等保 2.0 三级要求一安全运维管理

#### 表 9-31 安全运维管理风险项检查项目

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

# 9.3 配置基线检查功能所需的权限

当您需要使用SA的**基线检查**功能时,需要给操作账号配置"Tenant Administrator" 权限和IAM相关权限。 本章节将介绍如何配置SA相关功能所需的权限。

#### 前提条件

已获取管理员账号及密码。

#### 配置基线检查功能所需的权限

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"管理与监管 > 统一身份认证服务",进入统一身份认证服务管理控制台。
- 步骤3 添加IAM相关权限。
  - 在左侧导航栏选择"权限管理 > 权限",并在权限页面右上角单击"创建自定义 策略"。
  - 2. 配置策略。
    - a. 策略名称: 自定义。
    - b. 作用范围:选择"全局级范围"。
    - c. 策略配置方式:选择"JSON视图"。
    - d. 策略内容: 请直接复制粘贴以下内容。



3. 单击"确定"。

步骤4 在左侧导航栏选择"委托",进入委托页面。

- 步骤5 在委托列表中选择"ssa\_admin\_trust",进入委托详情页面。
- 步骤6选择"授权记录"页签,并在页面中单击"授权"。
- 步骤7 在权限配置栏目搜索并选择"Tenant Administrator"和步骤3创建的权限。

#### 图 9-1 基线检查权限策略

委托	'ssa_adr	nin_trust"将拥有所选策略				新建策略
	直君已选()	2) 从其他区域项目复制权限	全部类型 🔻	所有云服务	▼ 请输入名称或描述	Q
	1	名称		类型		
	~	sa 		自定义策略		
	~	Tenant Administrator 全部云服务管理员(除IAM管理权限)		系统角色		

步骤8 单击页面下方"下一步",设置最小授权范围。

**步骤9**单击页面下方的"确定",完成配置。

# 9.4 设置基线检查计划

态势感知支持根据基线检查计划检查您的服务器基线配置是否存在风险。 本文档介绍了如何新增、编辑、删除基线检查计划。

# 背景信息

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

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

# 约束限制

创建检查计划是同一个检查规范只能属于一个检查计划。

#### 前提条件

已购买态势感知标准版或专业版。

# 创建检查计划

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 进入基线检查计划配置页面。
  - 方法一:
    - a. 在左侧导航栏选择"基线检查",进入基线检查页面。
    - b. 单击页面右上角的"设置检查计划",进入检测设置页面。

<sup>----</sup>结束

#### 图 9-2 进入基线检查计划配置页面

态势感知 	基线检查				<ul> <li>② 评价</li> <li>② 专业版:</li> </ul>
安全概况 资源管理 业务分析 ▼	区域 	检查规范数 4/4	检查项 		设置检查规范 2 ジ目始直 2 ジ目始直 1 2 ジ目始直 1 3 1 1 1 1 1 1 1 1 1 1 1 1 1
综合大屏 资产管理 威胁告誓	检查项合稿本 ⑦	风险资源分布	不合格检查项数	风险管理的	
漏洞管理 基线检查	● 台格 (16) ● 不合格 (17) ● 检查失败 (9)	数命 高危 中危	0 8 4	0 57	_
检测结果 分析报告 日本解研	• 待检童 (154)	低危	4	8	E

• 方法二:

在左侧导航栏选择"设置 > 检测设置",进入检测设置页面。

图 9-3 检测设置页面

态势感知	检测设置	🥥 专业版 🗄
2全看板		
综合大屏		
资产管理		
成肋告答	创建计划	
漏洞管理	default (系统默认) 立即检查	
基线检查	10 毎3天0.00-6.00检査一次	
检测结果	检查规范	
分析报告	安全上云合规检查1.0	
日志管理		
安全产品集成		
设置		
通知设置		
检测设置		

**步骤4** 在检测设置页面中,选择待创建计划所在的区域,并单击"创建计划",系统右侧弹出新建检查计划的页面。

图 9-4 创建检查计划

	2004-00 • 请能入意识的关键字 已建模	<sup>絵</sup> 宣 Q 操作
田雄八川初島称     田雄八川初島称     国雄八川初島称     国雄八川和島称     国雄八川和島称     国雄八川和島称     国雄八川和島称     国雄八川和島称     国雄八川和島称     国雄八川和島称     国雄八川和島和	200-6:00 · · · · · · · · · · · · · · · · · ·	を 章 、 保作
総置时间 毎1天 (0) 法学检查规范 (前級人団用的大能学 Q) ()可勉強 ()毎620三級要求 () (1000年)	200-6-00 • - - - - - - - - - - - - -	松宣 Q 操作
<ul> <li>透野社会规范</li> <li>(日本) 三田田(大田)</li> <li>(日本) 三田田(大田)</li> <li>(日本) 三田田(大田)</li> <li>(日本) 三田田(大田)</li> </ul>	语输入面询的关键字 已选项	Q 操作
<ul> <li>         · 資金入室加約关键字 Q         · 可請及         · 可請及         · 受保2.0三級要求         · の口がで         ·         ·         ·</li></ul>	请输入宣询的关键字 已逸顶	Q 操作
<ul> <li>可透版</li> <li>等保2 0三级要求</li> </ul>	已选顶	操作
● 等保2.0三级要求		
U PMSE	<b>日</b> 元秋和秋湖	

步骤5 配置检查计划。

1. 填写基本信息,具体参数配置如表9-32所示。

### 表 9-32 检查计划基本信息

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

2. 选择检查规范。

选择需要检测的基线检查项目。更多关于基线检查项目详细描述请参见<mark>云服务基</mark> 线简介。

----结束

相关操作

基线检查计划创建后,您可以查看检查计划、对检查计划进行编辑或删除。

- 查看已有检查计划
  - a. 登录管理控制台。
  - b. 在页面左上角单击 ── ,选择"安全与合规 > 态势感知",进入态势感知管 理页面。
  - c. 在左侧导航栏选择"设置 > 检测设置",进入检测设置页面。
  - d. 在检测设置页面中,查看已有的基线检查计划。
- 编辑检查计划
  - a. 在目标计划所在框的右上角单击"编辑",系统右侧弹出编辑检查计划页 面。
  - b. 编辑需要修改的计划参数。
  - c. 单击"确定"。
- 删除检查计划
  - a. 在目标计划所在框的右上角单击"删除"。
  - b. 在弹出的对话框中,单击"是"。

# 9.5 执行基线检查计划

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

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

- 定期自动检查:根据SA为您提供的默认基线检查计划或您自定义的基线检查计划,定时自动执行基线检查。默认检查计划每隔3天在0点的时候自动执行基线检查。
- 立即检查:如果您新增或修改了自定义的基线检查计划,您可以在基线检查页面 选择该基线检查计划,立即执行基线检查,实时查看服务器中是否存在对应的基 线风险。

### 约束限制

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

# 前提条件

已配置自定义的基线检查计划。

### 立即检查所有检查规范

SA可根据您设置的检查规范,立即执行已配置的检查规范。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- **步骤3** 在左侧导航栏选择"基线检查",并在基线检查页面右上角单击"设置检查规范", 系统弹出选择检查规范窗口。

#### 图 9-5 基线检查页面

态势感知	基线检查				
安全概范					
资源管理	区域	检查规范数	检查项		2 设置检查规范 立即检查
业务分析 ▼	最近检查时间: 2022/01/27 12:00:05 GMT+08:00	4/4			设置检查计划
综合大屏					
资产管理	检查项合格率 ⑦	风险资源分布			
威胁告誓			不合格检查项数	风险资源数	
漏河管理	● 台悟 (16) ■ 万全核 (17)	数命	0	0	
基线检查 1	8% 检查失败 (9)	高危	8	57	
检测结果	0% 待检查 (154)	中危	4	13	e
分析报告		提示	1	0	G
日志管理			_		4

步骤4 在弹出的选择规范窗口中,选择检查规范,并单击"确定"。

**图 9-6** 选择检查规范

选择检查	题规范				×
1 系统	将为您检查全部有效资	<u>ģ</u>			
0	检查规范	检查计划	合格率	最近检查时间	
$\checkmark$	安全上云合规检	default	• 26%	2022/03/01	
	等保2.0三级要求		%		
	护网检查		81%	2022/03/01	
		确定 取消	á		

**步骤5** 在页面右上角单击"立即检查",立即执行扫描任务。 刷新页面,查看"最近检查时间",即可确认是否为最新的扫描结果。 系统将立即执行已配置的检查规范。

----结束

### 立即执行某个检查计划

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

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"设置 > 检测设置",进入检测设置页面。
- 步骤4 在检测设置页面,选择检查计划所在的区域。
- 步骤5 在待执行立即手动检查的检查计划所在栏的上方单击"立即检查"。

图 9-7 执行某个检查计划

test4	立即检查	编辑 删除
🖸 每1	天6:00-12:00检查一次 🚺	
检查规范	ŧ	
安全上艺	云合规检查1.0	

系统将立即执行已选择的基线检查计划。

----结束

# 9.6 执行手动检查

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

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

### 前提条件

- 已购买态势感知专业版,且在有效使用期内。
- 已在线下完成检查。

### 约束与限制

反馈结果有效期为7天,7天后请重新手动检查。

#### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4选择待查看检查结果所在的区域。
- 步骤5 在待反馈结果检查项目所在行的"操作"列,单击"反馈结果"。

图 9-8 反馈结果入口

检查规范检查资源	检查结果							
全部规范 (土) 安全上云合规检查1.0 12%	检查反馈结果	忽略 取消忽略			全部	•	请输入检查项名称搜索	Q
+ 等保2.0三级要求%	检查顶	检查状态↓Ξ	检查方式 🔽	风险资源 ↓Ξ	描述	最近检查↓日	操作	
+ 护网检查 35%	机房场地应选择在具	待检查 ?	手动检查	0	检查您规划机房的地		反馈结果 查看讲	羊情
							2	

步骤6 在弹出提示框中,选择反馈结果,并单击"确定"。

#### **图 9-9** 反馈结果

手动检查反馈结果			×
检查顶	描述	检查状态	
机房场地应选择在具有防	检查您规划机房的地址位	待检查	
反馈结果 合格	○ 不合格		
① 反馈结果有效期为7天,	7天后请重新手动检查。		×
	确定 取消		

🗀 说明

反馈结果有效期为7天,7天后请重新手动检查。

----结束

# 9.7 查看基线检查结果

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

#### 前提条件

- 已购买态势感知**专业版**,且在有效使用期内。
- 已扫描云服务基线。

# 查看检查结果总数据

查看某区域中所有检查项的检查结果。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果所在的区域,系统将展示当前区域的所有检查结果相关数据。

步骤5 查看当前区域检测到的基线检查结果汇总数据。

#### 图 9-10 检查结果总数据

区域 最近检查时间: 2022/01/27 12	▼ 00:05 GMT+08:00	检查规范数 4/4	检查项 		设置检查规范         立即检查           设置检查计划         设置检查计划
检查项合格率 ⑦		风险资源分布			
			不合格检查项数	风险资源数	
	● 合格 (16)	致命	0	0	
806	🛑 不合格 (17)	南危	8	57	
0%	检查失败 (9)	中危	4	13	
	待检查 (154)	低危	4	8	
		提示	1	0	

- 检查规范数:最近一次执行基线检查的检查规范数/检查规范总数。
- 检查项:最近一次执行基线检查中所有的检查项数目。
- 检查项合格率:最近一次执行基线检查的基线合格率。
   整体合格率=合格检查项数量/检查项总数。合格率的统计范围为全部规范的全部 检查项目。
   检查项目。
  - 检查项结果分为合格、不合格、检查失败和待检查几种。
- 风险资源分布:最近一次执行基线检查的风险资源分布情况以及风险资源的数量。

风险等级分为: 致命、高危、中危、低危、提示几个级别。

----结束

#### 查看基线检查规范列表

步骤1 登录管理控制台。

- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果的区域,并选择"检查规范"页签。
- **步骤5** 在基线检查规范中,选择"全部规范",系统将显示当前区域所有检查规范及其详细 信息,如<mark>图9-11</mark>所示。

检查规范 检查资	源	检查结果							
全部规范	8%	检查	全部 (346)	不合格 (16	<ol> <li></li></ol>	(11) 待检查	(293) 合格	(26) 请输入检查	重項名称撞索 Q
安全上云合规检查1.0	24%	检查顶	检查状态↓Ξ	检查方式	检查分类	风险资源 ↓Ξ	描述	最近检查 ↓Ξ	操作
等保2.0三级要求	96	主机防护状态检查	● 不合格	自动检查		10	企业主机安全服务	2022/03/01 12:00:	检查 宣誓详情
护网检查	63%	主机Agent状态检查	● 不合格	自动检查		10	企业主机安全服务	2022/03/01 12:00:	检查 查若详情
		安全组入方向规则	● 不合格	自动检查		8	安全组入方向规则	2022/03/01 12:00:	检查 查若详情
		高危端口、远程管	● 不合格	自动检查		8	安全组是一个逻辑	2022/03/01 12:00:	检查 查若详情
		// 绑定EIP的ECS配置	● 不合格	自动检查		2	当存在ECS对外器	2022/03/01 12:00:	检查 宣誓详情
		ELB健康状态检查	● 不合格	自动检查		1	弹性负载均衡 (Ela	2022/03/01 12:00:	检查 查看详情
		OBS桶服务端加密	● 不合格	自动检查		7	OBS服务端加密是	2022/03/01 12:00:	检查 查看详情
		日志指标过滤和告	● 不合格	自动检查		3	日志审计模块是信	2022/03/01 12:00:	检查 查看洋情
		□ 日志指标过滤和告	● 不合格	自动检查		3	日志审计模块是信	2022/03/01 12:00:	检查 查看详情
		ELB证书有效性检查	● 不合格	自动检查		1	弹性负载均衡 (Ela	2022/03/01 12:00:	检查 查看详情
		10 ▼ 总条数: 346 (	1 2 3 4	5 35 <b>&gt;</b>					

#### **图 9-11** 全部检查规范

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

#### 🛄 说明

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

----结束

#### 查看某个基线检查项目详情

🗋 说明

SA**基础版**和**标准版**暂不支持云服务基线查看详情功能。如需查看"风险资源列表","修复方 式"等详情信息,建议您<mark>购买专业版</mark>。

步骤1 登录管理控制台。

**步骤2** 在页面左上角单击 ── ,选择"安全与合规 > 态势感知",进入态势感知管理页面。 **步骤3** 在左侧导航栏选择"基线检查",进入基线检查页面。

文档版本 54 (2022-11-24)

步骤4 选择待查看检查项目的区域,并选择"检查规范"页签。

**步骤5** 在基线检查规范列表中,在待查看检查项目所在行的"操作"列,单击"查看详 情",系统进入检查项目详情页面。

冬	9-1	2 检查1	页目详情
---	-----	-------	------

检查规范检查资	ご涙	检查结果								
全部规范	8%	检查	全部 (346)	不合格 (16)	检查失败	(11)	待检查 (293)	合格 (26)	请输入检查	项名称搜索 C
安全上云合规检查1.0	24%	检查顶	检查状态↓Ξ	检查方式	检查分类	风险资源	Ξ 描述	最近检查	: 1≡	操作
等保2.0三级要求	96	主机防护状态	始査 🛛 不合格	自动检查		10	企业主机度	安全服务 2022/03	/01 12:00:	检查 查看详情
护网检查	63%	主机Agent状	添检查 ● 不合格	自动检查		10	企业主机委	安全服务 2022/03	/01 12:00:	检查 查看详情
		安全组入方向	列規则… ● 不合格	自动检查		8	安全组入方	5向规则 2022/03	/01 12:00:	检查 查看详情

步骤6 在检查项目详情页面,查看检查项目的详细信息。

查看该风险检查项的详细描述、检查提示和检查结果等。

#### 图 9-13 检查项目详情页面

	用户开启登录保护检查						
1 列表内	检查结果"不合格"资源可通过"加固建议"进行修复,修复完成后再次点击"检查"操作,可	可刷新检查结算	缺态				
检查状态	不會格	最近检查	2022/01/27 12:00:05 GMT+08:00		检查方式	自动检查	
风险螺纹	施性	影响	参考详细描述		规范与分类	【安全上云合规检查1.0】: 身份与议	的管理;
描述	在IAM的安全设置中息用登录保护后,登录时还需要通过透现MFA或短信或邮件验	检查过程	①使用管理员帐号登录管理控制台		相关资料	统一身份认证服务用户指南	
	证,再次确认整录者身份,进一步提高帐号安全性,有效避免钓鱼式攻击或者用户密		②在服务列表远择"管理与部署 > 统一身	合认证服务"(IAM)			
	荷意外泄漏,保护您安全使用云产品。		③在左侧导航栏中选择"安全设置"				
	检查在IAM的安全设置中是否开启整录保护。		③在新窗口中远择"歌感操作"页签				
			③检查"登录保护"是否为"已开启"				
检查	全部 (33) 不会悟 (33) 检查失败 (0)	合格 (0)					
3	· 资源关型	检查	加结果	最近检查	加困建议		操作
	b53 lam_user	•	不合格 ⑦	2022/01/21 00:00:04 GMT+08:00	请在IAM 景的安全 摄作方法 选择"安结 编辑按钮 证方式,	用户中开启整录保护,提高帐号整 性。 : 进入得微放IAM用户详情页面 > 论量"页签 > 单击"音频保护"后的 > 在理出边对话帽中选择登录的验 开启整录保护。	检查

----结束

# 查看检查资源列表

资料列表只展示已检查的资源。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果的区域。
- 步骤5选择"检查资源"页签,系统将显示当前区域所有检查资源以及其详细信息,如图 9-14所示。

检查	规范检查资源	检	查结果					
检查	资源列表为您展示日	验查的资	遼 全部 (148)	不合格 (79) 检	查失败 (O)	合格 (69)	请输入资源名称搜索	Q
	名称/ID ↓Ξ		资源类型	检查项 ↓=	风险项 」	=	操作	
	vpc-382d 42b3ce0t	:6	vpcs	6	5		检查 查看详情	
	SCC 963	lf85	iam_user	10	3 2		检查 查看详情	
	893f 893f	afe afe	security_group_rules	1	1		检查 查看详情	
	cef84 cef84	зб зб	security_group_rules	1	1		检查 查看详情	
	113c2 113c2	36 36	security_group_rules	1	1		检查 查看详情	
	6a8 6a8	21 21	security_group_rules	1	1		检查 查看详情	
	df57 df57	3-a2 3-a2	security_group_rules	1	1		检查 查看详情	
	d5be( d5be(	9-9a 9-9a	security_group_rules	1	1		检查 查看详情	
	a052bff a052bff	-750 -750	security_group_rules	1	1		检查 查看详情	
	cert- af17(	0897	elb_cei s	1	1		检查 查看详情	
10	▼ 总条数: 148 〈	1 2	3 4 5 15 >					

#### **图 9-14** 全部检查资源

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

#### ----结束

### 查看某个资源的检查详情

🛄 说明

SA**基础版**和**标准版**暂不支持云服务基线查看详情功能。如需查看"风险资源列表","修复方 式"等详情信息,建议您<mark>购买专业版</mark>。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查项目的区域,并选择"检查资源"页签。
- **步骤5** 在检查资源列表中,在待查看资源所在行的"操作"列,单击"查看详情",系统进入资源详情页面。

#### **图 9-15** 检查资源详情

检查	规范检查资源检查资源	查结果			
检查	资源列表为您展示已检查的资	<b>登線</b> 全部 (148)	不合格 (79) 检查	失败 (0) 合格 (69)	请输入资源名称搜索 Q
	名称/ID JΞ	资源类型	检查项 ↓Ξ	风险项 ↓=	操作
	vpc-382d 42b3ce0f-2aab-47b1-b1eb-e6	vpcs	6	5	检查 查看详情
	SCC_SA_h00536693 9635ca200c794ddc8a1804f85	iam_user	10	3 2	检查 查看详情

#### 步骤6 在资源详情页面,查看资源的详细信息。

查看该资源的检查项、检查状态、检查方式、最近检查时间等。

#### 图 9-16 检查资源详情页面

< vpc-				
检查		全部 (6)	不合格 (5) 检查	失败 (0) 合格 (1)
检查项	检查状态	检查方式	最近检查	操作
日志指标过滤和告答事件 (网络	● 不合格 ?	脚本自动检查	2021/06/24 10:06:43 GMT+08:	检查 查看详情
日志指标过滤和告警事件 (VPC	● 不合格 ?	脚本自动检查	2021/06/24 10:06:43 GMT+08:	检查 查看详情
日志指标过滤和告答事件(子网	• 不合格 ?	脚本自动检查	2021/06/24 10:06:44 GMT+08:	检查 查看详情
日志指标过滤和告答事件(安全…	• 不合格 ?	脚本自动检查	2021/06/24 10:06:44 GMT+08:	检查 查看详情
高危端口、远程管理端口暴露检	<ul> <li>合格</li> </ul>	脚本自动检查	2021/06/24 10:06:42 GMT+08:	检查 查看详情
日志指标过滤和告答事件 (VPN	● 不合格 ?	脚本自动检查	2021/06/24 10:06:44 GMT+08:	检查 查看详情

----结束

# 查看检查结果列表

🛄 说明

SA**基础版**和**标准版**暂不支持云服务基线查看检查结果功能。为及时了解云服务配置状态,以及 确保云服务的配置的合理性,建议您<mark>购买专业版</mark>。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果的区域。
- 步骤5 选择"检查结果"页签,系统将显示当前区域所有检查结果以及其详细信息,如图 9-17所示。

图 9-	17	全部检查结果
------	----	--------

检查规范 检查资源	检查结果				
检查	全部 (16	2) 不合格 (87)	检查失败 (5)	合格 (75)	请输入检查项名称搜索 Q
检查项	检查结果	资源类型	资源名称/ID	检查时间	操作
会全组入方向规则控制检	● 合格	security_group_rules	04dacbde-371c-4b15-8c 04dacbde-371c-4b15-8c	2021/06/24 10:06:27 G	检查 查看详情
安全组入方向规则控制检	● 不合格 ?	security_group_rules	0808f374-99b8-46eb-b2 0808f374-99b8-46eb-b2	2021/06/24 10:06:27 G	检查 查看详情
安全组入方向规则控制检	<ul> <li>合格</li> </ul>	security_group_rules	0968b7bd-cc8d-4b21-b6 0968b7bd-cc8d-4b21-b6	2021/06/24 10:06:27 G	检查 查看详情
安全组入方向规则控制检	<ul> <li>合格</li> </ul>	security_group_rules	09877856-1afe-413c-83 09877856-1afe-413c-83	2021/06/24 10:06:27 G	检查 查看详情
安全组入方向规则控制检	● 不合格 ?	security_group_rules	1051c3db-a1cc-43ba-83 1051c3db-a1cc-43ba-83	2021/06/24 10:06:28 G	检查 查看详情
安全组入方向规则控制检	• 不合格 ?	security_group_rules	10ac39f6-1192-42a1-bb 10ac39f6-1192-42a1-bb	2021/06/24 10:06:28 G	检查 查看详情
安全组入方向规则控制检	• 不合格 ?	security_group_rules	113c2adb-932c-4703-bf 113c2adb-932c-4703-bf	2021/06/24 10:06:28 G	检查 查看详情
安全组入方向规则控制检	<ul> <li>合格</li> </ul>	security_group_rules	116af999-f016-4ece-b7 116af999-f016-4ece-b7	2021/06/24 10:06:29 G	检查 查看详情
安全组入方向规则控制检	<ul> <li>合格</li> </ul>	security_group_rules	11aab6c0-12ba-41d4-9e 11aab6c0-12ba-41d4-9e	2021/06/24 10:06:29 G	检查 查看详情
安全组入方向规则控制检	• 不合格 ?	security_group_rules	12896741-e435-44a5-a 12896741-e435-44a5-a	2021/06/24 10:06:29 G	检查 查看详情
10 🔻 总条数: 162 < 1	2 3 4 5 1	7 >			

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

----结束

# 9.8 处理基线检查结果

本章节介绍如何根据修复建议处理风险配置,以及如何反馈检查结果。

### 前提条件

- 已购买态势感知**专业版**,且在有效使用期内。
- 已扫描云服务基线。

#### 修复风险项

以修复"IAM用户开启登录保护检查"的子检查项为例。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果的区域。
- 步骤5 在"检查规范"页签中,选择"安全上云合规检查1.0",查看子检查项风险状态。

### 图 9-18 子检查项风险状态

古教練知	基线检查		😔 1940 💊 4920E : 🛛 SECONDAR
安全報志 法原管理 业态分析 ·	(Sht	1965322 1987 3a	administration and an and a second and a sec
综合大群 成計音管			
展明若理 	e del (15)     ··     ··     T096     /·     ··	Zetwissing         Zetwissing           Ratio         0           Ratio         0	
**************************************		金娜 (76) 不合格 (21) 杜麗決気 (3) 将经3	E (34) 合語 (21) 語絵入絵表示名印绘表 Q
17182 * 8R06 *	安全上茶中段社園10         20%         位数段         位数段         日           -%         (ANUTA-FEBB2589142)         ● 不合地         0	200万パ 松田分支 単純現金 (1) 構成 100公司 単純現金 (1) 構成 10公司 単合 ゆうかけ管理 (2) 石(いいわかなか)	新設計会前 1世 昭和
· · · · · ·	57% 安全地入方共同进行社会 • 不会情 1		同应编号

- 检查状态图标呈绿色,则表示配置合格,不存在风险配置;
- 检查状态图标呈红色,则表示配置不合格,资产存在一定风险。
- **步骤6** 在"IAM用户开启登录保护检查"所在行的"操作"列,单击"查看详情",系统进入检查项目详情页面。
- 步骤7 查看风险详细信息,并根据"检查结果"和"帮助指导",修复风险点。

表 9-33 子检查项信息说明

参数名称	参数说明
检查状态	呈现当前检查项的检查状态。 <ul> <li>合格,提示当前子检查项配置合理,全部合格。</li> <li>不合格,提示当前子检查项配置可能不合理,并列表呈现 检查结果。</li> </ul>
最近检查	最近一次执行当前检查项的时间。
检查方式	当前检查项的检查方式。
风险等级	当前检查项出现问题所属的级别。
影响	当前检查项如果有问题将会带来的安全影响。
规范与分类	当前检查项所属的规范以及分类。
描述	当前检查项的具体检查内容。
检查过程	当前检查项的具体检查过程。
相关资料	子检查项涉及云服务配置手册指导。 单击引导链接,可直接跳转至详细手册指导页面。
检查资源	执行当前检查项所属的资源。 检查结果呈现检查合格和不合格两种。 • 合格,提示当前子检查项配置合理,全部合格。 • 不合格,提示当前子检查项配置可能不合理,并列表呈现 检查结果,单击"操作"列引导,可直接跳转至配置项管 理页面,进行安全风险修复。

步骤8 修复所有存在风险的配置后,可单击"检查",确认风险项是否已修复。

----结束

#### 反馈结果

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

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果所在的区域。
- 步骤5 在待反馈结果检查项目所在行的"操作"列,单击"反馈结果"。

图 9-19 反馈结果入口

检查规范检查资源	检查结果						
全部规范 (土) 安全上云合规检查1.0 12%	检查反馈结果	忽略 取消忽略			全部	• H	創入检查项名称搜索 Q
+ 等保2.0三级要求%	检查顶	检查状态 ↓Ξ	检查方式 🍞	风险资源 ↓Ξ	描述	最近检查↓日	操作
+ 护网检查 35%	机房场地应选择在具	<ul> <li>待检查 ⑦</li> </ul>	手动检查	0	检查您规划机房的地		反馈结果 宣香详情

步骤6 在弹出提示框中,选择反馈结果,并单击"确定"。

手动检查反馈结果			×
检查顶	描述	检查状态	
机房场地应选择在具有防	检查您规划机房的地址位	待检查	
反馈结果 〇 合格	○ 不合格		
① 反馈结果有效期为7天,	7天后请重新手动检查。		×
	<b>确定</b> 取消		

#### 图 9-20 反馈结果

🛄 说明

反馈结果有效期为7天,7天后请重新手动检查。

----结束

#### 忽略检查项

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

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

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"基线检查",进入基线检查页面。
- 步骤4 选择待查看检查结果所在的区域。
- 步骤5 在"检查规范"页签中,在待忽略子检查项的"操作"列单击"忽略"。

下图以忽略"SA专业版购买检查"的子检查项为例:

**图 9-21** 忽略检查项

检查规范 检查资源 检查结果									
<ul> <li>全部规范</li> <li>         ●          ●         ●         ●         ●         ●         ●         ●         ●         ●         ●         ●         ●          ●          ●          ●          ●          ●          ●          ●</li></ul>	检查反该结果	<b>SIG</b> 106534			全部	▼ SA	XQ		
+ 等保2.0三级要求%	🔽 检查顶	检查状态 ↓Ξ	检查方式 🍞	风险资源 ↓Ξ	描述	最近检查 ↓=	銀作		
+ 护网检查 35%	SA专业级购买检查	● 台格	自动检查	0	志数委托提供基础板	2022/06/25 06:01:11	松童 忽略 童香洋情		

如果您想批量忽略检查项,可以勾选所有需要忽略的检查项,然后在列表左上角,单 击"忽略"。

步骤6 在弹出的确认框中,单击"确定"。

#### **图 9-22** 确认忽略

确定要忽略当前的检	查项吗?		×
检查顶	描述	检查状态	
SA专业版购买检查	态势感知提供基础版、标	合格	
	确定取消		

#### 🛄 说明

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

----结束

# **10** 检测结果

# 10.1 查看全部检测结果

您可以在"全部结果"页面,获取安全状态的全视图,助您及时确定检测结果的优先 级,统筹分析安全趋势。

"全部结果"支持以下特性:

- 支持呈现威胁告警、漏洞、风险、合规检查、违法违规、时讯舆情等领域信息。
- 支持实时接收安全产品检测数据,实时更新结果列表。
- 支持按时间范围、过滤场景等筛选结果。默认呈现近7天内检测结果。
- 支持查看检测结果详情,以及JSON格式的结果详情。
- 支持自定义结果列表呈现的属性。
- 支持标识检测结果的处理状态。
- 支持威胁情报溯源。

## 约束限制

- 按过滤场景筛选检测结果,最多可呈现10000条结果。
- 仅可呈现近180天的检测结果。

### 前提条件

• 已接收到安全产品的检测结果。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"检查结果",进入全部结果管理页面。

态势感知	1	全部结果⑦						
安全看板		洗濯盆洗条▼ 緊认体振翻接受						0
综合大屏		开始日期 - 结束日期 - 結本 現金 22	高合 56 耳立 10K+				(2)路 标	
资产管理				( bade	-	0.00	- Contraction (1)	
威胁告答			/*重导致 ?	77.6:	产品名称	公司各称	友规时间	BRITE
漏洞管理		_ 题的始始 Scanner & Crawter	<ul> <li>1日175</li> <li>1日175</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	20時   初応2月15日 トタビ生
基线检查		或助告答 Scanner & Crawler	<ul> <li>揭示</li> <li>:</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	忽略   标记为线下处理
检测结果			<ul> <li>揭示</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	忽略   标记为线下处理
日志管理		威胁告誓 Scanner & Crawler	<ul> <li>→ 提示</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	忽略   标记为线下处理
安全产品集成		Scanner & Crawler	<ul> <li>● 提示</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	忽略 标记为线下处理
设置	•	Scanner & Crawler	<ul> <li>● 提示</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	忽略   标记为线下处理
网络安全	*	威胁告答 Scanner & Crawler	● 提示 (	未处理	WAF	Huawel	2020/10/10 1	忽略   标记为线下处理
主机安全	Ŧ	威胁告答 Scanner & Crawler	● 提示 :	未处理	WAF	Huawel	2020/10/10 1	忽略   标记为线下处理
赵用安全	,	_ 威胁告答 Scanner & Crawler	● 提示 :	未处理	WAF	Huawel	2020/10/10 1	忽略 标记为线下处理
安全管理	*	威胁告答 Scanner & Crawler	● 提示 :	未处理	WAF	Huawel	2020/10/10 1	忽略 标记为线下处理 (
		10 - 总祭数: 10,000 < 1 996 997 998 999 100	0 >					4
								(

#### 图 10-1 查看全部结果列表

步骤4 筛选查看检测结果。

- 在场景列框选择过滤场景,单击<sup>Q</sup>,即可查看到目标场景下检测结果。
- 当过滤后的结果仍较多时,可补充过滤条件和选择时间范围,快速查找结果。
  - 在筛选框补充过滤条件,添加一项或多项过滤条件,并配置相应条件属性, 单击Q,快速查找指定条件属性的结果。
  - 在时间过滤框中,选择检测结果发现的时间范围,单击"确认",快速查找 指定时间范围内的结果。

#### 步骤5 查看检测结果列表。

筛选后的列表,可查看满足条件的检测结果列表,以及结果统计信息。

#### 步骤6 查看检测结果详情。

1. 单击列表中结果的"标题",右侧滑出结果详情窗口。

#### 图 10-2 检测结果详情

17K U			结果详情	5						查看JSON
择筛选 ▼ 2	业务领域: 威胁告警	◎ 添加筛选组	基本信息							
			标题	Account weak	password					
22/09/03 17:28:52	- 2022/0×	(待处理总)	级别	中危	状态	未处理	时间	2022/09/10 01:31:2	7 GMT+08:00	
业务领域	标题	严重等级	业务领域	威胁告警	公司名称	Huawei	产品名称	HSS		
威胁告警	Account wea	• 中危	类别	attack/Abnorn	nalActions/Abnorr	nal Login				
威胁苦警	Account wea	• 中危								
威胁告警	Account wea	• 中危	描述							
威胁告警	Account wea	●中危	[{"pwc 3","pw cd281							3a23 e":"ro
威胁告警	Account wea	• 中危	ot","pwd_r	nax_days":null,"I	user_home_dir":nu	JU[}]				
威胁告警	Account wea	●中危	资源信息							
威胁告警	Account wea	●中危	资源名称		资源ID		资源类型		资源区域	
			C1	TEST	79'	380	af clo	ars	m .	
									20.88 标记	为线下外理

 查看与该结果相关的"基本信息"、"描述"、"资源信息"、"攻击信息"、 受影响的用户等信息,更多参数说明请参考表10-1。

#### 表 10-1 检测结果详情参数说明

参数	参数说明
基本信息	检测结果的基本信息,包括标题、级别、状态、时间、业务领 域、公司名称、产品名称、类别等信息。
描述	检测结果的简要介绍。
资源信息	受影响的资源信息,包括资源名称、资源ID、资源类型、资源区 域等信息。
租户信息	受影响的用户信息,包括租户ID、项目名称、项目ID、用户所在 区域等信息。
攻击源信息	攻击来源信息,包括攻击源IP、 <mark>查看威胁情报溯源</mark> 、攻击源端 口、经度等信息。
攻击目标信 息	攻击目标信息,包括攻击目标IP、攻击目标端口等信息。
相关检测结 果	相关联检测结果的信息,包括相关联资源名称、结果来源等信 息。
漏洞信息	漏洞结果信息,包括漏洞ID、CVSS分数、CVSS版本、提供方等 信息。
漏洞影响范 围	漏洞影响范围信息,包括影响版本、安全版本等信息。
合规检查信 息	合规检查基本信息,包括检查项、检查结果等信息。
涉及CVE	漏洞结果CVE编号。
参考链接/ 链接	结果相关参考链接。
修复建议/ 处置建议	结果修复或处置建议说明。

3. 单击"查看JSON",查看JSON格式检测结果详情。

----结束

# 查看威胁情报溯源

本部分介绍如何查看威胁情报溯源。

#### 前提条件

已启用产品集成,具体操作请参见<mark>启用产品集成</mark>。

#### 操作步骤

步骤1 进入目标检测结果的详情页面,在"攻击源信息"中,单击"威胁情报溯源"。

#### 图 10-3 威胁情报溯源

攻击源信息				
攻击源IP	威胁情报溯源	攻击源端口	经度	纬度
1 4	S		12 5	31 8

#### 步骤2 选择威胁情报分析平台。

#### **图 10-4** 分析平台

攻击源信息						
攻击源IP	威胁情报溯源	攻击源端口	经度		纬度	
18 4	S		12 '5	5	3	3
	请选择分析平台					
攻击目标信息	•安天:威胁情报综合分析平台	<b>ġ</b> ♂				
攻击目标IP	查看全部可集成产品	攻	击目标端口			
12 10		33	89			

**步骤3** 在弹出的确认框中,确认授权并单击"同意并立即前往",系统进入安天威胁分析平台。

首次登录需注册。

🗋 说明

安天分析平台在用户注册后,享受免费试用24小时。试用结束后,需要用户线下购买安天分析 能力服务,安天平台人工审核通过后,可继续享用该服务。

步骤4 查看威胁分析数据。

安天威胁分析示例如图10-5所示。

#### **图 10-5** 威胁分析数据



----结束

# 10.2 处理检测结果

当接收到检测结果后,您可标记结果处理状态。

- 忽略:如果确认该检测结果不会造成危害,在"忽略风险项"窗口记录"处理人"、"忽略理由",可标记为"已忽略"状态。
- 标记为线下处理:如果该检测结果已在线下处理,在"标记为线下处理"窗口记录"处理人"、"处理时间"和"处理结果",可标记为"已线下处理"状态。

#### 🛄 说明

由于SA中的检测结果汇聚了企业主机安全(Host Security Service,HSS )、DDoS高防 (Advanced Anti-DDoS,AAD )、Web应用防火墙(Web Application Firewall,WAF )等安 全防护服务上报的告警数据,因此,处理检测结果时须注意以下顺序:

- 1. 需先在SA检测结果详情页面查看来源。
- 2. 前往来源服务进行优先处理。
- 3. 处理后再到SA中来标记结果处理状态。

例如,告警显示来源产品名称为HSS,则需在HSS控制台上进行处理后,再在SA中进行标记处理。

前提条件

已接收到安全产品的检测结果。

操作步骤

- 步骤1 登录管理控制台。
- 步骤2 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"检测结果",进入全部结果管理页面。

图	10-6	处理检测结果
---	------	--------

态势感知	全部结果 ⑦			
安全看板				0
综合大屏	开始日期 箇 待处理总数 10K+ 数余 22 番	流 56 其它 10K+		忽略 标记为线下处理 🚺 🞯
资产管理	小袋做鸭 控制	严重集级 北赤	产品名称 公司名称	发现时间 编作
威胁告警	成防告答 Scaper & Crawler	• 揭示 未处理	WAE Huawei	2020/10/10 1 忽略 标记为线下处理
漏洞管理		- 49	MIT Hand	
基线检查	题的省誉 Scanner & Crawter	<ul> <li>通示</li> <li>未必埋</li> </ul>	WAF Huawei	2020/10/10 1 総略 初始の時後下型地
检测结果	威助告答 Scanner & Crawler	<ul> <li>提示 未处理</li> </ul>	WAF Huawei	2020/10/10 1 忽略   标记为线下处理
日志管理		● 提示 未处理	WAF Huawei	2020/10/10 1 忽略 标记为线下处理
安全产品集成	威胁告答 Scanner & Crawler	<ul> <li>提示 未处理</li> </ul>	WAF Huawei	2020/10/10 1 忽略   标记为线下处理
设置		<ul> <li>提示 未处理</li> </ul>	WAF Huawei	2020/10/10 1 忽略   标记为线下处理
网络安全	威胁告答 Scanner & Crawler	<ul> <li>提示 未处理</li> </ul>	WAF Huawei	2020/10/10 1 忽略   标记为线下处理
主机安全	威胁告答 Scanner & Crawler	<ul> <li>提示 未处理</li> </ul>	WAF Huawel	2020/10/10 1 忽略   标记为线下处理
MERCE .	威助告答 Scanner & Crawler	<ul> <li>提示 未处理</li> </ul>	WAF Huawel	2020/10/10 1 忽略   标记为线下处理
安全管理	威胁告答 Scanner & Crawler	<ul> <li>提示 未处理</li> </ul>	WAF Huawel	2020/10/10 1 忽略 标记为线下处理 (
	10 ▼ 总条数: 10,000 < 1 996 997 998 999 1000			4
				(

#### 步骤4 筛选检测结果。

文档版本 54 (2022-11-24)

步骤5 批量标记检测结果。

选择一个或多个"未处理"状态的结果,单击"忽略"或"标记为线下处理",对不同检测结果批量执行相应的处理操作。

步骤6 单个标记检测结果。

- 在结果列表对应"操作"列,单击"忽略"或"标记为线下处理",对单个检测 结果执行相应处理操作。
- 在结果详情窗口,右下角单击"忽略"或"标记为线下处理",对单个检测结果 执行相应处理操作。

----结束

# 10.3 导出检测结果

态势感知支持一键导出检测结果。

导出的excel文件中包含"产品名称"、"公司名称"、"受影响资源"、"业务领 域"、"标题"、"发生时间"、"发生次数"、"置信度"、"重要性"和"状 态"等信息。

约束限制

- 按过滤场景筛选检测结果,最多可导出10000条结果。
- 仅可导出近180天的检测结果。

前提条件

• 已接收到安全产品的检测结果。

操作步骤

步骤1 登录管理控制台。

**步骤2** 在页面左上角单击 — ,选择"安全与合规 > 态势感知",进入态势感知管理页面。 **步骤3** 在左侧导航栏选择"检测结果",进入全部结果管理页面。

#### **图 10-7** 导出检测结果

态势感知	全部结果 ⑦	全部结果 ⑦						
安全看板								
综合大屏		(中日期 (日) (西小陽台数 10K	* 数余 22 高分 56 夏立 10K+			勿許 标	记为终下处理	ସ ର
资产管理			T ECO ZZ IANG JO FRE TONY					~
威胁告答	业务领域	「「「「「「」」「「」」「「」」「「」」「「」」「「」」「「」」「「」」「」」	严重等级	状态 ア	"品名称 公司名称	发现时间	操作	
漏洞管理		Scanner & Crawler	● 揭示	未处理 W	VAF Huawei	2020/10/10 1	忽略   标记为线下处理	
基线检查		Scanner & Crawler	• 提示	未处理 V	VAF Huawei	2020/10/10 1	忽略   标记为线下处理	
检测结果		Scanner & Crawler	• 提示	未处理 V	VAF Huawei	2020/10/10 1	忽略   标记为线下处理	
日志管理	成肋告答	Scanner & Crawler	• 提示	未处理 W	VAF Huawei	2020/10/10 1	忽略   标记为线下处理	
安全产品集成	威胁告誓	Scanner & Crawler	● 提示	未处理 W	VAF Huawei	2020/10/10 1	忽略   标记为线下处理	
设置 	<ul> <li>威胁告答</li> </ul>	Scanner & Crawler	• 提示	来处理 W	/AF Huawei	2020/10/10 1	忽略   标记为线下处理	
网络安全	<ul> <li>或助告答</li> </ul>	Scanner & Crawler	• 提示	未处理 V	VAF Huawel	2020/10/10 1	忽略   标记为线下处理	
主机安全	<ul> <li>威胁告答</li> </ul>	Scanner & Crawler	● 提示	未处理 V	VAF Huawel	2020/10/10 1	忽略   标记为线下处理	
<u></u> 別 ( ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) )	威胁告答	Scanner & Crawler	● 提示	未处理 W	VAF Huawel	2020/10/10 1	忽略 标记为线下处理	
安全管理	↓ 威胁告答	Scanner & Crawler	● 提示	未处理 W	VAF Huawel	2020/10/10 1	忽略   标记为线下处理	©
	10 - 总祭	数: 10,000 < 1 996 997 998	999 1000 >					0
								0

步骤4 筛选检测结果。

**步骤5** 单击**亡**,一键导出筛选的检测结果列表,并以.csv格式文件保存在本地。 导出完成后,即可离线查看结果。

----结束

# 10.4 自定义结果列表

态势感知支持自定义检测结果列表。

# 前提条件

• 已接收到安全产品的检测结果。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知管理页面。 **步骤3** 在左侧导航栏选择"检测结果",进入全部结果管理页面。

#### 图 10-8 自定义结果列表

态势感知	全部结果 ⑦				
安全看板	「浅煤盆洗条▼ 数认种标题增表			0	
综合大屏		版 56 其它 10K+		日本 1000 1000 1000 1000 1000 1000 1000 10	
资产管理					
威胁告答	亚劳领域 标题	严重等级 状态 产品名	称 公司名称	友规时间 操作	
漏洞管理	_ 威胁告答 Scanner & Crawler	<ul> <li>● 揭示 未处理 WAF</li> </ul>	Huawei	2020/10/10 1 忽略   标记为线下处理	
基线检查	或助告答 Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawei	2020/10/10 1 忽略   标记为线下处理	
检测结果	戴助告答 Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawei	2020/10/10 1 忽略 标记为线下处理	
日志管理	Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawei	2020/10/10 1 忽略 标记为线下处理	
安全产品集成	威胁告答 Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawei	2020/10/10 1 忽略   标记为线下处理	
· · · · · · · · · · · · · · · · · · ·	威胁告答 Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawel	2020/10/10 1 忽略   标记为线下处理	
网络安全 🔻	威胁告答 Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawel	2020/10/10 1 忽略   标记为线下处理	
主机安全 •	威助告答 Scanner & Crawler	<ul> <li>● 提示 未处理 WAF</li> </ul>	Huawel	2020/10/10 1 忽略 标记为线下处理	
应用安全 ▼ ********	威胁告答 Scanner & Crawler	● 提示 未处理 WAF	Huawel	2020/10/10 1 忽略 标记为线下处理	
xx(株文主 * 中全管理 *	威胁告答 Scanner & Crawler	<ul> <li>提示 未处理 WAF</li> </ul>	Huawel	2020/10/10 1 忽略 标记为线下处理	o
Automa -	10 - 航年数 10.000 く 1 996 997 998 999 1000				0
					0
					B

- **步骤4**单击<sup>①</sup>,展开结果列表属性框。
- **步骤5** 勾选结果属性。
- 步骤6 刷新结果列表,即可在列表查看目标属性。

----结束

# 10.5 管理筛选条件

筛选条件用于筛选符合场景中过滤条件的结果,呈现匹配的结果列表。例如筛选条件 添加产品名称和资源类型两个条件,属性分别为"企业主机安全"和"云服务器", 则匹配的结果必须同时符合这两个条件属性。

目前可添加的条件及属性如下:

- 标题:检测结果的标题内容,可输入关键字。默认按标题搜索。
- 严重等级:检测结果的风险等级,包括"致命"、"高危"、"中危"、"低危"、"提示"。
- 业务领域:检测结果所属业务领域,包括"威胁告警"、"漏洞"、"合规检查"、"违法违规"、"风险"、"舆情"、"安全公告"。
- 状态:用户对检测结果的处理状态,包括"未处理"、"已忽略"、"已线下处理"。
- 资源名称:检测结果来源资源的名称,需输入资源名称。
- 资源类型:检测结果来源资源的类型,包括"云服务器"、"虚拟私有云"、 "安全组"、"弹性公网IP"、"磁盘"、"其他"。
- 公司名称: 检测结果来源产品所属公司,需输入公司名全称。
- 产品名称:检测结果来源安全产品,需输入产品名全称。

# 约束限制

- 一个筛选条件仅能包含一组"标题"关键字。
- 一个筛选条件仅能包含一个"资源名称"。
- 一个筛选条件仅能包含一个"公司名称"。
- 一个筛选条件仅能包含一个"产品名称"。

### 创建筛选条件

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ── ,选择"安全与合规 > 态势感知",进入态势感知管理页面。 **步骤3** 在左侧导航栏选择"检测结果",进入全部结果管理页面。

#### **图 10-9** 检测结果

态势感知		全部结果⑦											
安全看板		选择筛选条 ▼	默认按标题搜索									(	a
综合大屏		开始日期 一 结束	899	待处理总数 10K+	数命 22 高危	56 其它 10K+				忽略 标	记为线下	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	0
资产管理		业务领域	标题			严重等级	状态	产品名称	公司名称	发现时间	操作		
威胁告罄		威胁告答	Scanner & Crawler			• 提示	未处理	WAF	Huawei	2020/10/10 1	忽略	标记为线下处理	
漏洞管理		威胁告答	Scanner & Crawler			• 提示	未处理	WAF	Huawel	2020/10/10 1	忽略	标记为线下处理	
基线检查		威胁告警	Scanner & Crawler			• 提示	未处理	WAF	Huawel	2020/10/10 1	忽略	标记为线下处理	
松池端朱		成防衛部	Scanner & Crawler			<ul> <li>構示</li> </ul>	未处理	WAF	Huawel	2020/10/10 1	5285	标记为线下处理	
安全产品集成			Scanner & Crawler			• 提示	主が環	WAF	Huawei	2020/10/10 1	016	杨语为维玉纳理	
设置			Conner & Conder				+ 6128	WAE	Universit	2020/10/10 1	mag	ACCOLUMN TO ACCE	
网络安全	•		Scanner & Crawler			- 18-T	#302#	WAF	Huawer	2020/10/10 1	100.48		
主机安全			Scanner & Crawter			<ul> <li>12示</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	12/49	Read 7388E IN SECTED	
应用安全	*	威胁告答	Scanner & Crawler			<ul> <li>提示</li> </ul>	未处理	WAF	Huawei	2020/10/10 1	忽略	标记为线下处理	
数据安全		威胁告答	Scanner & Crawler			● 提示	未处理	WAF	Huawei	2020/10/10 1	忽略	标记为线下处理	<b></b>
安全管理	*	威胁告答	Scanner & Crawler			● 提示	未处理	WAF	Huawel	2020/10/10 1	忽略	标记为线下处理	0
		10 🔻 总条数	:10,000 < 1 9!	96 997 998	999 1000								
													B

步骤4 添加筛选条件。

- 在筛选框添加过滤条件,添加一项或多项过滤条件,并配置相应条件属性。
- 在时间筛选框中,选择时间范围。

步骤5 单击筛选框后"保存",弹出筛选条件保存窗口。

步骤6 配置筛选条件信息。

- 设置"场景名称",自定义筛选条件名称。
- (可选)勾选"设为默认筛选条件"。
- 步骤7 单击"确定",返回全部结果列表页面,即可在场景列框查看新建的筛选条件。

----结束

修改筛选条件

步骤1 登录管理控制台。

- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"检查结果",进入全部结果管理页面。
- 步骤4 在筛选条件列框,选择筛选条件。

**图 10-10** 保存筛选条件

步骤5 在筛选框后单击"编辑",弹出编辑窗口。

图 10-11 编辑筛选条件

编辑	筛选条件	×
名称	Test ✔ 设为默认筛选条件	
	<b>确定</b> 取消 删除	

步骤6 修改筛选条件名称。

步骤7 单击"确认",返回全部结果列表页面,即可查看已修改的筛选条件。

----结束

删除筛选条件

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知管理页面。
- 步骤3 在左侧导航栏选择"检查结果",进入全部结果管理页面。
- 步骤4 在筛选条件列框,选择筛选条件。

步骤5 在筛选框后单击"编辑",弹出编辑窗口。

#### 图 10-12 删除筛选条件

编辑	筛选条件	×
名称	Test ✓ 设为默认筛选条件	
	<b>确定</b> 取消 删除	

步骤6 单击"删除",返回全部结果列表页面,即完成筛选条件的删除。

----结束

# **11** 分析报告

# 11.1 创建安全报告

本小节主要介绍如何新建安全报告,以及通过复制已创建的报告快速创建报告。

# 约束限制

目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。

分析报告 Beta

- 仅**专业版**支持使用分析报告功能。
- 默认创建定期周报和月报各一个,可免费生成2期报告。专业版最多可创建12个安全报告,可多次生成报告。
- 支持创建周报、月报、自定义报告。
  - 周期报告:默认周报和月报,统计上一周或上一月安全信息。
  - 单次报告:可自定义季度报、月报、周报、日报等,分别按季度、月、周、 日等周期统计安全信息。

# 前提条件

已购买态势感知专业版,且在有效使用期内。

### 新建安全报告

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知 > 分析报告",进入安全报告 管理页面。

图 11-1	新建安全报告
--------	--------

态势感知	分析报告				🗊 历史报告
安全香板			THR		月报
综合大屏				_	_
资产管理		E			
威胁告警	+				
漏洞管理	创建报告	Weekly Report		Monthly Report	
基线检查		(A) 系统自动发送邮件(1)人	最近一期末发送	(A) 系统自动发送邮件 (1) 人	● 最近一期未发送
检测结果				<b>— — — —</b>	
分析报告			【 規制 曲座		90146 20179 #2149
日志管理	(a)/c		60.72		
安全产品集成					
设置 •		E.			
网络安全 •					
主机安全 🔹	On-Time Report	SA Report			
应用安全 🔻	春 手动触发发送邮件 (1) 人	4 手动触发发送邮件(1)人			
数据安全 🔻	-	-			
安全管理 🔹	编辑   复制   删除   编辑并发送报告	编辑   類制   删除   5	编辑并发送报告		

步骤3 单击"创建报告",跳转到报告基本信息配置页面。

# 图 11-2 配置报告基本信息

态势感知 / 分析报告 /	创建报告	基本信息	- ② 編輯内容	取消 下一步
* 报告名称	示例:安全态势报告			
报告类型	<ul> <li>● 尾級 (周一00.00-用日24.00)</li> <li>月級 (第一天00.00-最后一天24.00)</li> <li>● 単次</li> </ul>			
邮件发送方式	系统自动发送邮件 手动触发发送邮件			
邮件发送时间	每周- 00:00~06:00 ▼ 发送上周	报告		
* 邮件接收人		最多添加10个邮箱,当前:	0/10	
*报告汇报组织	示例:华为安全运维部			
汇报组织图标	示例 尺寸: 90·90 格式: PNG, JPG, JPG, SVG, G	IF		
	HOAWEI			0

步骤4 配置报告基本信息。

表	11	1-1	报告基本信息参数说明
---	----	-----	------------

参数	说明
报告名称	自定义报告名称,例如安全态势报告。
报告类型	<ul> <li>选择报告类型,可勾选"周报"、"月报"、"单次"。</li> <li>周报:默认统计上一周安全信息,上周一00:00到上周日24:00。</li> <li>月报:默认统计上一月安全信息,上月第一天00:00到上月最后一天24:00。</li> <li>单次:自定义选择时间范围,可统计一年、一季度、一月、一周、一天等安全信息。</li> </ul>

参数	说明
邮件发送方式	选择自动或手动发送邮件。
	<ul> <li>自动发送:定期自动发送安全报告,适用于"周报"和"月报"类型的报告。</li> </ul>
	<ul> <li>手动触发:手动触发发送安全报告,适用于需编辑报告小节内 容的报告。</li> </ul>
邮件发送时间	针对自动发送方式,需选择发送时间。
	● 默认可选择四个发送时间段。
	● "周报"默认为每周一发送上一周周报。
	• "月报"默认为每月一号发送上一月月报。
邮件接收人	添加邮箱地址,例如test@example.com。
	● 最多可添加10个邮箱。
报告汇报组织	自定义汇报组织,例如安全运维部。
汇报组织图标	单击"上传",上传组织图标。图标要求如下:
	● 尺寸90×90
	● 格式PNG、JPG、JPEG、SVG、GIF

步骤5 单击右上角"下一步",进入报告内容配置页面。

自定义报告内容。

- 勾选报告内容模块,可选择报告说明、报告总结、安全评分、资产风险、威胁告 警、基线风险、资产漏洞、后续规划等模块。
- 勾选"报告说明"、"自定义小结"、"后续规划"等模块后,需编辑小结内容。
- 步骤6 预览报告内容。
  - 1. 单击右上角"预览",预览自定义报告内容。
  - 2. 单击右上角"关闭预览",返回报告内容配置页面。
- 步骤7 单击右上角"保存",返回安全报告管理页面,即可查看创建的安全报告。

----结束

# 复制安全报告

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知 > 分析报告",进入安全报告管理页面。
- 步骤3 在已创建的安全报告模块,单击"复制",跳转到报告基本信息配置页面。

#### 图 11-3 配置报告基本信息

态势感知 / 分析报告 / 🔒	『建报告	1 基本信息	- ② 編輯內容	取消 下一步
* 报告名称	示例:安全态势报告			
报告类型	<ul> <li>● 周报 (周-00.00-周日24.00)</li> <li>● 月报 (第一天00.00-最后-天24.00)</li> <li>● 単次</li> </ul>			
邮件发送方式	系统自动发送邮件 手动触发发送邮件			
邮件发送时间	每周- 00:00~06:00 ▼ 发送上	周报告		
* 邮件接收人				
		最多添加10个邮箱,当前:	0/10	
*报告汇报组织	示例: 华为安全运维部			
汇报组织图标	示朝 HUAWEI 原造上後	GIF		• • • •

#### 步骤4 修改报告基本信息。

- 步骤5 单击右上角"下一步",进入报告内容配置页面,修改报告内容。
  - 1. 勾选报告内容模块。
  - 2. 重新编辑小结内容。
- 步骤6 单击右上角"预览",预览自定义报告内容
- 步骤7 单击右上角"保存",返回安全报告管理页面,即可查看新创建的安全报告。

----结束

# 11.2 发送安全报告

态势感知通过自动或手动方式发送报告到接收人邮箱,接收人收到报告邮件后,通过 报告"查阅/地址"可跳转到报告详情页面,查看或下载报告。

首次发送报告后,邮箱将收到"确认订阅"的邮件。确认订阅后,再次发送报告才会 收到报告查阅地址。

本小节主要介绍如何发送安全报告,包括自动发送报告、手动发送报告,以及如何发送历史报告。

# 约束限制

目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。

分析报告 Beta

安全报告发送的约束限制如表11-2所示。

#### 表 11-2 安全报告限制说明

报告类型	触发方式	是否支持多次编辑并发送			
单次报告	手动	支持			
周期报告	手动、自动 自动发送时,必须编辑接收人 邮箱地址、汇报组织、组织图 标等信息后,才能开启自动发 送。	仅支持编辑并发送一次			
历史报告	手动	不可编辑,支持多次发送			
所有报告一次最多可发送到10个邮箱。					

### 前提条件

• 已购买态势感知专业版,且在有效使用期内。

# 自动发送报告

定期发送的"周报"和"月报"创建完成后,默认状态为"已启用"。态势感知会在 设置的时间内,将安全报告自动推送到邮箱。

若后续不再需要推送该报告,可单击,切换报告状态为"未启用",关闭该报告的发送。

# **图 11-4** 关闭报告

	月报
安全态势月报	
(A) 系统自动发送邮件(1)人	
未启用	编辑   复制   删除

# 手动发送报告

手动触发发送的报告,在创建报告后,需编辑相关信息并

- 步骤1 登录管理控制台。

#### 图 11-5 手动发送报告

杰勒德知	八七四年				<b>1</b> 100-000
					E NARE
安全香板			JAHR		月报
综合大屏					_
资产管理		E			
威胁告警	+				
漏洞管理	创建报告	Weekly Report		Monthly Report	
基线检查		(A) 系统自动发送邮件 (1) 人	● 最近一副末发送	(A) 系统自动发送邮件(1)人	● 最近一期未发送
检测结果			ATTR CTALL INTO		ATTR COM INC.
分析报告			MITH 30.43 10.00	Cierti	WERN SCAL TERA
日志管理	<b>筆次</b>		單次		
安全产品集成		-	_		
设置 •					
网络安全 🔹					
主机安全 🔻	On-Time Report	SA Report			
应用安全 🔻	A 手动触发发送邮件 (1) 人	予 手动触发发送邮件(1)人			
数据安全 🔻					
安全管理 🔹	编辑   复制   删除   编辑并发送报告	编辑 复制	删除 编辑并发送报告		
安全管理					

步骤3 选择目标报告,单击"编辑并发送报告",跳转到报告内容配置页面。

#### 步骤4 编辑报告内容。

- 1. 勾选报告内容模块。
- 2. 重新编辑小结内容。
- 步骤5 单击右上角"预览",预览自定义报告内容
- **步骤6** 单击右上角"保存并发送邮件",返回安全报告管理页面,即可历史报告中查看发送记录。

----结束

## 发送历史报告

安全报告发送后,可在历史报告栏查看并发送历史报告。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知 > 分析报告",进入安全报告 管理页面。
- 步骤3 单击右上角"历史报告",展开历史报告列表。

#### 图 11-6 发送历史报告

#### 历史报告

全部	周报    月报	单次	统	计时间 开始日	日期 - 结束日期	Ħ
报告名称	统计时间	邮件发送方式	邮件发送时间	邮件接收人	操作	
一次性报告	2020/07/12~2021/01	1/07 手动触发发送邮件	2021/01/08 16	1	查看   下载   发送报告	
一次性报告	2020/07/12~2021/01	/07 手动触发发送邮件	2021/01/08 16	1	查看   下载   发送报告	
安全态势报告	2021/01/07~2021/01	1/07 手动触发发送邮件	2021/01/08 16	2	查看   下载   发送报告	
安全态势报告	2021/01/07~2021/01	/07 手动触发发送邮件	2021/01/08 16	2	查看   下载   发送报告	
安全态势报告	2021/01/07~2021/01	1/07 手动触发发送邮件	2021/01/08 16	2	查看   下载   发送报告	

×

步骤4 选择目标历史报告,在对应"操作"列单击"发送邮件",立即发送邮件。

🛄 说明

也可单击目标报告图标,进入报告详情页面,选择报告统计时间,再单击右上角"发送邮件", 立即发送邮件。

----结束

# 11.3 查看报告详情

本小节主要介绍发送报告后,如何查看历史报告详情。

### 约束限制

• 目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。

分析报告 Beta

• 成功发送一期报告后,才能查看历史报告详情。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知 > 分析报告",进入安全报告管理页面。
  - 图 11-7 查看报告列表

态势感知	分析报告		5 历史报告
安全香板		JUHR	月报
综合大屏			
资产管理			
威胁告警	+		<b></b>
漏洞管理	创建报告	Weekly Report	Monthly Report
基线检查		<ul> <li>(A) 系统自动发送邮件 (1) 人</li> <li>● 最近一期未发送</li> </ul>	<ul> <li>(A) 系统自动发送邮件 (1) 人</li> <li>● 最近一期未发送</li> </ul>
检测结果			
分析报告			
日志管理	<b>第次</b>	90	
安全产品集成			
设置 -			
网络安全 🔻			
主机安全 🔻	On-Time Report	S& Report	
应用安全 🔻	5 手动触发发送邮件 (1) 人	4 手动触发发送邮件 (1) 人	
数据安全 🔻	-	-	
安全管理 🔹	编辑 复利 曲除 编辑并发送报告	编辑   氯制   無除   编辑并发送报告	

**步骤3**选择目标报告,单击报告图标,跳转到最新一期报告详情页面。 查看最新一期发送的报告基本信息、报告内容、报告发送信息、报告发送状态等。 图 11-8 查看报告详情

滤鹅感知 / 分析报告 / SA Report	2021/01/07~2021/01/07 🔹		
报告类型 第次	邮件发送方式 平 <b>叶轴给</b> 给给###	邮件发送时间 2021/01/08 16:50:24 GMT+08:00	部件接收人(2人)
+~	TWIRKKARONIT	2021/01/00 10.30.24 001100.00	enumer.com,catecountre
08M	SA Re 2020/07/15-2	<b>port</b> 021/01/10	来自 态势感知(华为云) 2021/01/08 16:45:58 GMT+08:00 生成
一、本周期总结			
最新安全评分为0分,整体态路冲级为"致命",安全态势 1.无风险资产,资产继续状态良好。 2.系统无威胁告誓。 3.云服务基线共检查0项,通过率为0%,共有0项风险项	■		
本周期最新安全评分	本周期风险资产	总资产	本周期威胁告警
0 🕱	<b>0</b> r	0 个	<b>0</b> $\uparrow$
较上月 → 0分	较上月 → 0个	较上月 → 0个	较上月 → 0个
本周期漏洞	本周期基线风险	本周期威胁告警处理率	近2周期威胁告誓处理率
0 个	<b>0</b> $\uparrow$	0 %	0 %
较上月 → 0个	较上月 → 0个	-	-

**步骤4** 在"统计时间"框中,选择报告统计时间,可切换到其他历史报告详情页面,查看相应历史报告详情。

----结束

# 11.4 下载历史报告

报告发送后,态势感知支持下载的历史报告到本地。

本小节主要介绍如何下载历史报告。

# 约束限制

• 目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。

分析报告 Beta

• 默认支持下载pdf格式的报告。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ──,选择"安全与合规 > 态势感知 > 分析报告",进入安全报告 管理页面。
| 合析化         分析化         ① (111)           反总规则         (111)         (111                                      | 图 11-9                               | Ŧ     | 「载历史报告   |   |                           |  |   |
|--|--------------------------------------|-------|--|---|---------------------------|--|---|
| 支払報         通知時         通知時 </th <th>态势感知</th> <th></th> <th>分析报告</th> <th></th> <th></th> <th></th> <th>🗊 历史报告</th>               | 态势感知                                 |       | 分析报告   |   |                           |  | 🗊 历史报告  |
| Nitted         Network         Network         Montplageort           Nitted         Nit | 安全番板<br>综合大屏<br>资产管理<br>威胁告警         |       | +  | <b>E</b> G  | Renta                     |  | 月报  |
| 日志報道     (本)     (本)     (本)       安全市品集成     (本)     (本)     (本)       内陽安全     (本)     (本)     (本)       直前安全     (本)     (本)     (本)       白原安全     (本)     (本)     (本)       反開安全     (本)     (本)     (本)       反開安全     (本)     (本)     (本)       反開安全     (本)     (本)     (本)       反開安全     (本)     (本)     (本)       反生物道     (本)     (本)     (本)  | 漏洞管理<br>基线检查<br>检测结果<br>分析报告         |       | 山道根告   | Weekly Report           (2) 系統目动設述部件(1)人           〇〇 日島用 | ● 最近一期末发送<br>編輯   复射   删除 | Monthly Report<br>(A) 系統自动波送邮件 (1) 人<br>〇〇 已営用 | <ul> <li>最近一期本发送</li> <li>編辑</li> <li>編辑</li> <li>复制</li> <li>删除</li> </ul> |
| On-Time Report         SA Report           回用完全         合 非总能发发进版件 (1) 人         SA Report           数据完全         合 非总能发发进版件 (1) 人         合 非总能发发进版件 (1) 人           发生管理         小鍋目 发展   動像   病鍋目 光波   動像   病鍋目 光波振音         所編   放射   画像   病鍋目 光波振音  | 日志管理<br>安全产品集成<br>设置<br>网络安全<br>中机安全 | * * * |  | Ē.  | <b>#</b> X                |  |   |
|  | 应用安全<br>数据安全<br>安全管理                 | •     | On-Time Report           占 手術総定定送照件(1)人           編編 200 日前後 日前後日 編編并22回経告 | SA Report   | 田称   编辑并交送报告              |  |   |

### 步骤3 单击右上角"历史报告",展开历史报告列表。

### **图 11-10** 历史报告列表

历史报告						×
全部	周报 月报	单次		统计时间 开始	日期 - 结束日期	Ħ
报告名称	统计时间	邮件发送	的式 邮件发送时间	邮件接收人	操作	
一次性报告	2020/07/12~202	1/01/07 手动触发	支发送邮件 🛛 2021/01/08	16 1	查看   下载   发送报	ŧ
一次性报告	2020/07/12~202	1/01/07 手动触发	之发送邮件 🛛 2021/01/08	16 1	查看   下載   发送报	<b></b>
安全态势报告	2021/01/07~202	1/01/07 手动触发	支发送邮件 🛑 2021/01/08	3 16 2	童香   下載   发送报	±
安全态势报告	2021/01/07~202	1/01/07 手动触发	支发送邮件 🛛 2021/01/08	3 16 2	查看   下载   发送报	ŧ

步骤4 选择目标历史报告,在对应"操作"列单击"下载",跳转到报告详情页面。

### **图 11-11** 报告详情页面

漆鹅蛾斑 / 分析报告 / SA Report	2021/01/07~2021/01/07 👻		●本期报告已发送邮件 发送邮件 下戰
报告类型	邮件发送方式	邮件发送时间	邮件接收人 (2人)
単次	手动触发发送邮件	2021/01/08 16:50:24 GMT+08:00	@huawei.com;test@example
08M	SA Rej 2020/07/15-21	<b>port</b> 021/01/10	来自 态势感知(华为云) 2021/01/08 16:45:58 GMT+08:00 生成
一、本周期总结			
最新安全评分为0分,整体态数评级为"款命",安全态数5 1.无风险资产,资产健康状态良好。 2.系统无威胁告誓。 3.云服务基线共给童叹顶,通过率为0%,共有叹风险烦	L.白桃要如下:		
本周期最新安全评分	本周期风险资产	总资产	本周期威胁告誓
0 😚	<b>0</b> 个	0 个	<b>0</b> 个
较上月 → 0分	较上月 → 0个	较上月 → 0个	较上月 → 0个
本周期漏洞	本周期基线风险	本周期威胁告警处理率	近2周期威胁告警处理率
0 个	<b>0</b> $\uparrow$	0 %	0 %
	较上月 → 0个		

**步骤5** 查看历史报告,单击右上角"下载",将报告下载到本地。

### 🗀 说明

也可单击目标报告图标,进入报告详情页面,选择报告统计时间,再单击右上角"下载",下载 报告。

----结束

## 11.5 查看安全报告

本小节主要介绍态势感知生成的月报样例以及月报显示的信息。

### 前提条件

• 目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。



• 已下载安全月报。

### 安全月报样例

态势感知安全月报将显示当月的安全评分、整体态势、威胁告警等相关信息,具体信息如下图所示。

### 图 11-12 月报样例 1-本月总结

#### 一、本月总结

本月最新安全评分为72分,整体态势评级为"低危",本月安全态势重点摘要如下:

1,有风险的资产增加较为明显,增加了15个,约占总资产10%,其有中致命风险的资产数据占比36%,环比增加28%。资产风险中威胁告警占比较高,为整体的67%,需要强关注。

2、本月虱胁告警共有1485次,较上月增加12%。主要威胁攻击集中在DDoS、暴力破解、web攻击、后门木马,占总威胁攻击的85%,主要来源于日本及澳大利亚。 3、云殿务基线本月增加12枪宣项,通过率为79%,主要问题在身份认证、访问控制、日志审计和数据安全方面,主机基线不合格的主要是口令复杂度策略,32%的主机存在该问题。

4、漏洞个数本月有所上升,主机里面的致命漏洞占总漏洞的36%,需要重点关注最新的"宝塔面板未鉴权访问数据库漏洞",该漏洞在89%的主机中都存在。

本月最新安全评分	本月风险资产	总资产	本月威胁告警
<b>70</b> 分	<b>60</b> 个	148	1485
较上月 ↑ 10分	较上月 ↑10分	较上月 ↑ 10分	较上月 ↑ 10分
本月漏洞	本月基线风险	本月威胁告警处理率	本年威胁告警处理率
<b>167</b> ↑	<b>163</b> ↑	89%	92%
较上月 ↑ 10分	较上月 ↓ 10分	1485/1637	1485/1637

### 图 11-13 月报样例 2-安全评分





### 图 11-14 月报样例 3-资产风险







### 图 11-16 月报样例 5-基线风险





## 11.6 编辑安全报告

本小节主要介绍创建报告后,如何修改报告基本信息和报告内容。

### 约束限制

目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。

分析报告	Beta
------	------

- 报告类型不支持修改。
- 周期报告可修改报告名称、发送方式、发送时间、接收人、汇报组织、组织图标等信息。
- 单次报告可修改报告名称、接收人、汇报组织、组织图标等信息。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知 > 分析报告",进入安全报告管理页面。

### **图 11-18** 编辑安全报告

态势感知	分析报告				₿ 历史报告
安全番板			TRHR		月报
综合大屏					
资产管理					
威胁告警	+				
漏洞管理	创建报告	Weekly Report		Monthly Report	
基线检查		(A) 系统自动发送邮件 (1) 人	● 最近一期未发送	(A) 系统自动发送邮件 (1) 人	● 最近一期未发送
检测结果			(C28 (C24) (2014)		(C28   C24)   2044
分析报告			MUMBA (50,073) (20,047)		MI-18 (0,17) 4347
日志管理	<b>第次</b>		92/2		
安全产品集成			_		
设置 •					
网络安全 🔹					
主机安全 🔻	On-Time Report	SA Report			
应用安全 🔹	A 手动触发发送邮件 (1) 人	5 手动触发发送邮件 (1) 人			
数据安全 🔻					
安全管理 🔹	编辑   复制   删除   编辑并发送报告	编辑 复制	删除 编辑并发送报告		

步骤3选择目标报告,单击"编辑",跳转到报告基本信息配置页面。

### 图 11-19 修改报告基本信息

応勤感知 / 分析报告 /	编辑报告	<ol> <li>基本信息</li> </ol>	— ② 编辑内容	10月 下一步
* 招告实款	SA Report			
- 1011 Gev	Les report			
报告类型	原版 (周一00:00—周日24:00)			
	◎ 月报 (第一天00:00—最后一天24:00)			
	● 如次 2020/07/15 - 2021/01/10			
邮件发送方式	系统自动发送邮件 手动被发发送邮件			
	手动触发发送邮件运用于需在系统产生报告的基础上添加额外内容的场景			
邮件发送时间	手动发送			
* 節件接收人	@huawei.com  @ test@example.com  @			
		<b>星多滚加10个邮箱</b> ,当前:2/10		
* 报告汇报组织	O8M			
	75위 R寸: 90'90 HUAWEI HUAWEI			
	上傳			

- 步骤4 (可选)编辑报告基本信息。
- **步骤5** 单击"下一步",跳转到报告内容配置页面。
- 步骤6 (可选)勾选报告模块,自定义小结。
- **步骤7** 单击右上角"保存",返回安全报告管理页面。
  - ----结束

## 11.7 删除报告

本小节主要介绍如何删除报告。

### 须知

删除报告后,相应历史报告数据及记录也将被删除且不可找回,请谨慎操作。

### 约束与限制

目前分析报告功能处于公测(beta)阶段,如有问题,请联系华为云技术支持进行处理。

分析报告 Beta

### 操作报告

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ──,选择"安全与合规 > 态势感知 > 分析报告",进入安全报告 管理页面。
  - **图 11-20** 删除安全报告

志势感知	分析报告		₿ 历史报告
安全著板			JRH2 Fig
综合大屏			
资产管理			
威胁告警	+		<u> </u>
漏洞管理	创建报告	Weekly Report	Monthly Report
基线检查		<ul> <li>(A) 系統自动发送邮件 (1) 人</li> <li>最近一期相</li> </ul>	* 2 (2) 気気白动发送部件(1)人 ● 最近一期未发送
检测结果			
分析报告			
日志管理	92/2		(a)/2
安全产品集成			
20世 🔹			
网络安全 🔹			
主机安全 🔹	On-Time Report	S& Report	
应用安全 🔻	▲ 手动就发发送邮件 (1) 人	A 手討能发发送邮件 (1) 人	
数据安全 🔹			
安全管理 🔹	编辑   复利   删除   编辑并发送报告	编辑   氦制   删除   编辑并没3	送帰告

步骤3选择目标报告,单击"删除",弹出删除报告确认窗口。

图 11-21 删除报告确认

▲ 删除报告 您确认删除该报告吗?	×
是否	

**步骤4**单击"是",返回安全报告管理页面。

----结束

## **12**日志管理

通过授权对象存储服务(Object Storage Service,OBS)存储态势感知日志,帮助用 户轻松应对安全日志存储、导出场景,以及满足日志存储180天及集中审计的要求。

为应对SA日志的容灾恢复,将存储到OBS桶的日志,通过数据接入服务(Data Ingestion Service)传输到线下SIEM系统,恢复和离线管理SA日志数据。同时,可将 线下SIEM系统日志数据,通过DIS重新传输上云进行分析和存储。

### 门 说明

- DIS支持通过以下几种方式上传和下载数据: Kafka Adapter、DIS Agent、DIS Flume Plugin、DIS Flink Connector、DIS Spark Streaming、DIS Logstash Plugin等,详细说明请 参见使用DIS。
- 存储至OBS功能为Region级别功能。
- OBS独立收费,具体收费情况请以OBS服务为准。

### 前提条件

- 已购买专业版态势感知,且在有效使用期内。
- 操作账号权限检查。使用资源管理功能时,除了需要"SA FullAccess"、"SA ReadOnlyAccess"策略权限,还需要"Tenant Administrator"权限,请提前授 予操作账号对应权限。

"Tenant Administrator"权限配置详细操作请参见如何配置日志管理功能所需的权限。

### 创建日志存储至 OBS 桶

为满足安全审计日志存储180天要求,可将日志存储至OBS桶。OBS支持长久存储日志 数据,并支持在OBS控制台下载日志文件。

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知 > 日志管理",进入日志管理 页面。

步骤3 在"存储至OBS桶"栏中,单击 , 开启存储,如图12-1所示。

### 图 12-1 存储至 OBS 桶

存储至OBS桶	ă 🌒
提供态势感知日	日志存储功能,帮助用户轻松应对安全日志存储、导出场景,以及满足日志存储180天及集中审计的要求。
桶名称	obs-s 💌
对象名称	please input
存储路径	obs://ol
	确定 取消

### 步骤4 配置存储日志相关参数,具体参数说明如表12-1所示。

表12-1 配置存储日志参数说明

参数名称	参数说明
桶名称	选择已创建的OBS桶。 如果没有可选择的OBS桶,单击"您没有可用的OBS桶, 请前往创建",进入对象存储服务管理控制台,创建OBS 桶。 <b>说明</b> • 目前仅支持选择当前账号所在的区域中已有的OBS桶。 • 目前仅支持存储类别为"标准存储"和"低频访问存储"的 OBS桶。
对象名称	自定义对象名称。
存储路径	根据桶名称和对象名称生成的存储路径。

**步骤5** 单击"确定",完成配置。

配置成功后,日志将在大约10分钟后存储至OBS桶。

----结束

### 其他操作

若不再需要将日志存储至OBS,可在"存储至OBS桶"栏中,单击 , 关闭日志存储至OBS桶。取消后,显示如图12-2所示。取消后,已上传存储到OBS桶的日志数据不会被删除。

### **图 12-2** 取消存储

存储至OBS桶

提供态势感知日志存储功能,帮助用户轻松应对安全日志存储、导出场景,以及满足日志存储180天及集中审计的要求。

## **13** 产品集成

## 13.1 管理产品集成

态势感知通过集成安全防护产品,接入各安全产品检测数据,集中管理风险检测结 果。

目前默认支持以下产品/服务的集成管理:

- 企业主机安全(HSS)
- Anti-DDoS流量清洗(Anti-DDOS)
- Web应用防火墙(WAF )
- 云堡垒机(CBH)
- 容器安全服务(CGS)
- 漏洞管理服务(CodeArts Inspector)
- 安天威胁情报综合分析平台(TID)

### 🗀 说明

若需启用其他产品集成,请在"安全产品集成"页面,单击右上角"我要推荐",反馈相关产品 信息。

本小节主要介绍如何管理安全产品集成,包括启用和取消产品集成。

### 约束限制

- 需按区域分别启用或取消产品集成。
- 启用产品集成需账户具有"Tenant Administrator"角色。

### 启用产品集成

步骤1 登录管理控制台。

文档版本 54 (2022-11-24)

### 图 13-1 产品集成

态势感知	区域 华北北京一 华东上海二 华南,广州 华北北京四 华南,深圳 西南县	\$8- \$F.F	ē-	
安全看板				
综合大屏	全部     日集成 未集成     全部集成     支部集成     支部     支     支部     支	明代志	·             ·	QC
资产管理	4004 华为:企业主机安全	从未探测	华为: Anti-DDoS流量清洗	从未探测
威胁告答	HUAWEI 主机入侵检测 合规检测 主机源网检测		DDoSth#	
混词管理	企业主机安全服务(Host Security Service, HSS)是提升主机整 结果数量(个) 宣答 体安全性的服务、例け主机管理 风险预防 入侵险测 医吸防		Anti-DDoS流型漆洗服务(以下簡称Anti-DDoS)为公网IP提供四 结果数量(个)查看 到计局体DDoS放走的社体面对击中的快感得到。因时、Anti-DDoS	
基线检查	線、安全运営、网页防算改功能,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提上将主入侵行为,帮助企业均建服		可以總升用戶常說利用率,确保用户业务稳定运行。 转至联络主	
检测结果	务器安全体系,降低当前服务器面临的主要安全风险。 <b>终至服务</b> 主页		如何載成這服务?	
分析报告	如何集成京服务? • 购买服务: 去购买:		<ul> <li>购买服务:</li> <li>- 申末下布兼成开关的研 通信局否注注部包数或方法因此参考印:</li> </ul>	
日志管理	<ul> <li>点击右下角集成开关按钮,选择型百构该服务数据发送至应势感知;</li> </ul>		The second	
安全产品集成	Aller wertermaktum	从未探测	41 COM	从未探测
(CE *	4-1-3. Web应用防火機 Web应用防火機			
网络安全 🔻	Web应用防火塔 (Web Application Firewall, WAF),通过对 结果数量 (个) 宣誓		云虚曲机 (Cloud Bastion Host, CBH) 是华为云的一款44病一安 结果数量 (个) 宣誓	
主机安全 🔻	HTTP(5)寄使进行经通。设想所相联5Q(显人、雾站脚本双击,闲 近一小时:0 页示马上传。命令/代码注入、文件包含、做资文件访问、第三方 总量:0		全體理学術、方企URE例實中的新号 (Account)、語訳 近一小时:0 (Authorization)、认证 (Authentication)和审计 (Audit) 管 总量: 0	
应用安全 🔻	127日10年の時代に、COCUL、第25日に出る時、時日日本の1日年の1日年の1日年の1日日、1日 がWeb部分支全絶定。 1927年に注意時代		1000, Maleo IV	
数据安全 🔻	x1/19曲04/1809: - 购买服务: 志购买;		xx1+10m040fm80+: • 购买服务: 麦购买;	
安全管理 ▼	<ul> <li>所出右下角编成并关按钮,通缉造首将该服务数据发送至市场感知;</li> </ul>		<ul> <li>//出古下角集成开关按钮, 透耀地皆将谋服务数据发送至志的他们;</li> </ul>	
	40.4 华为: 重潮扫描服务	探测正常	40.4 华为: 容器安全服务	从未解测 🕤
	MUAWEI 漢明:法思好		NUAWEI 容器根像安全 容器安全策略 容器运行时安全	9
	識別問題服务 (Vulnerability Scan Service) 銀Web濃潤問題、资 产力会会保险制 動品目的第三大統心功能,自己的知識以前服务		容器安全服务 (Container Guard Service, CGS) 前修扫册服象中 結果数量 (个) 查看 於靈母山和兩信見,將動令沙輪為傳統安全的件子決得扣兩個环境	0
	器在网络中的安全风险,为云上业务提供多填虚的安全检测服务, 近一小时:0 满坦合规数求,让安全规电元所提出转至服务主员 总量:0		的问题:同时提供容器进程自名单、文件只读保护和容器迅速检测 近一小时:0 功能,有效防止音器进行时安全风险事件的发生。好至服务主页 总量:0	
	如何興成谅服务?		如何删成说服务?	
	<ul> <li>购买服务: 去陶实;</li> <li>点击右下角集或开关按钮, 运程是目梢该服务数据发送至多期感知;</li> </ul>	-	<ul> <li>则天服务: 去购买;</li> <li>// / / / / / / / / / / / / / / / / / /</li></ul>	

步骤3选择"区域"。

选择产品所在的区域,可选择"华北-北京一"、"华北-北京四"、"华东-上海 二"、"华东-上海一"、"华南-深圳"、"华南-广州"或"西南-贵阳一"。

步骤4 查询目标产品。

选择"未集成"筛选条件,查找符合条件的产品。更多查询方式请参见**查看产品集成** 列表。

步骤5 开启接收检测结果。

在目标产品列框,单击"开启集成",开启接收来自该产品的检测数据。

启用产品集成后,约5分钟后即可接收到产品上报的数据。

🛄 说明

为确保产品检测数据的正常接收,请确保已开启各产品相应防护功能。

----结束

### 取消产品集成

- 步骤1 登录管理控制台。

图 13-2 产品集成

态势感知	区域 华北北京一 华东。上海二 华南,广州 华北北京四 华南、深圳 西南,景	\$FE- 华东-1	<del>7</del> -	
安全番板				
综合大展	全部         已集成         未集成         全部集成员型          全部探訪	制状态	<ul> <li>▼ (清給入关地可提表)</li> </ul>	QC
		11 10 22 24 10		11-12-22-201
资产管理	华为:企业主机安全	100000	华为: Anti-DDos流量清洗	101010
威胁告答	HUAWEI 主机入侵检测 合规检测 主机漏洞检测		DDos款控	- II
通问管理	企业主机安全服务 (Host Security Service, HSS) 是提升主机整 結果数量 (个) 宣誓 体完全性的服务 通过主机管理 国际预防 入高标则 原因的		Anti-DDoS流量満法服务(以下簡称Anti-DDoS) 为公同IP提供四 結果数量(个) 宣香 新士局約DDoSで本形は約ITID本にお仕等時刊 同社 Anti-DDoS	- II
基线检查	線、安全运営、网页防蓄波功能、全面间别并管理主机中的信息资 这一小时:0 2023年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		可以提升用户带宽利用率,确保用户业务稳定运行。转至股务主    近一小时:0	- II
松测结果	广、吴町国现土町中的风险升相江市法人侵行为,約40匹至49座版 务器安全体系,降低当前服务器面临的主要安全风险。终至服务 		х	
04687#	主页 如何集成该服务?	_	如何集成浪服务? . BolTM2AS-	
Classical Control of C	<ul> <li>         ·</li></ul>		<ul> <li>州市和國政</li> <li>州市本下角集成开关按钮,选择是否将该服务数据发送至志物例扣;</li> </ul>	_
日志管理	* .m.1/2 11999800/1700012, 204420149980099004202230997804			
安全产品集成		从未探测		从未探测
()프 ·			ギカ: 太陸坐机	
网络安全 🔻	HUAWEI		HUAWEI	
	Web应用防火墙(Web Application Firewall, WAF),通过对 结果数量(个)宣誓 HTTP(5)请求进行绘测,记时间断SOL评入,激励制态攻击,网		云堡垒机 (Cloud Bastion Host, CBH) 是华为云的一款44統一安 結果数量 (个) 宣誓 全管神平台、为企业提供集中的新导 (Account) 、接収	
主机安全  ▼	页木马上传、命令代码注入、文件包含、敏感文件访问、第三方		(Authorization)、认证 (Authentication) 和审计 (Audit) 管 总量: 0	- II
应用安全 ▼	Web服务安全稳定,转至服务主页		38809, ME8051X	
数据安全 🔻	如何無成液酸等?		如何集成该额务?	
安全管理 🔻	<ul> <li>州大政57、支持大,</li> <li>点击右下角集成开关投田,选择是百得该服务数据发送至志势感知;</li> </ul>	_	<ul> <li>为大概5. 医内关,</li> <li>点击右下角集成开关按钮,选择是否将该服务数据发送至态物感知;</li> </ul>	_
				ų
	▲●●▲ 华为: 瀧洞扫描服务	探测正常	▲●●▲ 华为: 容器安全服务	从未穿到
	HUAWEI 漏洞已接服务		HUAWEI 容器摄像安全 容器安全策略 容器运行时安全	9
	漢附出機關务 (Vulnerability Scan Service) 集Web漢附出旗、资 結果数量 (个) 宣誓		容器安全服务 (Container Guard Service, CGS) 能够扫册服像中 结果数量 (个) 宣誓	٢
	产内容合规检测、器密码检测三大核心功能,自动发现网站或服务 器在网络中的安全风险,为云上业务提供多维度的安全检测服务,并用		的羅爾与配墨信息,帮助企业解决传统安全软件无法感知音器环境 的问题;同时提供容器进程白名单、文件只读保护和容器进造检测	B
	满足合坝要求,让安全路点无所遗形 <del>转至服务主</del> 页 总量: 0		功能,有效防止管器运行时安全风险事件的发生。 转至服务主页 总量: 0	
	如何興动浪छ吗?		如何興成這眼時?	
	<ul> <li>购买服务:去购买;</li> <li>/点击右下角集成开关按钮,选择是冒将该服务数据发送至态期感知;</li> </ul>		<ul> <li>购买服务:去购买;</li> <li>点击右下角集成开关按钮,选择是目传该服务数据发送至应购感知;</li> </ul>	

步骤3选择"区域"。

选择产品所在的区域,可选择"华北-北京一"、"华北-北京四"、"华东-上海 二"、"华东-上海一"、"华南-深圳"、"华南-广州"或"西南-贵阳一"。

步骤4 查询目标产品。

选择"已集成"筛选条件,查找符合条件的产品。更多查询方式请参见<mark>查看产品集成</mark> 列表。

步骤5 取消接收检测结果。

在目标产品列框,单击"关闭集成",取消接收来自该产品的检测数据。

----结束

## 13.2 查看产品集成

启用产品集成,并接入安全产品数据后,您可以管理集成列表,并可查看从产品接收 的统计结果数量。

### 查看产品集成列表

步骤1 登录管理控制台。

**步骤2** 在页面左上角单击 — ,选择 "安全与合规 > 态势感知 > 安全产品集成",进入产品 集成管理页面。

### 图 13-3 产品集成

ett		全部 已集成 未集成 全部集成类型	* 全部研究状态	• ⑦ 产品名	■ 请输入关键词投资	QC
10冊 18団		华为:企业主机安全	从未预测	华为: Anti-DDoS流量清洗		从未辨测
10		HUAWEI 主机入侵检测 合规检测 主机漏调检测		DDoSthip		- I
5理 2世		企业主机安全服务 (Host Security Service, HSS) 建银升主机塑 構築 体安全性如服务, 删试主机管理, 风险预验, 入碳检验, 凝极的 低, 安全证金, 用切动情况如此, 全级阳极时管理工作中的信息型 产, 实时运用主机中的创始并相,让专人保行为, 将加全的修整 后期一, 此此时也经常可能中非主要人的。他们都是	改量 (个) 宣告 NHJ: 0 0	Anti-DOoS流型清光服务(以下部附Anti-DOoS)为 到七层的DOoS双击防护和双击实时告智通知。同时 可以想升用户带宽利用率,确保用户业务稳定运行。 页	公阿IP提供四 <b>結果数量 (个) 查香</b> , Anti-DDOS 近一小时:0 時至服务主 总量:0	
课		10日本1日本55、1日本日本1日4500日1日日日本1日本4日、1日本500日 主義 ための第二十日本55		如何集成该服务?		
告		x1ml集成(kill)() ・ 购买服务: 去购买;		<ul> <li>购买服务:</li> <li>点由右下角集成开关按钮,选择是否将该服务数据</li> </ul>	魔发送至赤贽憾知;	
12		<ul> <li>点击右下角集成开关按钮,选择是目梢该服务数据发送至态势感知;</li> </ul>				- I
品集成			从未探测			从未探测
	•	华为:Web应用防火墙 Web应用防火墙		华方:云堡垒机 HUAWEI 云堡垒机		
£ \$	*	WebEI別的公理(Web Application Firewall、WAF),通过対 HTTPO 語表述行始過、空初相関部公共力、調知超率交流、同 近一づ 気が為した後、多時代観光人、数件包含、動気では内切り、第二つ を引い取りた。このた正、服務施設大的語等交流、保 WebEI影を今日表、整要を参すの	牧量(个) 宣誓 (NIJ: 0 0	云堡急机 (Cloud Bastion Host, CBH) 是华为云的 全管独平台,为企业提供集中的新号 (Account)、 (Authorization)、认证 (Authentication) 和审计 理能务。 统备服务主页	- 歌4A病-安 結果数量(个) 宣誓 接収 近一小时:0 ・ (Audit) 管 总量: 0	
全 뙈	-	20何儀或读服务? 购买服务:去购买; 然主右下角集成开关股田,选择是否将该服务数据发送至志势感知;		如何 <b>奧成该服务</b> ? • 购买服务: <u>去购买;</u> • 点击右下角集成开关按钮,远继是宫将该服务数3	戰從送至赤弱感知;	
		华为: 瀧洞扫描服务	探测止带	华为: 容器安全服务		MARSHARE CO
		HUAWEI 漏洞扫描服务		容器機像安全 容器安全策制	8 容器运行时安全	9
		識別注面服务(Vulnerability Scan Service) 無Web漏附注機、资 产内容合規定通、部時12度通二大核心功能。自定成現例和認識系 器件四等中中的全元段。力工止均常肥料。報酬的安全的限度等, 漏足合規要求、让安全和用形所證明。转至服务主页	牧量 (个) 宣告 NHJ: 0 0	容器安全服务(Container Guard Service, CGS) 能 的尾眼与配置信息,帮助企业解决将完全实际无法 的问题;同时提供穿器进程白各单、文件只遗居护和 功能,有效防止容器运行时安全风险事件的发生。	※13目前後中 協同部副研究 消落近後途別 完成第主式 規定の第二、 第二、 第二、 第二、 第二、 第二、 第二、 第二、 第二、 第二、	0
		如何 <b>贵成说服务</b> ? • 别玩服务: <u>去现天;</u> • 中古太下龟血中开关10月,洗纸用的滤试服备煮暖为惊砾态热味到;		如何 <b>奧成说服务</b> ?  • 別天服务: 去 <b>別</b> 天;  • 点本去下留集成开关时时, 选择是否适该服务数4	國发送至此時感到;	

步骤3选择"区域"。

选择产品所在的区域,可选择"华北-北京一"、"华北-北京四"、"华东-上海 二"、"华东-上海一"、"华南-深圳"、"华南-广州"或"西南-贵阳一"。

步骤4选择"集成类型"和"探测状态"。

集成类型分为"检测结果类产品集成"、"调查分析类产品集成"。 探测状态分为"探测正常"、"探测异常"、"从未探测"、"停止探测"。

步骤5选择"产品名称"、"产品类型"或"公司名称"筛选条件。

**步骤6** 在搜索框输入关键字,单击<sup>Q</sup>,即可查看到满足条件的产品。

----结束

### 查看产品集成结果

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知 > 安全产品集成",进入产品 集成管理页面。

### **图 13-4** 产品集成

- TETEK							
大屏	全部 已集成 未集成 全部集成类型	▼ 全部探測:	f态	• (?)	产品名称	<ul> <li>▼ 清箱入关键词搜索</li> </ul>	QC
방팬	华为:企业主机安全		从未研测	华为: Anti-DDoS	流量清洗		从未新测
告량	HUAWEI 主机入侵检测 合规检测 主机漏词检测			HUAWEI DDoS助护			
世辺	企业主机安全服务 (Host Security Service, HSS) 是提升主机整 体安全性的服务,通过主机管理、风险预防、入侵检测、高级防	結果数量 (个) 宣誓 近一小时: 0		Anti-DDoS流量清洗服务(以下窗称Anti 到七层的DDoS攻击防A和攻击实时告答	-DDoS) 为公网IP提供四 通知, 同时, Anti-DDoS	結果数量 (个) 宣香 近一小时: 0	
检查	個、安全运営、阿贝防算成功制,全面に例开管埋主利中的信息贷 产,实时运测主机中的风险并相止非法入侵行为,帮助企业构建服 各型本件任,即任他的风险并相止非法入侵行为,帮助企业构建服	总量: 0		可以超升用户常数利用率,确保用户业的 页	?അ定率行, 骑笙殿势王	总量: 0	
结果				如何集成该服务?			
<b>报告</b>	<ul> <li>NUN 集成248397</li> <li>购买服务: 去购买;</li> </ul>			<ul> <li>购买服务:</li> <li>点击右下角集成开关按钮,选择录音;</li> </ul>	专注服务数据发送至去的研	ED.;	
10月11日	<ul> <li>杰击右下角集成开列按钮,选择是否将该服务数据发送至应数感知;</li> </ul>						
产品集成	the survey of the second state		从未探测	1 (M - 840			从未探测
•	Web应用防火墙 Web应用防火墙			中方: 云塗塗机 HUAWEI 云虚金机			
72 ¥	Web应用防火塔(Web Application Firewall, WAF),通过对 HTTP/S)通常进行控制,记取进用MSO(注入,算法就本因于,图	結果数量 (个) 宣告		云堡垒机 (Cloud Bastion Host, CBH) 全管地平台、汚企业提供集中的新号 (A	是华为云的一款4A统一安 crount) 授权	結果数量 (个) 宣告	
段全 ▼ 쿥金 ▼	页水马上传、命令代码注入、文件包含、敏感文件访问、第三方 应用漏洞双击、CC双击、恶意能会归根、除沾清水的迷等双击、保 如从山秘经宁会展示。如果服务主用	近一小时:0 总量: 0		(Authorization) 、 认证 (Authenticat 理訳符。 特至服务主页	ion) 和审计 (Audit) 管	近一小时:0 总量: 0	
安全 💌	如何集成该服务?			如何集成该服务?			
B谜 ▼	<ul> <li>购买服务: 去购买;</li> <li>杰击右下角集成开关按钮,选辑是否将该服务数据发送至志数感知;</li> </ul>			<ul> <li>购买服务:去购买;</li> <li>//::</li> <li>/::</li> <li>/:</li> <li>/:<td>特该服务数据发送至志数感</td><td>0;</td><td></td></li></ul>	特该服务数据发送至志数感	0;	
	4/4, 353011128252		探测正常	44.0500A8	*		从未探测
	APP / 3. ABLART INNER/99 演員には最初分				95 第四十十章 1938年 - 1938年 - 1938年 - 1939年 - 19	打倒全	
	Web深刻泪痕影(Vulnerability Scan Service)复Web深刻泪痕、资	結果数量 (个) 宣告		容器安全服务 (Container Guard Servic	e, CGS) 能够扫描镜像中	結果数量 (个) 宣告	
	产内寄合规绘测、器密码检测三大核心功能,自动发现网站成服务 器在网络中的安全风险,为云上业务提供多缜查的安全检测服务,	近一小时:0		的運得与配置信息,帮助企业解决传统5 的问题;同时提供容器进程自名单、文件	E全软件无法感知容器环境 #只读保护和容器迅速检测	近小时:0	
	With continues of the case of the second second second second	725.88		1688 高速化化上的增速分子和中心中的复数	101-101-101-101-101-101-101-101-101-101	705-888- U	

步骤3选择"区域"。

选择产品所在的区域,可选择"华北-北京一"、"华北-北京四"、"华东-上海 二"、"华东-上海一"、"华南-深圳"、"华南-广州"或"西南-贵阳一"。

步骤4 查询目标产品。

选择"已集成"、集成类型和探测状态,查找符合条件的产品。更多查询方式请参见 查看产品集成列表。

步骤5 查看接收结果数量。

- 在目标产品列框,可查看从该产品的接收的全部和近一小时接收的结果数量。
- 单击"查看",可跳转到"全部结果"管理页面,呈现该产品的检测结果列表。
   更多检测结果说明,请参见查看全部检测结果。

图 13-5 查看产品上报数据

	华为:企业主机	安全		探测正常
HUAWEI	主机入侵检测	合规检测	主机漏洞检测	
企业主机安全(Ho 洞管理、基线检查 篡改等功能,帮助 足等保合规要求 轄	st Security Service 、入侵检测、程序) 企业更方便地管理 至服务主页	2) 是服务器则 运行认证、文 主机安全风险	结果数量(个)查看 件完整性校验,安全运营、网页防 ,实时发现黑客入侵行为,以及满总量:约6.46万	Ŧ
如何集成该服务?				
<ul> <li>购买服务: 去り</li> <li>点击右下角集成</li> </ul>	购买; (开关按钮,选择是	否将该服务数	据发送至态势感知;	

----结束

## 13.3 查看探测状态

"探测状态"是指安全产品数据上报到SA的状态。通过查看探测状态,您可以判断是 否正常上报当前产品数据。

文档版本 54 (2022-11-24)

### **表 13-1** 探测状态说明

状态	说明
探测正常	表示一个小时内,数据接口被调用次数大于等于8次,接口连通性正 常,"探测状态"检测正常,正常上报当前产品数据。 启用产品集成后一个小时内,默认探测状态为正常。
探测异常	表示一个小时内,数据接口被调用次数大于0次小于8次,接口连通性异 常,"探测状态"检测异常,不能正常上报当前产品数据。
停止探测	表示已停止上报当前产品数据。
从未探测	表示从未上报当前产品数据。

### 🛄 说明

探测正常状态判断原则:启用产品集成上报数据后,产品可每5分钟调用一次探测接口确认连通性。通过记录产品调用数据接口次数,判断探测健康状态。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知 > 安全产品集成",进入产品 集成管理页面。

### 图 13-6 产品集成页面

态势感知		区域 华北北京一 华东上海二 华南,广州 华北北京四 华南,深圳 西南县	第一 第五、	5-	
安全看板		▲ ▲ ▲ 本 本 本 本 本 本 本 本 本 本	04.m		
综合大屏			90.00		u c
资产管理		华为:企业主机安全	从未新期	华为: Anti-DDoS流量清洗	从未新潮
威胁告答		HUAWEI 主机入侵检测 合规检测 主机漏悶检测		HUAWEI DDositige	I
混词管理		企业主机员全服务 (Host Security Service, HSS) 思想开主机器 结果数量 (个) 查卷 体安全性的服务,通过主机管理,风险预防,入侵险制,高限防 的,也会一座,同型性性和环境,通常风险的化验检疫的原		Anti-DDoS资量清洗服务(以下部标Anti-DDoS)为公用P提供四 新七局的DDoS资量清洗服务(以下部标Anti-DDoS)为公用P提供四 新七局的DDoS资量清洗服务(以下部标Anti-DDoS) 近一小时:0	I
基线检查		後、安全巡告、內300時以60時、至兩位的打音進至60下的言語50 产,與时监測主机中的风险并阻止非法入侵行为,帮助企业构建服		10.0277日(14:04/04年),第66日(12576日221),第主統54工 总量: 0	
检测结果		务器安全体系,降低当期股务器面临的主要安全30%。 <b>终全服务</b> 主页		如何奧成说服务?	
分析报告		10何集成其限务? • 购买服务: 去购买;		<ul> <li>购买服务:</li> <li>//出本下角集成开关按钮, 选择是否将该服务数据改进至志数例如;</li> </ul>	
日志管理		<ul> <li>除出石下桶桶成并完成性, 选择定日有余能的数据及适金态制地和;</li> </ul>			
安全产品集成			从未探测		从未探测
195	•	本方: Web应用防火调 HUAWEI Web应用防火调		本の: 本語生死 HUAWEI 王虚金和	
网络安全	•	Web应用防火槽 (Web Application Firewall, WAF),通过对 结果数量 (个) 宣誓		云堡会机 (Cloud Bastion Host, CBH) 是华为云的一款14統一安 結果数量 (个) 宣誓	I
主机安全	Ť	THTPS/器使出版。世纪时指出研究已不见,就是方 近不马上传、命令代码起义、文件和全、频频文件均同、第二方 应用是影响先、CC双击、差频是世出推、除动语术的虚等攻击、俱 的体验和研究中心的一个。		全部空中局, AFEITERING (Autominity Amount)、moto (Autorisation)、以近に(Authentication)和新计(Audit)管 起量: 0 環際所,統全線务主要	
教課の会		2010年1月1日1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	_	如何集成读服务?	
安全管理	*	<ul> <li>购买服务: 去购买;</li> <li>: 出出石下角垂成并关设钮,选择型百符该服务数据发送至态势感知;</li> </ul>		<ul> <li>购买服务: 去购买;</li> <li>, 点击右下角曲或开关扳钮, 选择是当将该服务数据改适至态数感知;</li> </ul>	
			探测正常		从未探测 6
		45: 講演扫描服务			4
		HUAWEI (RATE HERON		HUAWEI 發酵開來文主 容器文主策略 容器运行时安全	G
		aminames。(Vulnerelikity Scan Service) 最Web爆制油瓶。资 产中音音相绘制。而新田园和三大场心力能。自由发现网站起服务 器石用用中的经生现合,为正上出导度中多峰值的安全组织的外。 通是合规要求、让安全和和天所激彩 转音服务主义		回器安全服务(Container Guard Service, CGS) 能够过程删除中 <b>结果安置</b> (个) 重著 的服用中国研究局,帮助企业和时候的完全软件无法的用中国环境 的回题。同时提供常器进程自然单、文件开述是非常容器建造绘力 功能,有效力止智器运行时安全现些明朴的发生。转至服务主贯	
		20何集成決戰時?		如何奧成波觀時?	
		<ul> <li>购买服务: 去购买;</li> <li>点击右下角集成开关投租,连组是目梢该服务数据发送至态势感知;</li> </ul>		<ul> <li>则天服务:去购买;</li> <li>病击右下角集成开关按钮,选择是習得该服务数据发送至必务感知;</li> </ul>	

步骤3选择"区域"。

选择产品所在的区域,可选择"华北-北京一"、"华北-北京四"、"华东-上海 二"、"华东-上海一"、"华南-深圳"、"华南-广州"或"西南-贵阳一"。

步骤4 在探测状态中,选择目标状态,即可呈现该状态的全部产品。

### 步骤5 在产品介绍栏,即可查看从该产品接收的数据量,以及该产品探测状态。

### 图 13-7 查看产品上报数据

HUAWEI	<b>华为:企业主机</b> 主机入侵检测	<b>ໄ安全</b> 合规检测	主机漏洞检测					探测正常
企业主机安全(1 洞管理、基线检 复改等功能,帮归 足等保合规要求	Host Security Servic 查、入侵检测、程序, 协企业更方便地管理 转至服务主页	e)是服务器则 运行认证、文 主机安全风险	站身安全管家,通过 件完整性校验,安 ,实时发现黑客入	过资产管理、漏 全运营、网页防 侵行为,以及满	4 1	<b>吉果数量</b> 丘―小时: 总量:	(个) 查看 0 约6.46万	
如何集成该服务	•							
• 购买服务: = • 点击右下角集	<mark>-购买;</mark> 成开关按钮,选择是	否将该服务数	如据发送至态势感知	П;				



# **14**<sub>设置</sub>

## 14.1 告警设置

### 14.1.1 设置告警通知

开启通知告警功能后,如果用户的资产受到了威胁,态势感知将会定时向用户发送提 示消息(短信或Email )。

### 前提条件

已购买态势感知标准版或专业版,且在有效使用期内。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择"安全与合规 > 态势感知",进入态势感知页面。
- **步骤3** 在左侧导航栏选择"设置 > 通知设置",并在设置页面,选择"告警设置 > 通知告警",进入告警通知设置页面。

### 图 14-1 告警通知设置页面

态势感知	设	置										\$	增加配额	
安全看板														
综合大屏	0	告警设置	授权设置	扫描任务										
资产管理	6	通知音響	青樹並拉设置											
威胁告答														
漏洞管理		1.告偿通知有可能 2.短信/邮件通知	8被当成垃圾信息而且 按满息通知服务规则	当我,如未收到告偿通 收费。	19日,请确认是否被拦截。									
基线检查														
检测结果		每日告答通知												
0K85		通知项目				告警等级					遭知时间			
カロ扱言		✓ DDoS ✓ 漏洞攻击	✓ 暴力破解✓ 暴力破解✓ 僅戶主机	<ul> <li>✓ Web攻击</li> <li>✓ 命令与控制</li> </ul>	✓ 后门木马✓ 异常行为	🔽 致命	☑ 高危	🔽 中危	🗹 低電	☑ 提示	10:00			
安全产品集成														0
RE 0 .		实时告警通知												9
通知设置 🕗		遵知项目				告警等级					遭知时间			0
检测设置		✓ DDoS ✓ 漏洞攻击	✓ 暴力破解✓ 暴力破解✓ 優户主机	✓ Web攻击 ✓ 命令与控制	<ul> <li>✓ 后门木马</li> <li>✓ 异常行为</li> </ul>	💟 数命	🗹 高忠	🖌 中態	- (HB	□ 揭示	24/J##     08:00 ▼	20:00 💌		

步骤4 选择重点关注的通知项目和告警等级。

### 每日告警通知

每日告警通知会在每天10:00向您发送告警通知消息。

选择关注的威胁告警和告警等级。只有当"通知项目"和"告警等级"同时有选 项被选中时,每日告警通知才能够生效。

• 实时告警通知

实时告警通知会在威胁告警发生后的整点时刻向您发送告警提示消息。

选择重点关注的威胁告警和告警等级。只有当"通知项目"和"告警等级"同时 有选项被选中时,实时告警通知才能够生效。

为了避免过多信息打扰您的日常工作,除了全天通知,您还可以选择仅在特定时 段发送实时告警通知。在通知时间栏选择"24小时"或指定时间段。

- 步骤5选择消息通知主题。
  - 通过下拉框选择已有的主题,或者单击"查看消息通知主题"创建新的主题,具体操作请参见创建主题。
  - 每个消息通知主题可添加多个订阅,并可选择多种订阅终端(例如短信、邮件等),详细订阅说明请参见添加订阅。

🛄 说明

在选择主题前,请确保您主题中订阅状态为"已确认",即当前订阅终端可用,否则可能 不能收到告警通知。

更多关于主题和订阅的信息,请参见《消息通知服务用户指南》。

步骤6 单击"应用",生效告警通知。

当关注的威胁攻击事件发生后,将收到来自手机短信、邮箱邮件的告警通知。

----结束

### 14.1.2 设置告警监控

用户可通过告警监控设置想要监控的告警信息,设置后态势感知将仅检测并推送关注的告警信息。

- 目前支持从"告警监控名单"、"告警监控类型和级别"及"监控的告警源"三个维度来设置监控信息。
  - · "告警监控名单"支持的格式为IP、IP:端口、IP/掩码或IP-IP,两条信息之间 以换行符相隔、不可重复,最多可包含50条。
  - "告警监控类型和级别"支持设置DDoS、暴力破解、Web攻击、后门木马、 漏洞攻击、命令与控制、异常行为、僵尸主机八大类告警类型,以及选择设 置致命、高危、中危、低危、提示全部类型告警等级。
  - "监控的告警源"支持设置接入的告警源,包括IDS、IPS、DDoS、HSS、WAF等。
- 设置告警监控后, "威胁告警"列表仅呈现同时满足设置条件的告警信息,重点 监控关注的威胁告警。告警监控设置仅对新上报的告警生效,不影响历史告警列 表的呈现。
- 默认不设置,态势感知将监控对资产所有的端口及IP的攻击,呈现所有资产威胁告警信息。

### 约束限制

- 需至少选择一类告警类型,每类告警类型下需至少选择一个告警等级,否则告警 监控应用无效。
- 需至少选择一种告警源,否则告警监控应用无效。

### 前提条件

已购买态势感知专业版,且在有效使用期内。

### 操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知页面。
- **步骤3** 在左侧导航栏选择"设置 > 通知设置",并在设置页面,选择"告警设置 > 告警监控 设置",进入告警监控设置页面。

### 图 14-2 告警监控设置页面

态势感知	设置						
安全看板							
综合大屏	音響设置 接权设置 扫描任务						
街产管理							
威胁告替							
漏洞管理	告警监控可设置关注的告答信息,设置告警监控后态势感知将检测以及统计这些告答信息。						
基线检查	告警监控名单 ②						
检测结果	如果不设置告智监控名单,则默认监控针对资产所有的端口及IP的攻击。						1
分析报告	设置项	操作					
日志管理	告智监控名单	设置名单					
安全产品集成	告警监控的关型和级别 ⑦						-
RT 1							0
通知设置 🕗	週知项目 	告警等级	_	_		-	8
检测设置	DDoS	⊻ 設命	▶ 高度	₩ 中地	1任范		
网络安全 💌	□ 親力破解	💟 致命	🔀 高彦	🔽 中危	□ 低電	提示	

#### 步骤4 设置告警监控名单。

在"告警监控名单"区域下,单击"设置名单",弹出"告警监控名单"窗口,导入 或手动设置监控名单。

设置告警监控来源名单的方法如下:

1. 导入监控名单。

单击"添加文件",选择需要导入的监控名单文件,文件支持txt格式,导入后监 控名单会自动呈现在输入框内。

2. 在输入框中输入符合格式的监控名单。

如<mark>图14-3</mark>,若设置了22和3389 端口以及IP10.1.1.1,态势感知将只展现来自于这些IP/端口的告警信息。

- 同步安全组策略。
   单击"同步安全组策略",可直接将安全组同步到监控名单,同步后监控名单会 自动呈现在输入框内。
- 4. 单击"确定",完成监控名单的设置。

图 14-3 告警监控名单

告警监控名单	×
✓ 设置告警监控来源IP名单后,态势感知将只展现针对名单IP攻击的告警信息。	
导入告答监控名单 ?	
请选择导入的文件,支持txt格式 添加文件	
请输入IP、IP:端口、IP/掩码或IP-IP,并以换行符相隔,不可重复,最多可输入50个。 ?	
0.0.0.0/0:3389 0.0.0.0/0:22 10.1.1.1	
同步安全组策略	
确定取消	

步骤5 设置告警监控的类型和级别。

在"告警监控的类型和级别"区域下,勾选需监控告警类型的"通知项目"和"告警 等级"。未勾选的"通知项目"和"告警等级",相关告警类型将不会被监控。

设置成功后将仅监控关注类型和等级的告警信息。

图 14-4 选择通知项目和告警等级

告警监控的类型和级别 ⑦					
通知项目	告警等级				
☑ DDoS	🔽 致命	▶ 高危	🗹 中危	🗹 低危	☑ 提示
☑ 暴力破解	🔽 致命	✓ 高危	🖌 中危	🗹 低危	✔ 提示
✔ Web攻击	🔽 致命	✓ 高危	🖌 中危	🗹 低危	✔ 提示
☑ 后门木马	🔽 致命	▶ 高危	🗹 中危	🗹 低危	✔ 提示
▼ 漏洞攻击	🔽 致命	▶ 高危	🗹 中危	🗹 低危	✔ 提示
▼ 命令与控制	💟 致命	▶ 高危	🗹 中危	🗹 低危	☑ 提示
✔ 异常行为	🗹 致命	✓ 高危	🗹 中危	🗹 低危	✔ 提示
☑ 僵尸主机	☑ 致命	▶ 高危	🗹 中危	🗹 低危	✔ 提示

步骤6设置监控的告警源。

在"监控的告警源"区域下,勾选需监控的告警源的"通知项目"。 设置成功后将仅监控关注来源的告警信息。

### 图 14-5 选择通知项目

监控的告警源 ?					
通知项目					
🗹 IDS 🕜	IPS 🕐	V DDoS	🔽 主机	WAF	日志分析
应用					

步骤7 单击"应用",3~5分钟后告警监控配置将生效。

----结束

## 14.2 授权设置

### 14.2.1 主机授权

只有经过授权的主机,态势感知才能对其执行漏洞扫描。请在添加主机后,使用此功 能对Linux或Windows主机进行授权。

目前Linux主机授权可通过"SSH账号登录"和"授权脚本执行"两种方式,而Windows主机授权通过关联"Windows账号登录"方式。

### 前提条件

• 已在"漏洞扫描服务 > 资产列表"中完成"添加主机"操作。

### 操作步骤

- **步骤1** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知页面。
- **步骤2** 在左侧导航栏选择"设置 > 通知设置",并在设置页面选择"授权设置 > 主机授权",进入主机授权设置页面。

### 图 14-6 主机授权设置页面

态势感知	设置				S 4772 :	12106280
安全着板	8					
综合大屏	告警设置 授权设置 扫描任务					
资产管理	主机振权 日志振权					
威胁告誓						
漏洞管理	接权账号:输入您的账号,以便VSS能登录您的机器。	为您的主机进行黨兩扫描以及導保合規配置项检测導服务。				
基线检查	批量配置接权信息					
检测结果		101614	増れ収益米利	160000 HA		
分析报告		IF AGAE.	1011-3PO409Call	DOMPSE DOF		
日士管理	ecs-SA日志!	1	linux	2 83	度权信息   解除授权	
安全产品集成	ccs-78 14	19 9	Unux	智未配置 配置	接权信息   解除接权	0
	ecs-	1 1	linux	智未配置 配置	授权信息   解除授权	9
1 300 cm (2)	ecs-l	1 2	linux	「「「「「」」 「「」」 「「」」 「「」」 「」 「」 「」 「」 「」 「」	授权信息   解除授权	0 Ri
检测设置	ecs-M	1	Unux	智未配置 配置	接权信息 解除接权	

步骤3 单击待配置主机"操作"列的"配置授权信息"。

如果需要同时为多个主机授权,请勾选各个主机前的勾选框,单击主机列表上方的 "批量配置授权信息"。

步骤4 对Linux和Windows操作系统,分别选择相应授权方式进行主机授权。

- Linux操作系统: SSH账号登录
- Linux操作系统:授权脚本执行
- Windows操作系统: Windows账号登录
- 步骤5 单击"确定",完成主机授权。

授权成功后,可在主机授权列表,查看对应主机的已授权信息。

🗀 说明

脚本执行授权成功后,在主机授权列表页面,暂时不能显示已授权信息,仅能通过脚本运行结果 验证授权成功与否。

----结束

### Linux 操作系统: SSH 账号登录

步骤1 在弹出的"配置授权信息"窗口中,选择"方法一: SSH账号登录"。

图 14-7 选择 SSH 账号

🔒 您可通过SSH	授权 , 或者执	行授权脚本,来授权服务访问》	欧的主机		
方式一:SSH账	号登录	方式二:授权脚本执行			
SSH授权登录方式	<ol> <li>选择已有</li> </ol>	≒SSH授权 ○ 创建SSI	H授权		
选择已有SSH账号	2		•		
	2	🖉 编辑 词 删除			
	登录端口	2			
	登录方式	密码登录			
	用户名	root			

步骤2 在下拉框中选择已有的SSH账号。

步骤3 单击"确定",完成Linux主机授权。

授权成功后,可在主机授权列表,查看对应主机的已授权信息。

### 🗀 说明

- 若无可用SSH账号,需首先创建SSH账号。
   单击"创建SSH账号",账置SSH账号信息,具体参数说明参考表14-1。设置完成后,单击 "确认",即可使用该账号对主机授权。
- 若需要修改已有SSH账号,单击"编辑",修改账号信息。
- 若需要删除已有SSH账号,单击"删除",删除账号。

### 图 14-8 账建 SSH 账号信息

配置授权信息				
1 您可通过SSH授权,或者执行授权脚本,来授权服务访问您的主机				
方式一:SSH账	号登录 方式二:授权脚本执行			
SSH授权登录方式	○ 选择已有SSH授权			
SSH账号别名		]		
登录端口		]		
选择登录方式	密码登录    ▼	]		
选择加密密钥	kps/default_cn-north-1	创建密钥		
Root权限是否加固				
sudo用户名	root			
sudo密码		加密保存⑦		
	确定取消			

### **表 14-1** 参数说明

参数名称	参数说明
SSH账号别名	自定义SSH账号名称。
登录端口	SSH账号登录的端口号。
选择登录方式	选择登录方式。可选择:"密码登录"或"密钥登录"。 选择"密钥登录"时,需要"创建私钥"。
选择加密密钥	选择已有的加密密钥,或者单击"创建密钥",创建新的密 钥,具体方法请参考 <mark>创建密钥</mark> 。
Root权限是否加 固	打开该权限后,不可以用root账号直接登录,而是只能通过普 通用户登录,然后才能切换到root用户。
sudo用户名	默认为root。

参数名称	参数说明
sudo密码	设置sudo用户对应的密码,单击"加密保存",对密码进行加密保存。

----结束

### Linux 操作系统:授权脚本执行

- 步骤1 在弹出的"配置授权信息"窗口中,选择"方法二:授权脚本执行"。
- 步骤2 单击右侧的"复制",复制开通授权的命令。
- 步骤3 使用远程管理工具(例如: "Xshell"、"SecureCRT"、"PuTTY"),通过弹性IP 地址登录到待开通授权的弹性云服务器。

也可使用弹性云服务器的"远程登录"功能,登录弹性云服务器。

步骤4 执行复制的命令(这里用"SecureCRT"工具登录)。

提示"Install Success"时则执行成功,完成Linux主机授权。

🛄 说明

脚本执行授权成功后,在主机授权列表页面,暂时不能显示已授权信息,仅能通过脚本运行结果 验证授权成功与否。

# curl -O -s http://XX.XX.XX/southchina-vss-hostscan/vss\_hostscan\_427c\_install.sh && bash vss\_hostscan\_427c\_install.sh --start [INFO] Uninstall Success [INFO] Create vss\_hostscan\_55e9 account [INFO] Grant sudo privileges for vss\_hostscan\_55e9 [INFO] Inject SSH Public Key [INFO] Install Success

----结束

### Windows 操作系统: Windows 账号登录

- 步骤1 在弹出的对话框中,选择已有Windows账号。
- 步骤2 单击"确定",完成Windows主机授权。

授权成功后,可在主机授权列表,查看对应主机的已授权信息。

### 图 14-9 配置授权信息

配置授权信息	
windows授权登录方式	● 选择已有windows授权 ○ 创建windows授权
选择已有windows账号	▼
	1 夕 編辑 ① 删除 密码登录 用户名 Administrator
	确定取消

### 🗀 说明

- 若无可用Windows账号,需首先创建Windows账号。
   单击"创建Windows账号",配置Windows账号信息,具体参数说明参考表14-2。设置完成后,单击"确认",账可使用该账号对主机授权。
- 如果需要修改已有Windows账号,单击"编辑",修改号信息。
- 如果需要删除已有Windows账号,单击"删除",删除账号。

### 图 14-10 创建 Windows 账号

配置授权信息					
windows授权登录方式 〇 选择已有windows授权 <ul> <li>创建windows授权</li> </ul>					
windows账号别称					
选择加密密钥	kps/default_cn-north-1	创建密钥			
用户名	Administrator				
密码					
账号域	如CHINA , 可为空				
	确定取消				

### **表 14-2** 参数说明

参数名称	参数说明
Windows账号别称	自定义Windows账号名称。
选择加密密钥	选择已有的加密密钥,或者单击"创建密钥",创建新的密 钥,具体方法请参考 <mark>创建密钥</mark> 。
用户名	默认为Administrator。
密码	Windows系统登录密码。
账号域	查看该Windows系统的账号域并填写到此处,该参数也可 以为空,不填写。

----结束

## 14.3 启动主机扫描任务

在对主机授权后,可以参考此章节启动主机漏洞扫描和主机基线扫描任务。

### 前提条件

- 已购买态势感知**专业版**,且在有效使用期内。
- 已在"漏洞管理服务 > 资产列表"中完成"添加主机"操作。
- 已在"态势感知 > 设置 > 通知设置 > 授权设置 > 主机授权"中对主机完成授权。

### 🛄 说明

为了确保扫描成功,在开启主机扫描前,请先完成以下操作。

- 1. 完成**主机授权**。
- 2. 如果主机所在的安全组设置了对漏洞管理服务(CodeArts Inspector )的访问限制,请参见**如何解决主机不能访问**添加策略允许CodeArts Inspector的IP网段访问您的主机。
- 3. 如果用户同时使用了**主机安全服务**,参见配置SSH登录IP白名单将您的主机IP配置为白 名单。否则,主机IP会被当成不信任IP被**主机安全服务**拦截,造成扫描任务失败。

### 背景信息

在使用态势感知的**主机漏洞扫描**功能时,请参考如下使用流程:

- 1. 添加主机:请在"漏洞管理服务 > 资产列表"中完成。
- 主机授权:请在"态势感知 > 设置 > 通知设置 > 授权设置 > 主机授权"中完成。
- 启动扫描任务:请在"态势感知 > 设置 > 通知设置 > 扫描任务"中执行。请参考本章节执行。
- 4. 查看主机漏洞扫描结果:请在"态势感知 > 漏洞管理 > 主机漏洞"中查看。
- 5. 查看主机基线数据:请在"态势感知 > 检测结果"中查看。

### 操作步骤

步骤1 登录管理控制台。

- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知页面。
- **步骤3** 在左侧导航栏选择"设置 > 通知设置",并在设置页面选择"扫描任务"页签,进入 扫描任务设置页面。

### 图 14-11 扫描任务设置页面

态势感知	设置			STRUCTURE : STALES (S)
安全看板				
综合大屏	告替设置 授权设置 扫描任务 8			
资产管理	主机漏洞扫描&主机基线检测			
威胁舌管	① 扫描和检测能力由展用扫描服务提供, 请前往 展用扫描	服务 查看洋信		
漏洞管理				
基线检查	主机名称	IP地址	上一次扫描时间	扫描状态
检测结果	ecs-e15 BJ1	1 96	2020/09/30 11:51:28 GMT+08:00	<ul> <li>已失敗</li> </ul>
分析报告	ecs-	15 )	2020/09/30 11:51:28 GMT+08:00	<ul> <li>已失败</li> </ul>
日志管理	ecs-M //s	15 .0	2020/09/30 11:51:28 GMT+08:00	
安全产品集成	ecs1	1: )	2020/09/30 11:51:28 GMT+08:00	• B%%
	ecs-sa- }	1 10	2020/09/30 11:51:28 GMT+08:00	• Exp
通知设置 松潤设置	5 × 思想就:105 < 1 2 3 4 5	_ 21 >		ß
网络安全	开始扫描 一級同步			

- 步骤4 在"主机漏洞扫描&主机基线扫描"栏下,单击"一键同步",同步当前账号下的弹性服务器IP信息,刷新"IP地址"列表。
- **步骤5** 在"主机漏洞扫描&主机基线扫描"栏下,选择需要执行扫描的主机,单击"开始扫描",启动扫描任务。

"扫描状态"为"已完成"时,可在"态势感知 > 漏洞管理 > 主机漏洞"和"态势感 知 > 检测结果"查看详细扫描结果。

----结束

## 14.4 检测设置

使用云服务基线相关功能时,需要先参考本章节设置检查计划。

操作步骤

- 步骤1 登录管理控制台。
- **步骤2** 在页面左上角单击 ,选择 "安全与合规 > 态势感知",进入态势感知页面。
- 步骤3 在左侧导航栏选择"设置 > 检测设置",进入检测设置页面。

### 图 14-12 检测设置

ち動感知	检测设置	🔾 专业策:
1全看板		
输大屏	5748 Y	
师管理	12.0h	
助告智	创藏计划	
用河管理	default (系统版认) 立即绘塑	
线检查	〇 每3天0.00-6.00检查一次	
(別結果	检查规范	
析报告	安全上云合规检查1.0	
志曾理		
全产品集成		
置 1 🔒		
通知设置		
128628		

**步骤4** 在检测设置页面中,选择待创建计划所在的区域,并单击"创建计划",系统右侧弹出新建检查计划页面。

副語の目前の       第第八十回公本         日本市会       第二十回公本         日本市会       第二十回公本         日本市会       日本市会         日本市会       日本市会 <t< th=""><th>新建检查计划</th><th></th></t<>	新建检查计划	
H 松和 (新路入計加設件) 松園 (新兵 ・ 000-6.00 ・ 松園 送課检査が応 「新路入国2005/編字 Q 「新路入国2005/編字 Q 「新路入国2005/編字 Q 日本版 (新路入国2005/編字 Q 日本版 (新路入国2005/編字 Q) 日本版 (新路入国2005/編字 Q) 「新路入国2005/編字 Q 日本版 (新路) 第第二版 (新路) 第二版 (新路) [1] (新B) [1] (新B)	基本信息	
総型利 (単元 、) (00-600 、) 松室 送野社会規定 (注私)(生100)(天田子 Q) (可加減 (単内松室) (単内松室) (注入水松松)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本	计划名称 请输入计划名称	
送理社会規約 - 可違版 - 可違版 - 可違版 - 学程2 (三)要求 - デ約1社室 - デ約1社室 - デ約1社室 - デ約1社室 - デ約1社室 - デ約1社室 - デ約1社室 - 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	检查时间 每1天 •	0:00-6:00 × 检查
·	选择检查规范	
可論員     已過員     證書       ● 毎歳20三級要求	请输入宣询的关键字    Q	请输入宣询的关键字    Q
● 毎後2.0三級要求       ● 炉闷祉量       ● 炉闷祉量       ● 戸戸社会会       ● 万元和板装置	可选顶	已选项 操作
	<ul> <li>● 等62.2—E0要求</li> <li>● 护用检查</li> </ul>	東元地林の第

### **图 14-13** 创建检查计划

步骤5 配置检查计划。

1. 填写基本信息,具体参数配置如表14-3所示。

表 14-3 检查计划基本信息

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

2. 选择检查规范。

选择需要检测的基线检查项目。更多关于基线检查项目详细描述请参见<mark>云服务基</mark> 线简介。

### 3. 单击"确定"。

### 步骤6 检查计划创建完成。

SA会在指定的时间执行云服务基线扫描,扫描结果可以在"安全与合规 > 态势感知 > 基线检查"中查看。

----结束