态势感知

用户指南

文档版本	02
发布日期	2023-04-24

华为技术有限公司

商标声明


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

注意

您购买的产品、服务或特性等应受华为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 产品介绍

1.1 什么是态势感知?

态势感知（Situation Awareness，SA）是可视化威胁检测和分析的平台。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

工作原理

态势感知通过采集全网流量数据和安全防护设备日志信息，并利用大数据安全分析平台进行处理和分析，态势感知检测出威胁告警，实时为用户呈现完整的全网攻击态势，进而为安全事件的处置决策提供依据。

1.2 功能特性

态势感知提供全局安全态势集中管理，包括**安全概览**、**资源管理**、**威胁告警**、**基线检查**、**检测结果**、**日志管理**、**产品集成**等功能。

安全概览

安全概览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

表 1-1 安全概览功能介绍

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

资源管理

态势感知支持呈现云上资产实时安全状态。

表 1-2 资源管理功能说明

功能模块	功能详情
资源管理	同步当前帐号中所有资源的安全状态统计信息。 支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题并提供解决方案。

威胁告警

“实时监控”云上威胁攻击，提供告警通知和监控，记录近180天告警事件详情，分析威胁攻击情况，并针对典型威胁事件预置策略实施防御手段。

目前，支持检测和呈现威胁告警事件，包括DDoS、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击和命令与控制。

表 1-3 威胁告警功能说明

功能模块	功能详情
告警列表	列表呈现威胁告警事件统计信息，支持查看告警事件和受威胁资产详情，并支持导出全部告警事件。
威胁分析	支持从“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。
通知告警	自定义威胁告警通知，支持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。

威胁告警事件

默认“实时监控”并上报威胁告警事件，支持检测和呈现威胁告警事件，包括DDoS、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击和命令与控制。

表 1-4 威胁告警事件说明

告警名称	威胁告警说明
DDoS	“实时检测”互联网主机的DDoS攻击。 共支持检测100+种子类型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	“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	“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	“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。 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。

告警名称	威胁告警说明
僵尸主机	“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	“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。 ● 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。
漏洞攻击	“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。 ● WebCMS漏洞攻击
命令控制	“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

基线检查

通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。

表 1-5 基线检查功能说明

功能模块	功能详情
云服务基线	通过一键扫描或设置定级扫描，分类呈现云服务配置检测结果，提示不合格检测项，并提供相应配置加固建议和帮助指导。

检测结果

通过集成安全防护产品，接入安全产品检测数据，管理全部检测结果。

表 1-6 全部结果功能说明

功能模块	功能详情
检测结果	通过呈现多种结果类型，支持标记、导出检测结果，并支持自定义结果列表。 ● 结果类型 威胁告警、漏洞、风险、合规检查、违法违规、舆情、安全公告。

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，满足日志存储180天及集中审计的要求。

表 1-7 日志管理功能说明

功能模块	功能详情
日志管理	通过OBS存储日志，满足SA日志审计和容灾需求。

产品集成

通过集成安全防护产品，接入安全产品检测数据，管理检测结果的数据来源。

表 1-8 产品集成功能说明

功能模块	功能详情
安全产品集成	通过集成安全防护产品，接入安全产品检测数据，管理检测结果的数据来源，支持查看传输数据量，管理数据上报健康状态。

1.3 应用场景

资产风险管理

云上业务众多，云上资产日益庞大，以及云资产的变化频繁，大大增加了云上安全风险。

态势感知集中呈现云上所有资产安全状况，实时监控云上业务整体安全，让服务器中的漏洞、威胁和攻击情况一目了然，保障所有资产的安全，帮助企业轻松应对资产安全风险。

威胁事件告警

面对云上各类安全威胁，以及不断涌出的新型威胁类型，态势感知通过汇集全网流量数据和安全防护设备日志信息，能够实时检测和监控云上安全风险，实时呈现告警事件的统计信息，并可对各种威胁事件进行汇聚统计。

风险配置管理

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。

1.4 服务版本差异

目前态势感知提供基础版和专业版两个版本，不同版本有不同功能使用范围，详细功能介绍请参见**功能特性**。

版本功能差异

说明

不同版本支持功能差别，标识符号说明如下：

- ×：代表不支持该功能。
- √：代表支持该功能。

表 1-9 不同版本功能差异

服务功能	功能模块	功能概述	基础版	专业版
安全概览	安全评分	集中呈现资产安全风险评分和风险等级分布，同时展示当前风险防御能力。	√	√
	安全监控	实时呈现展示待处理威胁告警、待修复漏洞、基线异常问题的安全监控统计数据。	√	√
	安全趋势	展示近7天内您的整体资产安全健康得分的趋势。	√	√

服务功能	功能模块	功能概述	基础版	专业版
资源管理	资源安全状况	同步资源信息，集中呈现资源整体安全状况。	×	√
威胁告警	告警列表	集中呈现威胁告警事件统计信息，导出告警事件。	√	√
		通过将告警忽略、标记为线下处理，标识告警事件。	×	√
	威胁分析	根据“攻击源”的IP查询被攻击的资产信息，亦可根据“被攻击的资产”的IP查询威胁攻击来源信息。	×	√
基线检查	云服务基线	通过一键扫描云服务基线，分类呈现云服务配置项检测结果信息。	×	√
		通过一键扫描云服务基线，分类呈现云服务配置项检测结果信息。支持查看检测结果详情，并提供相应修复建议。	×	√
检测结果	全部结果	集中呈现安全产品的检测结果，可导出结果、标识结果等。	√	√
日志管理	日志管理	通过授权OBS存储SA日志，满足日志审计和容灾需求。	×	√
产品集成	安全产品集成	通过集成安全产品，接入安全产品检测结果，管理检测结果的数据来源。	√	√

1.5 计费说明

计费项

态势感知**基础版**免费体验，**专业版**按选购的资产配额数计费。

表 1-10 计费项说明

版本	计费项	计费说明
基础版	无	免费体验，不计费。
专业版	资产配额	按购买的资产配额数计费，包括主机资产配额数和网站资产配额数。
	按需购买计费	即开即停，按小时结算。

计费模式

态势感知的计费模式为按需计费。按小时结算，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

变更配置

- 变更资产配额

  当您的资产数量增加，可在当前计费模式内增加资产配额数，不支持减少配额数。

1.6 基本概念

本节介绍态势感知相关概念。

安全风险

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

威胁告警

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

网站漏洞

网站漏洞是通过网络进行爬虫，智能对比漏洞特征检测出的web漏洞。态势感知具有OWASP TOP10和WASC的漏洞检测能力，支持扫描22种类型以上的漏洞，扫描规则云端自动更新，全网生效，及时涵盖最新爆发的漏洞及支持HTTPS扫描。

云服务基线

云服务基线是应用在云场景下，帮助用户检测云产品上存在的风险配置项，并提供修复建议。

攻击类型

- 暴力破解

  暴力破解法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。

- Web攻击

  Web攻击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。

- 僵尸主机

  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。

- 异常行为

  异常行为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。

- 漏洞攻击

  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。

1.7 SA 权限管理

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

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

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

SA 权限

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

SA部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问SA时，不需要切换区域。

权限根据授权精细程度分为角色和策略。

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

如**表1-11**所示，包括了SA的所有系统权限。

表 1-11 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 ReadOnlyAccess	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。

1.8 与其他云服务的关系

本小节主要介绍态势感知与其他云服务之间的关系。

与安全服务的关系

态势感知从企业主机安全（Host Security Service，HSS）等安全防护服务中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能AI分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

与 ECS 的关系

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

与 OBS 的关系

通过对象存储服务（Object Storage Service，OBS），您可以将SA日志存储至OBS桶中，确保日志不丢失，实现数据持久化。

2 升级版本

态势感知提供基础版、专业版供您选择。

- **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**专业版**。
  - **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、基线检查等功能。
  - 更多基础版、专业版功能差异，请参见**服务版本差异**。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 在页面左上角单击，选择“安全 > 态势感知”，默认进入态势感知安全概览管理页面。

步骤4 单击右上角“升级”，进入购买专业版页面。

步骤5 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。

步骤6 选择“计费模式”，可以选择包周期或按需。

步骤7 选择“态势感知版本”，此处默认选择专业版。

步骤8 配置“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。
- 当前账户下主机总数量>10台：主机配额最大限制=当前账户下主机总数量x10台
  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。

说明

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9 当“计费模式”选择“包周期”时，需要选择“购买时长”。

步骤10 确认参数配置无误后，在页面右下角单击“立即购买”。

步骤11 确认订单详情无误后，单击“去支付”，完成购买操作。

步骤12 进入“付款”页面，选择付款方式进行付款。

----结束

后续管理

若不再使用态势感知专业版功能，可单击“取消”，可继续使用基础版功能。

3 权限管理

3.1 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，您可以使用统一身份认证服务（Identity and Access Management，IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用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、高效的其他帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

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

本章节为您介绍对用户授权的方法，操作流程如**图3-1**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权限管理**。

如**表3-1**所示，包括了SA的所有系统权限。

表 3-1 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 ReadOnlyAccess	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

图 3-1 给用户授予 SA 权限流程

1. 创建用户组并授权
   在IAM控制台创建用户组，并授予态势感知的权限“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**。

3.2 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。

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": [
      {
         "Effect": "Allow",
         "Action": [
            "sa:threatevent:getList",
            "sa:threatevent:getAnalyze"
         ]
      }
   ]
}
```

- 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:*"
        ]
    }
  ]
}
```

3.3 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），如果登录帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用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，分为角色和策略。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

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

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

4 版本管理

4.1 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 4-1 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。

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，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 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

4.2 退订

若用户不再使用态势感知防护功能，可执行一键取消操作。

- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

取消按需计费

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择，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，单击“取消”，一键释放按需计费的资产配额。

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

5 安全概览

5.1 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**

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。

图 5-1 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”、“合规检查”两大类别。
- “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**：
  i. 在“安全评分”栏中，单击“立即处理”，系统右侧弹出“安全风险处理”页面。
  ii. 在“安全风险处理”页面中，单击“前往处理”，进入检测结果页面。
  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**、**合规检查**问题的安全监控统计数据。

图 5-2 安全监控

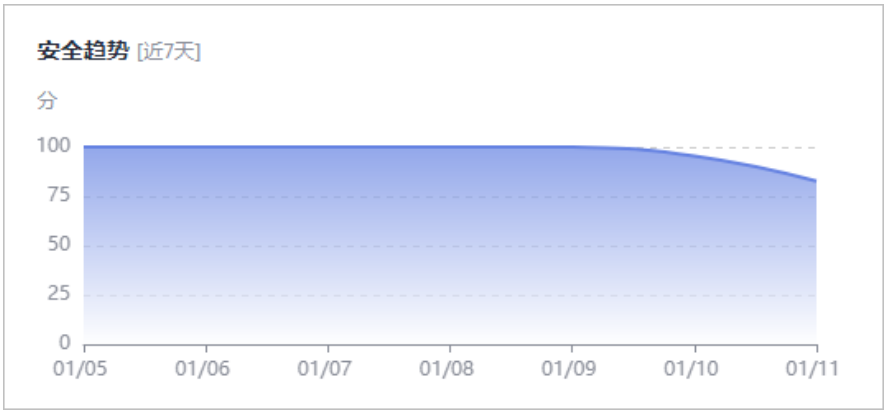
表 5-1 安全监控参数说明

参数名称	参数说明
威胁告警	呈现最**近7天内**未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 ● 单击威胁告警模块，系统将列表实时呈现**近7天内**TOP5的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况。 – 列表呈现近7天TOP5的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 若列表显示内容为空，表示近7天无威胁告警事件。 – 单击“查看更多”，可跳转到“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。
合规检查	展示您资产中**近30天内**存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了不合规的配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常配置，建议您及时查看该合规检查项目的详情。 ● 单击合规检查异常模块，系统将列表实时呈现**近30天内**TOP5的合规检查异常事件，可快速查看合规检查详情。 – 列表呈现最近一次合规检查中TOP的合规异常事件详情，包括合规检查项目名称、等级、资产名称、发现时间。 – 若列表显示内容为空，表示近30天无合规异常事件。 – 单击“查看更多”，可跳转到“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。

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 5-3 安全趋势



5.2 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 5-2 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。

风险等级	安全分值	分值说明
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5-3所示。

表 5-3 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，修复后重新触发扫描任务，自动刷新评分。	20
	存在未处理的高危不合规项	5		
	存在未处理的中危不合规项	2		
	存在未处理的低危不合规项	0.1		
威胁告警	存在未处理的致命告警事件	10	按照威胁事件处置指导建议进行修复，修复后自动刷新评分。	30
	存在未处理的高危告警事件	5		
	存在未处理的中危告警事件	2		
	存在未处理的低危告警事件	0.1		

6 资源管理

态势感知提供资源管理功能。在“资源管理”页面，您可以查看当前帐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、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。

前提条件

- 操作帐号权限检查。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，请提前授予操作帐号对应权限。

  “Tenant Administrator”权限配置详细操作请参见**配置资源管理、日志管理功能所需的权限**。
- 已升级为态势感知专业版，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 单击页面左上方的 ☰，选择“安全 > 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6-1**所示。

图 6-1 资源管理

表 6-1 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。
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	呈现资源的安全风险等级。 ● 风险等级包括“致命”、“高危”、“中危”、“低危”、“提示”和“无风险”。 ● 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。 ● 单击，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**近7天内**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**近24小时内**未修复的漏洞总数。 ● 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。 ● “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。
基线	呈现资源**近30天内**存在的基线风险总数。 ● 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。 ● “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。
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。
- **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  ，即可查看目标资源的安全状态。

----结束

7 威胁告警

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。

DDoS 事件

“实时检测”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。

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。

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。

- 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 > 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“威胁告警”，默认进入态势感知告警列表管理页面。

图 7-1 威胁告警

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🔍，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。

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

已升级为态势感知专业版，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 > 态势感知 > 威胁告警 > 威胁分析”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“威胁告警”，进入威胁告警页面后，选择“威胁分析”页签，进入威胁分析管理页面。

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

7.4.1 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。

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表7-1。

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。

7.4.2 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。

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。

7.4.3 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，如各种帐户、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。

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。

7.4.4 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。

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**表7-2**。

表 7-2 漏洞攻击类威胁处理建议

威胁告警名称	告警等级	威胁说明	处理建议
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。

7.4.5 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。

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。

7.4.6 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。

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。

7.4.7 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。

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**表7-3**。

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
文件目录变更监测事件	提示	检测到ECS实例的关键文件被更改。	建议登录企业主机安全管理控制台处理。
系统成功登录审计事件	提示	检测到ECS实例已异常成功登录。	建议登录企业主机安全管理控制台处理。
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 基线检查

8.1 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。

约束与限制

- SA**基础版**暂不支持使用基线检查功能。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，建议您使用专业版。
- 操作帐号权限检查。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，请提前授予操作帐号对应权限。

  “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**。

8.2 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，需要给操作帐号配置“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

已获取管理员帐号及密码。

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。

1. 在左侧导航栏选择“权限管理 > 权限”，并在权限页面右上角单击“创建自定义策略”。
2. 配置策略。
   a. 策略名称：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。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:users:getUser",
                "iam:securitypolicies:getLoginPolicy",
                "iam:credentials:listCredentials",
                "iam:users:getUserLoginProtect",
                "iam:agencies:listAgencies",
                "iam:securitypolicies:getProtectPolicy",
                "iam:users:listUsers",
                "iam:securitypolicies:getPasswordPolicy",
                "iam:groups:listGroups",
                "iam:permissions:listRolesForAgencyOnProject",
                "iam:users:listUsersForGroup",
                "iam:projects:listProjectsForUser",
                "iam:permissions:listRolesForAgencyOnDomain"
            ]
        }
    ]
}
```

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 8-1 基线检查权限策略

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。

----结束

8.3 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：您帐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。

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 > 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。

图 8-2 进入基线检查计划配置页面

- 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 8-3 检测设置页面

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。

步骤5 配置检查计划。

1. 填写基本信息，具体参数配置如表8-1所示。

   表 8-1 检查计划基本信息

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

2. 选择检查规范。

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

3. 单击“确定”。

   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“基线检查”中查看。

----结束

相关操作

基线检查计划创建后，您可以查看检查计划、对检查计划进行编辑或删除。

- 查看已有检查计划
  a. 登录管理控制台。
  b. 在页面左上角单击 ☰，选择“安全 > 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”。

8.4 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 > 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 8-4 基线检查页面

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”。

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。

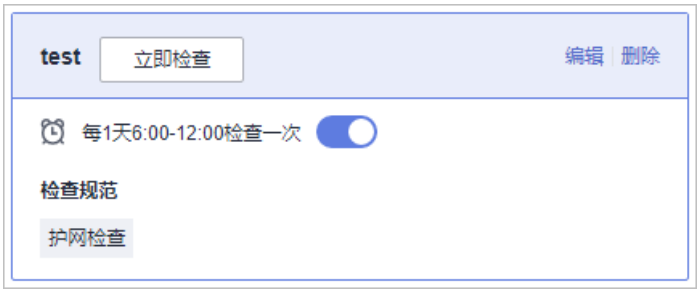
步骤2 在页面左上角单击 ☰，选择“安全 > 态势感知”，进入态势感知管理页面。

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 8-5 执行某个检查计划



系统将立即执行已选择的基线检查计划。

----结束

8.5 执行手动检查

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

基线检查的一些检查项目为手动检查项，需要您在线下执行检查后，再在控制台上反馈检查结果，以便计算检查项合格率。

前提条件

- 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 > 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”。

步骤6 在弹出提示框中，选择反馈结果，并单击“确定”。

图 8-6 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

8.6 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 > 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 8-7 检查结果总数据

- 检查规范数：最近一次执行基线检查的检查规范数/检查规范总数。
- 检查项：最近一次执行基线检查中所有的检查项数目。
- 检查项合格率：最近一次执行基线检查的基线合格率。

  整体合格率=合格检查项数量/检查项总数。合格率的统计范围为全部规范的全部检查项目。

  检查项结果分为合格、不合格、检查失败和待检查几种。
- 风险资源分布：最近一次执行基线检查的风险资源分布情况以及风险资源的数量。

  风险等级分为：致命、高危、中危、低危、提示几个级别。

----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 > 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。

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

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全 > 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。

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。

----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 > 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。

图 8-8 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

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全 > 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 8-9 检查资源详情

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 8-10 检查资源详情页面

----结束

查看检查结果列表

步骤1 登录管理控制台。

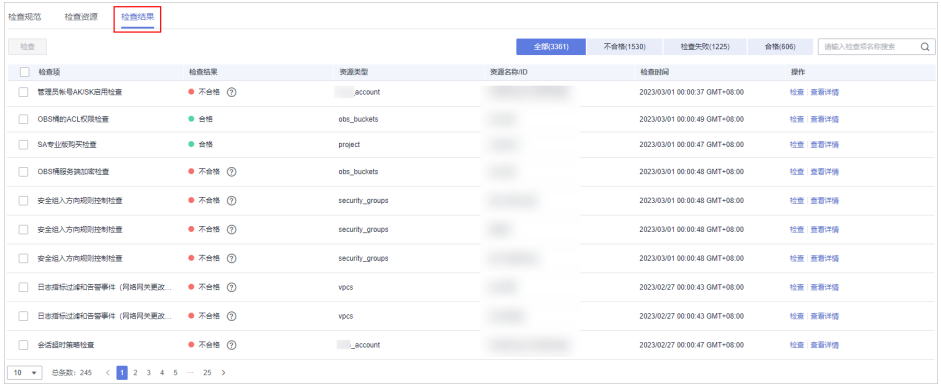
步骤2 在页面左上角单击 ☰，选择“安全 > 态势感知”，进入态势感知管理页面。

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。

图 8-11 全部检查结果



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

8.7 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

- 已扫描云服务基线。

修复风险项

步骤1 登录管理控制台。

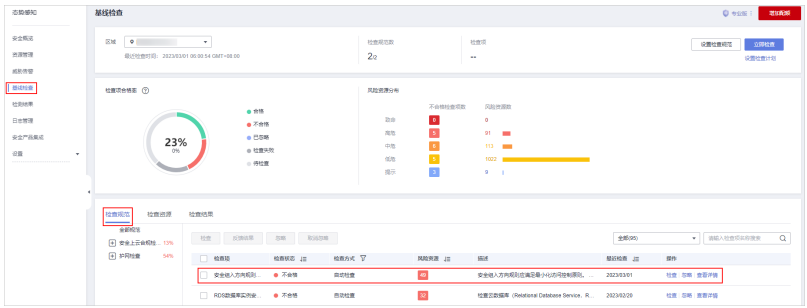
步骤2 在页面左上角单击 ，选择“安全 > 态势感知”，进入态势感知管理页面。

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，选择子检查项，查看子检查项风险状态。

图 8-12 子检查项风险状态



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

步骤6 在子检查项所在行的“操作”列，单击“查看详情”，系统进入检查项目详情页面。

步骤7 查看风险详细信息，并根据“检查结果”和“帮助指导”，修复风险点。

表 8-2 子检查项信息说明

参数名称	参数说明
检查状态	呈现当前检查项的检查状态。 • 合格，提示当前子检查项配置合理，全部合格。 • 不合格，提示当前子检查项配置可能不合理，并列表呈现检查结果。

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

步骤8 修复所有存在风险的配置后，可单击“检查”，确认风险项是否已修复。

----结束

反馈结果

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 > 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”。

步骤6 在弹出提示框中，选择反馈结果，并单击“确定”。

图 8-13 反馈结果

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

9 检测结果

9.1 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。

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。

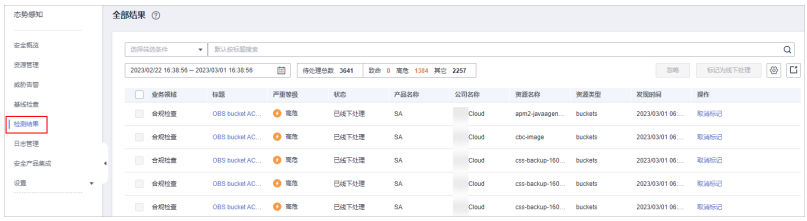
操作步骤

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 > 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。

图 9-1 查看全部检测结果



步骤4 筛选查看检测结果。

- 在场景列框选择过滤场景，单击，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，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 9-2 检测结果详情

2. 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9-1。

表 9-1 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、严重等级、状态、发现时间、业务领域、公司名称、产品名称、类型等信息。
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。

参数	参数说明
环境信息	受影响的用户信息，包括租户ID、项目ID、用户所在区域等信息。
攻击信息	攻击来源信息，包括攻击源IP、攻击目标IP、攻击源端口、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

9.2 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）、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 > 态势感知”，进入态势感知管理页面。

步骤3 筛选检测结果。

步骤4 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5 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

9.3 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 > 态势感知”，进入态势感知管理页面。

步骤3 筛选检测结果。

步骤4 单击 ，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

9.4 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 > 态势感知”，进入态势感知管理页面。

步骤3 单击⚙，展开结果列表属性框。

步骤4 勾选结果属性。

步骤5 刷新结果列表，即可在列表查看目标属性。

----结束

9.5 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”。

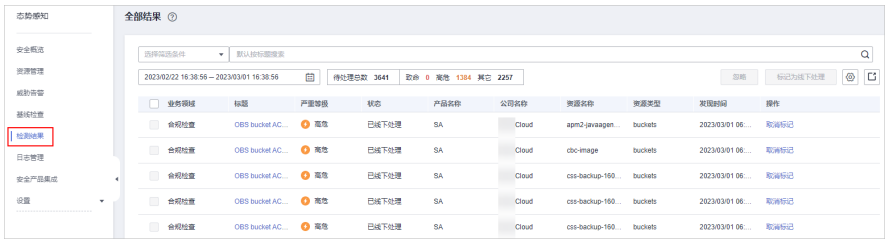
创建筛选条件

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 > 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 9-3 检测结果



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 > 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。

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 > 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。

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

10 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。

背景信息

日志管理通过授权OBS存储SA日志，可实现日志存储、导出场景。日志存储后，支持长久存储和本地下载日志数据。

前提条件

- 已购买专业版态势感知，且在有效使用期内。
- 操作帐号权限检查。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，请提前授予操作帐号对应权限。

  “Tenant Administrator”权限配置详细操作请参见sa_01_0016.html#section753419154403。

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 > 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。

图 10-1 存储至 OBS 桶

步骤4 配置存储日志相关参数，具体参数说明如表10-1所示。

表 10-1 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。 **说明** • 目前仅支持选择当前帐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，已上传存储到OBS桶的日志数据不会被删除。

11 产品集成

11.1 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。

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。

启用产品集成

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 11-1 产品集成

步骤3 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4 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 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**查看产品集成列表**。

步骤2 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

11.2 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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 11-2 产品集成

步骤3 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4 选择“产品名称”、“产品类型”或“公司名称”筛选条件。

步骤5 在搜索框输入关键字，单击🔍，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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 11-3 产品集成

步骤3 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4 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**。

----结束

11.3 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。

表 11-1 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 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 11-4 产品集成

步骤3 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4 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。

----结束

12 设置

12.1 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 > 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 12-1 检测设置页面

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。

步骤5 配置检查计划。

1. 填写基本信息，具体参数配置如表12-1所示。

表 12-1 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。

参数名称	参数说明
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**云服务基线简介**。

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 > 态势感知 > 基线检查”中查看。

----结束

13 常见问题

13.1 产品咨询

13.1.1 态势感知可以为我提供什么服务?

态势感知（Situation Awareness，SA）是可视化威胁检测和分析的平台。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

13.1.2 为什么没有看到攻击数据或者看到的攻击数据很少?

态势感知支持检测云上资产遭受的各类攻击，并进行客观的呈现。但是，如果您的云上资产在互联网上的暴露面非常少（所谓“暴露面”是指资产可被攻击或利用的风险点，例如端口暴露和弱口令都可能成为风险点），那么遭受到攻击的可能性也将大大降低，所以态势感知可能会显示您的系统当前遭受的攻击程度较低。

13.1.3 态势感知的数据来源是什么?

态势感知基于云上威胁数据和云服务采集的威胁数据，通过大数据挖掘和机器学习，分析并呈现威胁态势，并提供防护建议。

- 一方面采集全网流量数据，以及安全防护设备日志等信息，通过大数据智能AI分析采集的信息，呈现资产的安全状况，并生成相应的威胁告警。
- 另一方面汇聚企业主机安全（Host Security Service，HSS）等安全防护服务上报的告警数据，从中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能AI分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

态势感知通过对多方面的安全数据的分析，为安全事件的处置决策提供依据，实时呈现完整的全网攻击态势。

13.1.4 如何获取风险程度最高的资产信息?

通过查看资产风险排名，可以获取风险程度最高的资产信息，并可进一步了解该资产遭受的威胁告警统计信息。

用户可在**专业版**的“资源管理”页面查看风险资产。**基础版**不支持查看风险资产排名信息。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面的上方的 ☰，选择“安全 > 态势感知 > 资源管理”，进入态势感知服务资源管理页面。

单击“安全状况”、“威胁”、“漏洞”、或“基线”列排序按钮，排序当前资产风险排名。

----结束

13.1.5 态势感知与其他安全服务之间的关系与区别?

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

- 关联：

  SA：作为安全管理服务，依赖于其他安全服务提供威胁检测数据，进行安全威胁风险分析，呈现全局安全威胁态势，并提供防护建议。

  其他安全服务：威胁检测数据可以统一汇聚在SA中，呈现全局安全威胁攻击态势。

- 区别：

  SA：仅为可视化威胁检测和分析的平台，不实施具体安全防护动作，需与其他安全服务搭配使用。

  其他安全服务：仅展示对应服务的检测分析数据，并实施具体安全防护动作，不会呈现全局的威胁攻击态势。

SA与其他安全防护服务含义、关联与区别如表13-1所示。

表 13-1 SA 与其他服务的区别

服务名称	服务类别	关联与区别	防护对象
态势感知（SA）	安全管理	SA着重呈现全局安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，并提供防护建议。	呈现全局安全威胁攻击态势。
Anti-DDoS流量清洗（Anti-DDoS）	网络安全	Anti-DDoS集中于异常DDoS攻击流量的检测和防御。 同步相关攻击日志、防护等数据给SA。	保障企业业务稳定性。
企业主机安全（HSS）	主机安全	HSS着手于保障主机整体安全性，检测主机安全风险，执行防护策略。 同步相关告警、防护等数据给SA。	保障主机整体安全性。

服务名称	服务类别	关联与区别	防护对象
Web应用防火墙（WAF）	应用安全	WAF服务对网站业务流量进行多维度检测和防护，防御常见攻击，阻断攻击进一步威胁。 同步相关入侵日志、告警数据等给SA，呈现全网Web风险态势。	保障Web应用程序的可用性、安全性。
数据库安全服务（DBSS）	数据安全	DBSS着力于数据库访问行为的防护和审计。 同步相关审计日志、告警数据等给SA。	保障云上数据库安全和资产安全。

13.1.6 为什么主机最大配额不能小于主机数量?

主机最大配额是授权检测主机的最大数量。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。

操作步骤

登录态势感知控制台，单击“升级”。根据规划或现有主机数量，配置主机最大配额。

图 13-1 配置最大配额

13.1.7 如何更新安全评分?

态势感知支持实时检测整体资产的安全状态，评估整体资产安全健康得分。通过查看安全评分，可快速了解未处理风险对资产的整体威胁状况。

资产安全风险修复后，为降低安全评分的风险等级，目前需手动忽略或处理告警事件，刷新告警列表中告警事件状态。告警事件状态刷新并启动重新检测后，安全评分将更新。

图 13-2 安全评分

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 > 态势感知 > 检测结果”，进入全部检测结果页面。

步骤3 忽略告警事件。

在相应告警事件“操作”列，单击“忽略”，告警事件状态更新为“已忽略”。

步骤4 标记为线下处理。

1. 在相应告警事件“操作”列，单击“标记为线下处理”，弹出告警事件处理窗口。
2. 记录“处理人”、“处理时间”和“处理结果”。
3. 单击“确认”，返回告警列表页面，告警事件状态更新为“已线下处理”。

步骤5 相应告警事件已标记后，返回“安全概览”页面，单击“重新检测”，检测后可查看更新的安全评分。

说明

由于检测需要一定的时间，请您在单击“重新检测”按钮**5分钟**后，再刷新页面，查看最新检测的安全评分。

----结束

13.1.8 如何处理暴力破解告警事件?

暴力破解是一种常见的入侵攻击行为，攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制，严重危害资产的安全。

态势感知联动企业主机安全服务（HSS），接收HSS检测到的暴力破解行为，集中呈现和管理告警事件，提升运维效率。

处理告警事件

HSS通过暴力破解检测算法和全网IP黑名单，若发现暴力破解主机的行为，对发起攻击的源IP进行拦截，并上报告警事件。

当接收到来源于HSS的告警事件时，请登录HSS管理控制台确认并处理告警事件。

- 若您的主机被爆破成功，检测到入侵者成功登录主机，账户下所有云服务器可能已被植入恶意程序，建议参考如下措施，立即处理告警事件，避免进一步危害主机的风险。
  a. 请立即确认登录主机的源IP的可信情况。
  b. 请立即修改被暴力破解的系统账户口令。
  c. 请立即执行检测入侵风险账户，排查可疑账户并处理。
  d. 请及时执行恶意程序云查杀，排查系统恶意程序。
- 若您的主机被暴力破解，攻击源IP被HSS拦截，请参考如下措施，加固主机安全。
  a. 请及时确认登录主机的源IP的可信情况。
  b. 请及时登录主机系统，全面排查系统风险。

c. 请根据实际需求升级HSS防护能力。
d. 请根据实际情况加固主机安全组、防火墙配置。

标记告警事件

告警事件处理完成后，您可以根据处理情况，标记已识别的告警事件，加强对告警事件的管理。

步骤1 登录管理控制台。

步骤2 在页面左上角单击  ，选择“安全 > 态势感知 > 威胁告警”，进入告警列表管理页面。

步骤3 选择“暴力破解”事件类型，刷新告警列表。

步骤4 选择目标事件，根据实际情况忽略无威胁告警事件，标记已处理的告警事件。

----结束

13.1.9 如何给帐号配置相关功能所需的权限?

当您需要使用SA的**基线检查**、**资源管理**、**日志管理**功能时，需要给操作帐号配置“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。

- **配置基线检查功能所需的权限**
- **配置资源管理、日志管理功能所需的权限**

前提条件

已获取管理员帐号及密码。

配置基线检查功能所需的权限

操作过程中，须按照此步骤介绍的权限/策略进行配置，不可自定义勾选其他权限/策略，避免出现配置后功能仍不可使用的问题。

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。

1. 在左侧导航栏选择“权限管理 > 权限”，并在权限页面右上角单击“创建自定义策略”。
2. 配置策略。
   a. 策略名称：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。


```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:users:getUser",
                "iam:securitypolicies:getLoginPolicy",
                "iam:credentials:listCredentials",
                "iam:users:getUserLoginProtect",
                "iam:agencies:listAgencies",
                "iam:securitypolicies:getProtectPolicy",
                "iam:users:listUsers",
                "iam:securitypolicies:getPasswordPolicy",
                "iam:groups:listGroups",
                "iam:permissions:listRolesForAgencyOnProject",
                "iam:users:listUsersForGroup",
                "iam:projects:listProjectsForUser",
                "iam:permissions:listRolesForAgencyOnDomain"
            ]
        }
    ]
}
```

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 13-3 基线检查权限策略-示例

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。

----结束

配置资源管理、日志管理功能所需的权限

操作过程中，须按照此步骤介绍的权限/策略进行配置，不可自定义勾选其他权限/策略，避免出现配置后功能仍不可使用的问题。

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 在左侧导航栏选择“委托”，进入委托页面。

步骤4 在委托列表中选择“ssa_admin_trust”，进入委托详情页面。

步骤5 选择“授权记录”页签，并在页面中单击“授权”。

步骤6 在权限配置栏目搜索并选择“Tenant Administrator”权限。

图 13-4 资源管理权限策略

步骤7 单击页面下方“下一步”，设置最小授权范围。

步骤8 单击页面下方的“确定”。

----结束

13.1.10 为什么 WAF、HSS 中的数据和 SA 中的数据不一致?

由于SA中汇聚WAF和HSS上报的所有历史告警数据，而WAF和HSS中展示的是实时告警数据，导致存在SA与WAF、HSS中数据不一致的情况。

因此，建议您前往对应服务（WAF或HSS）进行查看并处理。

13.2 购买咨询

13.2.1 态势感知如何变更版本规格?

变更按需专业版规格

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择，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 添加需要增加的“主机配额”。

步骤7 配置完成后，单击“立即购买”。

步骤8 返回态势感知控制台页面，即可在版本管理窗口查看规格变化。

----结束

13.2.2 态势感知如何收费?

态势感知的计费模式为按需计费。按小时结算，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

13.2.3 态势感知支持退订吗?

若用户不再使用态势感知防护功能，可执行退订或一键取消操作。

- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

说明

免费版不支持退订。

退订按需专业版

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择，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，单击“取消”，一键释放按需计费的资产配额。

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

13.2.4 态势感知可以免费使用吗?

可以。

态势感知提供基础版、专业版两个服务版本。

- 用户可长期免费使用基础版。
- 专业版按需计费。

基础版、专业版在功能上的差异，请参见**功能特性**。

A 修订记录

发布日期	修改记录
2023-04-24	第二次正式发布。 • 新增**创建用户并授权使用SA**、**增加资产配额**、**退订**、**告警事件处理**、**如何获取风险程度最高的资产信息？**、**态势感知与其他安全服务之间的关系与区别？**、**为什么主机最大配额不能小于主机数量？**、**为什么WAF、HSS中的数据和SA中的数据不一致？**章节内容。 • 更新**资源管理**、**基线检查**、**检测结果**、**产品集成**章节内容，刷新图片。
2023-01-10	第一次正式发布。