态势感知

常见问题

文档版本 30

发布日期 2023-06-08

华为云计算技术有限公司

商标声明


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

注意

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

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

目 录

1 产品咨询

1.1 态势感知可以为我提供什么服务?

态势感知（Situation Awareness，SA）是华为云安全管理与态势分析平台。能够检测出8大类的云上安全风险，包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。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。

详细功能特性介绍请参见**功能介绍**。

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。

如果您认为态势感知未能真实反映系统遭受攻击的状况，欢迎您向客服反馈问题。

详细说明请参见**态势感知工作原理**和**功能介绍**。

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华为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）、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，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。

详细说明请参见**态势感知工作原理**。

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**标准版**或**专业版**的“资源管理”页面，以及“华为云主机安全态势”页面的“TOP5风险云主机”模块查看风险资产。**基础版**不支持查看风险资产排名信息。

详细说明请分别参见**资源管理**和**主机安全态势**。

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“安全与合规 > 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。

图 1-1 资产风险排序

步骤3 选择“安全与合规 > 态势感知 > 综合大屏”，单击“主机安全态势”，查看华为云主机安全态势大屏。

查看“TOP5风险云主机”窗口，如**图1-2**。可查看TOP5风险主机的名称、主机系统和安全风险等级，并按照风险等级从高到低的依次排序。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 1-2 风险云主机

----结束

1.5 如何获取攻击者的信息?

如需了解攻击者（即攻击源）的相关信息，可以查看攻击者排名列表。

用户可在**标准版**或**专业版**的“综合态势感知”页面的“威胁源主机TOP5”模块查看攻击者信息。**基础版**不支持查看攻击者排名信息。

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“安全与合规 > 态势感知 > 综合大屏”，单击“综合态势感知”，查看综合态势感知大屏。

查看“威胁源主机TOP5”窗口，如图1-3。可查看攻击者主机的IP地址、所属国家/地区和攻击次数，并按照攻击次数从高到低的依次排序。

图 1-3 威胁源主机 TOP5

----结束

1.6 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、AAD）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1-1所示。

表 1-1 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	功能详细介绍
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。	SA功能介绍

服务名称	服务类别	关联与区别	防护对象	功能详细介绍
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。	Anti-DDoS功能特性
DDoS高防（AAD）	网络安全	AAD将公网流量引流至高防IP，聚焦于大流量的DDoS攻击的检测和防御。 同步相关攻击日志、防护等数据给SA。	保障企业重要业务连续性。	AAD产品介绍
主机安全服务（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。	HSS功能特性
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。	WAF功能特性
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。	DBSS产品介绍

1.7 SA 与 HSS 服务的区别?

服务含义区别

- 态势感知（Situation Awareness，SA）是华为云可视化威胁检测和分析的**安全管理平台**。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，帮助企业构建全局安全体系，呈现全局安全攻击态势。
- 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。

简而言之，SA是呈现**全局**安全态势的服务，HSS是提升**主机**和**容器**安全性的服务。

服务功能区别

- SA通过采集**全网安全数据**（包括HSS、WAF、AntiDDoS等安全服务检测数据），使用大数据AI、机器学习等分析技术，从资产安全、威胁告警、漏洞管理、基线检查维度，分类呈现资产安全状况。

- HSS通过在**主机**中安装Agent，使用AI、机器学习和深度算法等技术分析主机中风险，并从HSS云端防护中心下发检测和防护任务，全方位保障主机安全。同时可从可视化控制台，管理主机Agent上报的安全信息。

表 1-2 SA 与 HSS 主要功能区别

功能项		共同点	不同点
资产安全	主机资产	呈现主机资产的整体安全状态。	● SA：仅支持同步HSS主机资产风险信息，列表呈现各主机资产的整体安全状况。 ● HSS：不仅支持呈现主机的安全状况，还支持深度扫描主机中的账号、端口、进程、Web目录、软件信息和自启动任务。
	网站资产	-	● SA：支持检查和扫描网站安全状态，列表呈现各网站资产的整体安全状况。 ● HSS：不支持该功能。
漏洞管理	应急漏洞公告	-	● SA：支持同步华为云安全公告信息，及时获取热点安全讯息。 ● HSS：不支持该功能。
	主机漏洞	呈现主机漏洞扫描结果，管理主机漏洞。	● SA：仅支持同步HSS主机漏洞扫描结果，管理主机漏洞。 ● HSS：支持检测Linux漏洞、Windows漏洞、Web-CMS漏洞、应用漏洞，提供漏洞概览，包括主机漏洞检测详情、漏洞统计、漏洞类型分布、漏洞TOP5和风险服务器TOP5，帮助您实时了解主机漏洞情况。
	网站漏洞	-	● SA：支持同步CodeArts Inspector网站漏洞扫描结果，管理网站漏洞。 ● HSS：不支持该功能。
基线检查	云服务基线	-	● SA：针对华为云服务关键配置项，从“安全上云合规检查1.0”、“等保2.0三级要求”、“护网检查”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。 ● HSS：不支持该功能。
	主机基线	-	● SA：不支持该功能。 ● HSS：针对主机，提供基线检查功能，包括检测复杂策略、弱口令及配置详情，包括对主机配置基线通过率、主机配置风险TOP5、主机弱口令检测、主机弱口令风险TOP5的统计。

1.8 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

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

更多购买操作说明，请参见**购买态势感知专业版**。

图 1-4 配置最大配额

说明

在态势感知使用期间，当账户下主机数量的总和超过主机最大配额时，您需及时扩充主机最大配额，变更版本规格，详情请参见**如何变更专业版规格?** 。

1.9 态势感知支持跨账号使用吗?

不支持。

态势感知服务暂不支持跨账号使用，用户仅能获取和管理当前账号下资源的威胁风险信息。

但一个账号下所有用户，即该账号及该账号下所有授权的IAM用户，可共享该账号的全局威胁风险信息。

1.10 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 1-5 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“安全与合规 > 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

更多安全评分说明，请参见**安全概览**。

1.11 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。

详情请参见**HSS如何处理账户暴力破解事件？**。

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“安全与合规 > 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

更多详情说明请参见**查看告警列表**。

1.12 为什么不能使用主机漏洞和网站漏洞功能?

因SA主机漏洞和网站漏洞功能接入的是漏洞管理服务（CodeArts Inspector）的扫描数据，由于CodeArts Inspector功能调整，原有主机扫描和网站漏洞功能将陆续从“安全产品集成”接入扫描数据，目前可能影响部分用户使用。

- 新用户以及付费版本到期的用户，开启HSS和CodeArts Inspector产品集成，接入扫描数据，即可在“全部结果”页面，获取漏洞扫描结果。
- 付费版本续存期用户，可继续正常使用主机漏洞和网站漏洞功能。

1.13 如何给账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。

- 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

已获取管理员账号及密码。

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 1-6 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 1-7 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

1.14 如何处理 SA 的 403 forbidden 报错?

故障现象

在SA控制台访问“威胁告警”页面时，用户不能正常访问网站，提示“403: Forbidden。”报错，如所示。

图 1-8 403 报错

故障原因

子账号权限不足，仅为操作账号配置了SA FullAccess或SA ReadOnlyAccess策略权限，未配置“Tenant Guest”角色。

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。

处理方法

通过管理员账号给IAM子账号配置“Tenant Guest”权限。

图 1-9 Tenant Guest

关于“Tenant Guest”权限的介绍和开通方法，详细参见**系统权限**，**将其加入用户组**，并**给用户组授予策略或角色**。

1.15 为什么 WAF、HSS 中的数据和 SA 中的数据不一致?

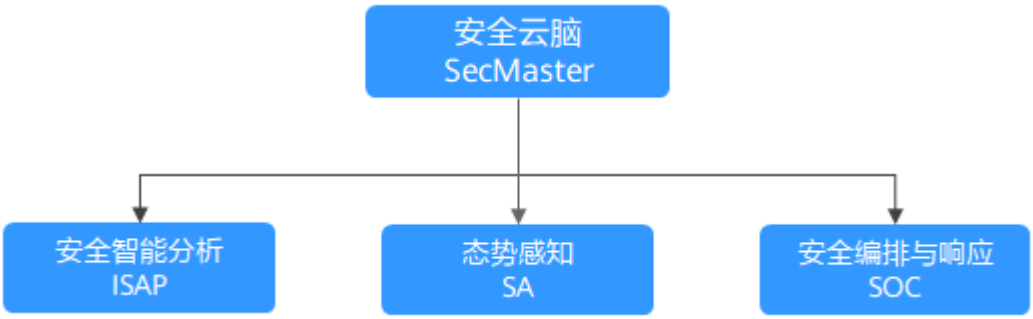
由于SA中汇聚WAF和HSS上报的所有历史告警数据，而WAF和HSS中展示的是实时告警数据，导致存在SA与WAF、HSS中数据不一致的情况。

因此，建议您前往对应服务（WAF或HSS）进行查看并处理。

1.16 SA 与 SecMaster 服务的关系与区别?

华为云提供有态势感知（Situation Awareness，SA）和安全云脑（SecMaster）服务，两者之间的关系与区别如下：

图 1-10 SA 与 SecMaster 的关系与区别



简而言之，安全云脑（SecMaster）包含了态势感知（SA）、安全智能分析（ISAP）和安全编排与响应（SOC）的功能。

- 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，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。
- 态势感知（Situation Awareness，SA）是华为云安全管理与态势分析平台。

  利用大数据分析技术，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。
- 安全智能分析（Intelligent Security Analysis Platform，ISAP）是安全运营分析建模的数据中台系统。

  支持云服务安全日志数据采集、数据检索、智能建模等功能，提供专业级的安全分析能力，实现对云负载、各类应用及数据的安全保护。
- 安全编排与响应（Security Operations Center，SOC）是云上开展安全运营业务活动时对风险要素、威胁、脆弱性做出快速响应的作战平台，结合安全编排与自动化相应系统（Security Operations，Analytics and Response，SOAR），对云上安全风险进行全局管控。

  提供基于完整安全运营业务框架的工作台入口，可对安全资产、安全策略进行统一管理；提供面向安全运营业务流，进行自助编排、自动响应、人工处置的能力。

2 购买咨询

2.1 态势感知如何变更版本规格?

购买态势感知后，当用户资产数量增加，或追加**综合大屏**功能，则需要变更版本规格，即需扩充“主机配额”或新增“安全大屏”。

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。

变更包周期专业版规格

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“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“包周期”，按配置周期计费。

步骤6 添加需要增加的“主机配额”或勾选“安全大屏”，确认“购买时长”。

说明

- 变更为增加“主机配额”规格时，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。
- 变更时开通的综合大屏的“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。
- 增加资产配额的“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。

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“去支付”。

步骤9 在支付页面完成付款后，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

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“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 添加需要增加的“主机配额”或勾选“安全大屏”。

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，即可在版本管理窗口查看规格变化。

----结束

3 区域与可用区

3.1 什么是区域和可用区?

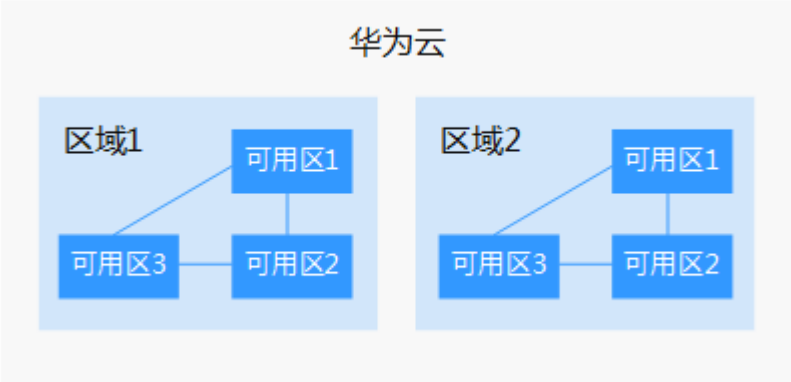
什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图3-1阐明了区域和可用区之间的关系。

图 3-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。
- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

3.2 态势感知支持跨区域使用吗?

支持。

态势感知为全局级服务，不需要切换区域，即可使用态势感知服务。

须知

部分区域暂不支持使用“基线检查”和“日志管理（存储至OBS）”功能，具体请以控制台显示为准。