威胁检测服务

常见问题

文档版本 13

发布日期 2022-07-16

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 产品咨询

1.1 什么是威胁检测服务?

此服务集成了AI智能引擎、威胁情报、规则基线三种检测方式，智能检测来自多个云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中的访问行为，去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。您可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护您的帐户安全、保障服务稳定运行。

各 Region 支持的检测类型

各Region支持的检测类型如**表1-1**所示。

表 1-1 各 Region 支持的检测类型

名称	IAM检测	DNS检测	CTS检测	OBS检测	VPC检测
华南-广州	√	√	√	√	√
华东-上海一	√	√	√	-	√
华北-北京四	√	√	√	√	-

1.2 威胁检测服务的检测源头是什么?

威胁检测服务的检测源头是日志，当前支持对接入的IAM日志、VPC日志，DNS日志、OBS日志和CTS日志进行分析，暂不支持其他类型的文件分析。

1.3 威胁检测服务的检测对象是什么?

威胁检测服务的检测对象为帐号和云负载（云上资源或服务）。

1.4 威胁检测服务能够解决什么其他安全服务解决不了的问题?

威胁检测服务可以检测IAM帐号安全风险，以及利用DNS进行攻击暴露出来的风险，还有在CTS日志中各种入侵行为暴露出来的风险，这几类安全风险其他任何安全服务暂时无法解决或能力较弱。

1.5 威胁检测服务可以检测哪些风险?

威胁检测服务接入全量的统一身份认证（IAM）、虚拟私有云（VPC）、云解析服务（DNS）、云审计服务（CTS）、对象存储服务（OBS）的日志数据，利用AI智能引擎、威胁情报、规则基线模型一站式检测，持续监控暴力破解、恶意攻击、渗透、挖矿攻击等恶意活动和未经授权行为，识别云服务日志中的潜在威胁，对检测出的威胁告警信息进行统计展示。

威胁检测服务通过弹性画像模型、无监督模型、有监督模型实现对风险口令、凭证泄露、Token利用、异常委托、异地登录、未知威胁、暴力破解七大高危场景实现了异常行为的智能检测。可有效对化整为零低频次的分布式暴破攻击行为进行成功捕获。同时可对Linux.Ngioweb僵尸网络、SystemdMiner挖矿木马、WatchBog挖矿木马、BadRabbit勒索病毒进行有效检测、捕获。

1.6 威胁检测服务购买后如何使用?

您完成创建威胁检测引擎和配置追踪器两步操作后，即可正常使用。

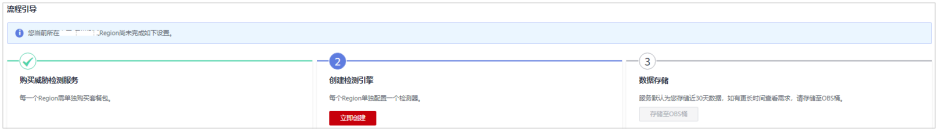
步骤一：创建威胁检测引擎

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 威胁检测服务”，进入威胁检测服务界面，如图 威胁检测服务首页所示。

图 1-1 威胁检测服务首页



步骤4 单击“创建检测引擎”下的“立即创建”，创建区域检测引擎，单击后待页面运行结束，页面右上角会提示“检测引擎创建成功”，页面会自动刷新一次，单击页面左上方流程引导的展开流程引导，显示如图 创建检测引擎成功所示，表示检测引擎创建成功。

图 1-2 创建检测引擎成功

----结束

步骤二：配置追踪器

步骤1 创建完威胁检测引擎后，总览页界面提示“以下服务无法直接获取日志数据，需要您进行配置”的提示框，如**图 追踪器配置提醒**所示。

图 1-3 追踪器配置提醒

步骤2 单击“创建追踪器”，跳转至CTS追踪器页面，在追踪器列表找到“追踪器类型”为“管理事件”的唯一默认追踪器，如**图 管理事件追踪器**所示。

说明

“追踪器类型”为“管理事件”的追踪器无需创建，系统默认生成。

图 1-4 管理事件追踪器

步骤3 单击目标追踪器“操作”列的“配置”，在弹出的“配置追踪器”窗口中，单击“事件分析”后的  ，开启事件分析，如**图 开启事件分析**所示，然后单击“确定”完成追踪器的配置。

图 1-5 开启事件分析

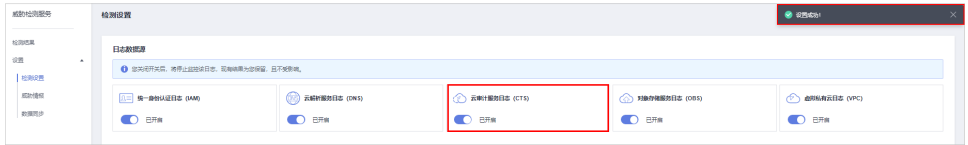
步骤4 在左侧导航树中，单击 ☰，选择“安全与合规 > 威胁检测服务”，返回威胁检测服务界面。

步骤5 在页面左上角选择“设置>检测设置”,进入检测设置界面，单击“云审计服务日志（CTS）”后的  ，在弹出的关闭确认窗口中单击“确认”关闭CTS日志检测，如**图 关闭云审计服务日志**所示。结束操作后，页面右上角提示“设置成功！”。

图 1-6 关闭云审计服务日志

步骤6 再次单击“云审计服务日志（CTS）”后的  ，开启CTS日志检测，页面右上角提示“设置成功！”，如**图 开启云审计服务日志**所示。

图 1-7 开启云审计服务日志



步骤7 在页面左上角选择“检测结果”进入检测结果页面，此时页面中“以下服务无法直接获取日志数据，需要您进行配置”的提示框已关闭，并且显示已开启云审计服务日志数据检测，表示配置追踪器成功。如**图 配置追踪器成功**所示。

图 1-8 配置追踪器成功

----结束

1.7 什么是 DGA 域名生成算法?

DGA(Domain Generate Algorithm域名生成算法)是一种使用时间，字典，硬编码的常量利用一定的算法生成的域名。 DGA生成的域名具有为随机性，用于中心结构的僵尸网络中与C&C服务器的连接，以逃避域名黑名单检测技术。

2 区域与可用区

2.1 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2-1阐明了区域和可用区之间的关系。

图 2-1 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**。

2.2 威胁检测服务可以跨区域使用吗?

不可以。

威胁检测服务是Region级服务，您只能在购买时选择的Region下使用。

3 购买咨询

3.1 购买 MTD 服务后，关闭所有日志数据源开关是否会计费?

购买MTD服务时您已支付所选套餐费用，之后若关闭日志数据源，不会额外计费。

在购买MTD服务后，只有当检测的日志数据源容量超过所购买的套餐容量后，才会额外**按需计费**。

3.2 威胁检测服务如何收费?

根据您选择的服务规格、使用时长和超出服务规格的检测量进行收费。

威胁检测服务提供包年/包月的计费方式，包年/包月支持入门包、初级包、基础包、高级包4种服务规格，您可以根据业务需求进行选购。同时，威胁检测服务还提供检测叠加包，当检测的日志数据源容量超过您所购买的服务规格后，威胁检测服务会自动为您购买检测叠加包，额外按需计费。

说明

如果您所购买的服务规格（入门包、初级包、基础包、高级包）到期，且未进行续购，MTD将根据您的使用情况按需计费。

有关MTD详细的计费说明，请参见**计费说明**。

详细的服务资费费率标准请参见**产品价格详情**。

3.3 威胁检测服务支持退订吗?

MTD暂不支持在管理控制台执行退订操作。

如果您不再使用威胁检测服务可以**提交工单**进行退订。

3.4 威胁检测服务到期后，如何续费?

威胁检测服务续费是在原已购买的服务规格的基础上，延长使用时间，因此续费操作不能变更服务规格。续费后，您可以继续使用威胁检测服务。

服务到期前，系统会以短信或邮件的形式提醒您服务即将到期，请您收到提醒后及时完成续费操作。

服务到期后，如果您没有按时续费，华为云将提供一定的资源保留期，保留期结束后，您的相关资源会被自动删除，且不能再找回资源，也不能再续费。关于保留期时长等信息请参考**资源停止服务或逾期释放说明**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在管理控制台界面上方，选择“费用与成本 > 续费管理”，进入费用中心“续费管理”页面。

步骤3 在“续费管理”页面，选择“手动续费项”页签。

步骤4 选中“产品类型”为“威胁检测服务”的所有待续费项，单击“批量续费”，跳转至“续费”页面。

步骤5 配置“续费时长”，如选择“9个月”。

步骤6 单击“去支付”，跳转至支付页面，完成付款。

步骤7 返回续费管理页面，可查看威胁检测服务已续费成功，确认倒计时天数。

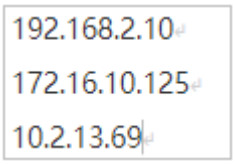
----结束

4 功能类

4.1 如何编辑 Plaintext 格式的对象?

创建打算上传至OBS桶的白名单和情报对象文件时，对象文件仅支持Plaintext格式，文件内可写入的IP或域名条数上限为10000条。

Plaintext格式即您想要上传至OBS桶的白名单列表或情报列表中，IP地址或域名范围必须用回车键隔开，每行只显示一个，如下图所示。



编辑好的对象文件格式建议存储为.txt的文件扩展名格式。

4.2 威胁检测服务是否支持自动防御措施?

威胁检测服务目前暂不支持自动防御措施功能。目前只支持对云服务（包含IAM服务、CTS服务、OBS服务、VPC服务、DNS服务）日志数据中的访问行为进行检测，去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。

4.3 如何通过主帐号对子帐号赋予 MTD 权限?

当您使用子帐号对服务进行创建检测引擎或其它操作时，需要您通过主帐号对子帐号进行授权才可使用子帐号对MTD服务进行操作。

前提条件

已经创建用户并添加到用户组。

步骤一：创建自定义策略

步骤1 登录统一身份认证服务控制台。

步骤2 在统一身份认证服务，左侧导航窗格中，选择“权限管理 > 权限”，单击右上方的“+创建自定义策略”。

图 4-1 创建自定义策略

步骤3 在“创建自定义策略”页面配置相关参数。

- “策略名称”：自定义。
- “作用范围”：“项目级服务”。
- “策略配置方式”：“可视化视图”
- “策略内容”：“允许”，选择“允许”。
  a. 在“允许”页签下选择“允许”。
  b. 在“云服务”页签，在搜索框中输入“MTD”搜索，选择“威胁检测服务(MTD)”。

图 4-2 输入策略名称

  c. 在所有操作页签，勾选“选择所有操作”。

图 4-3 选择所有操作

步骤4 单击“确定”。

----结束

步骤二：给用户的用户组授权

步骤1 在统一身份认证服务中，左侧导航栏选择“用户组”。

步骤2 在目标子帐号所属的用户组所在行的“操作”列，单击“权限配置”。

图 4-4 权限配置

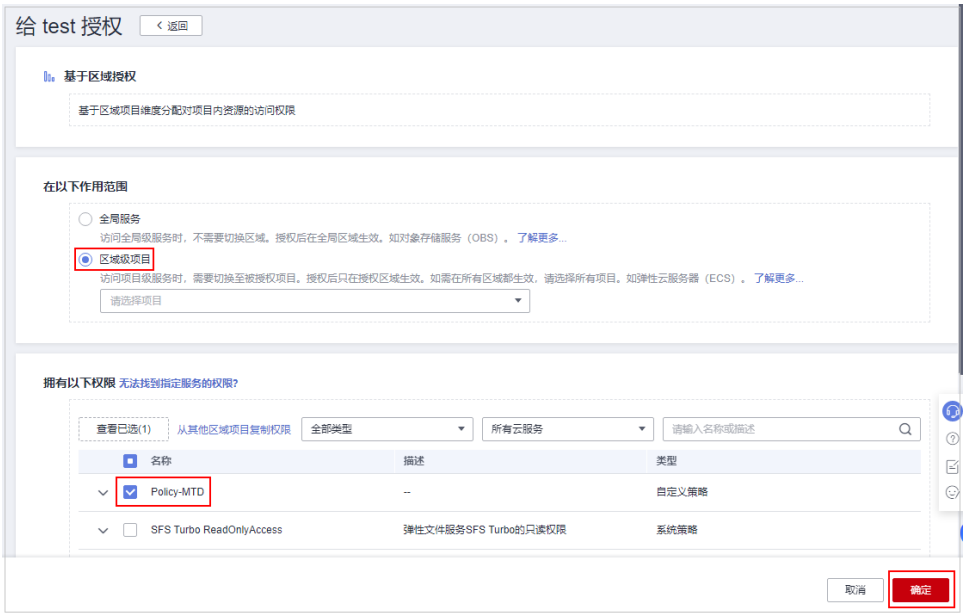
步骤3 在弹出的“授权记录”界面，单击“授权”。

图 4-5 授权

步骤4 在授权界面，“在以下作用范围”选择“区域级项目”。

步骤5 在“拥有以下权限”栏，选择**步骤一：创建自定义策略**配置好的策略。

图 4-6 给用户组授权自定义策略



步骤6 单击“确定”。

----结束

A 修订记录

发布日期	修改记录
2022-07-16	第十三次正式发布。 新增常见问题：**威胁检测服务如何收费？**、**威胁检测服务支持退订吗？**、**威胁检测服务到期后，如何续费？**。
2022-03-08	第十二次正式发布。 修改**什么是威胁检测服务？**。
2022-01-14	第十一次正式发布。 增加检查VPC能力，优化内容描述。
2021-12-03	第十次正式发布。 新增常见问题：**如何通过主帐号对子帐号赋予MTD权限?** 删除：威胁检测服务是否收费，能否免费使用? 删除：购买威胁检测服务（MTD）后，使用其他业务/服务出现token校验不通过怎么处理?
2021-11-30	第九次正式发布。 新增常见问题：**威胁检测服务可以跨区域使用吗?**
2021-11-17	第八次正式发布。 删除如何创建追踪器。
2021-09-29	第七次正式发布。 新增常见问题：**什么是DGA域名生成算法?**
2021-08-23	第六次正式发布。 新增：**购买MTD服务后，关闭所有日志数据源开关是否会计费?**

发布日期	修改记录
2021-07-10	第五次正式发布。 正式版本上线，修改章节如下： **什么是威胁检测服务？** **威胁检测服务的检测源头是什么？** **如何编辑Plaintext格式的对象？** **威胁检测服务购买后如何使用？** **威胁检测服务可以检测哪些风险？** **威胁检测服务是否支持自动防御措施？**
2021-07-02	第四次正式发布。 修改威胁检测服务是否收费，能否免费使用？章节。
2021-05-27	第三次正式发布。 新增用户使用过程出现的问题和一些常见问题，如下： **如何编辑Plaintext格式的对象？** 购买威胁检测服务（MTD）后，使用其他业务/服务出现token校验不通过怎么处理？ 威胁检测服务是否收费，能否免费使用？ **威胁检测服务购买后如何使用？** **威胁检测服务可以检测哪些风险？** **威胁检测服务是否支持自动防御措施？**
2021-04-27	第二次正式发布。 新增如何配置追踪器。
2021-01-20	第一次正式发布。