安全云脑

常见问题

文档版本 07

发布日期 2024-07-19

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 为什么没有看到攻击数据或者看到的攻击数据很少?

安全云脑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，安全云脑可能会显示您的系统当前遭受的攻击程度较低。

如果您认为安全云脑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。

1.2 安全云脑的数据来源是什么?

安全云脑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。
- 另一方面汇聚主机安全服务（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，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。

安全云脑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。

接入数据详细操作请参见**接入数据**。

1.3 安全云脑与其他安全服务之间的关系与区别?

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

- 关联：

  SecMaster：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SecMaster中，呈现全局安全威胁攻击态势。

- 区别：

  SecMaster：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。

SecMaster与其他安全防护服务区别，详细内容如**表1-1**。

表 1-1 SecMaster 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	功能差异
安全云脑（SecMaster）	安全管理	SecMaster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。	**SecMaster功能介绍**
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，相关攻击日志、防护等数据同步给SecMaster。	保障企业业务稳定性。	**Anti-DDoS功能特性**
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，相关告警、防护等数据同步给SecMaster。	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，阻断恶意流量攻击，防止对网站造成威胁。相关入侵日志、告警数据等同步给SecMaster，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，相关审计日志、告警数据等同步给SecMaster。	保障云上数据库安全和资产安全。	**DBSS产品介绍**

1.4 SecMaster 与 HSS 服务的区别?

服务含义区别

- 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。

- 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，SecMaster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

- SecMaster通过采集**全网安全数据**（包括HSS、WAF、AntiDDoS等安全服务检测数据），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。
- 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 SecMaster 与 HSS 主要功能区别

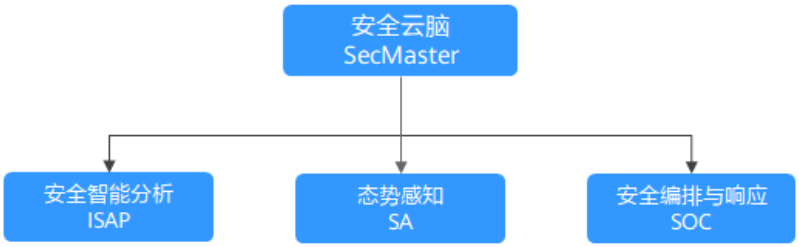
功能项		共同点	不同点
资产安全	主机资产	呈现主机资产的整体安全状态。	• SecMaster：仅支持同步HSS主机资产风险信息，呈现各主机资产的整体安全状况。 • HSS：不仅支持呈现主机的安全状况，还支持深度扫描主机中的账号、端口、进程、Web目录、软件信息和自启动任务。
	网站资产	-	• SecMaster：支持检查和扫描网站安全状态，呈现各网站资产的整体安全状况。 • HSS：不支持该功能。
漏洞管理	应急漏洞公告	-	• SecMaster：支持同步华为云安全公告信息，及时获取热点安全讯息。 • HSS：不支持该功能。
	主机漏洞	呈现主机漏洞扫描结果，管理主机漏洞。	• SecMaster：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。
基线检查	云服务基线	-	• SecMaster：针对华为云服务关键配置项，从“安全上云合规检查1.0”、“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。

功能项		共同点	不同点
	主机基线	-	• SecMaster：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。

1.5 安全云脑与态势感知服务的关系与区别?

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

图 1-1 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响应系统（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。

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。在购买安全云脑时，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。如果购买的最大配额小于主机数量，可能会造成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。

主机配额配置说明如**表1-3**所示。

表 1-3 主机配额参数说明

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。 **说明** • 主机配额最大限制为10000台。 • 为避免主机资产在防护配额外，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。

1.7 安全云脑支持跨账号使用吗?

支持。

安全云脑服务的空间托管功能支持跨账号安全运营，可实现Workspace委托集中安全运营查看统一资产风险、告警和事件等。

详细操作请参见**空间托管**。

1.8 如何更新安全评分?

安全云脑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。

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，选择区域和项目。

步骤3 在页面左上角单击 ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤4 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 1-2 进入目标工作空间管理页面

步骤5 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面，对不合格的基线检查项目进行处理。

步骤6 在左侧导航栏选择“风险预防 > 漏洞管理”，进入漏洞管理页面，对漏洞进行处理。

步骤7 在左侧导航栏选择“威胁运营 > 告警管理”，进入全部告警管理页面，对告警事件进行处理。

步骤8 相应基线、漏洞、告警处理后，返回“安全态势 > 态势总览”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**安全评分**。

1.9 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。

安全云脑联动主机安全服务（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，如果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。

- 如果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。
- 如果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 单击管理控制台左上角的，选择区域和项目。

步骤3 在页面左上角单击，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤4 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

图 1-3 进入目标工作空间管理页面

步骤5 在左侧导航栏选择“威胁运营 > 告警管理”，进入告警列表管理页面。

步骤6 选择“暴力破解”类型，刷新告警列表。

步骤7 选择目标告警，根据实际情况删除无威胁告警事件。

----结束

更多详情说明请参见**查看告警列表**。

1.10 数据同步或数据一致性相关问题

为什么 WAF、HSS 中的数据和 SecMaster 中的数据不一致?

由于SecMaster中汇聚了WAF、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SecMaster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。

为什么总览页面中没有显示资产总数?

问题现象:

工作空间新增完成后，在工作空间内的“资产管理”页面中同步并已显示资产信息，但是“总览”页面中的资产总数仍然显示为0。

图 1-4 总览无资产显示

问题原因：

工作空间创建成功，且资产等数据信息接入完成后，安全云脑将在**整点**进行数据同步，请耐心等待同步后再进行查看。

解决方法：

请您耐心等待，同步会系统将更新资产等相关数据信息。

1.11 如何给 IAM 子账号授权?

当您需要授予使用子账号操作安全云脑服务时，需要使用主账号对子账号进行授权操作。

操作步骤

步骤1 使用管理员账号登录管理控制台。

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 创建用户组。

1. 在左侧导航栏选择“用户组”，进入用户组页面后，单击右上角“创建用户组”。
2. 在创建用户组页面，设置用户组名称和描述信息。
   - 用户组名称：请设置为“SecMaster_ops”。
   - 描述：自定义描述信息即可。
3. 单击“确定”。

步骤4 新增自定义策略。

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：请设置为“SecMaster_FullAccess”。
   b. 策略配置方式：选择“JSON视图”。
   c. 策略内容：请直接复制粘贴以下内容。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "secmaster:*:*"
      ],
      "Effect": "Allow"
    }
```

```
    ]
}
```

a. 单击“确定”。

b. 并在弹出的对话框中，选择作用范围为“全局级范围”。

c. 单击“确定”。

图 1-5 创建策略

步骤5 给用户组授权。

1. 在左侧导航栏选择“用户组”，进入用户组页面后，单击“SecMaster_ops”，进入用户组详情页面。
2. 在“授权记录”页签中，单击“授权”。

图 1-6 角色授权

3. 在选择策略页面，搜索并选中“SecMaster_FullAccess”策略后，单击“下一步”。
4. 设置最小授权范围，请选择“所有资源”，设置完成后，单击“确定”。

步骤6 添加成功后显示如下：

图 1-7 授权成功

----结束

1.12 安全云脑中的日志存储时间是多久?

安全云脑支持接入WAF、HSS、OBS等云产品的日志数据，接入后可以对数据进行查询分析、智能建模等。

对于已接入安全云脑的日志数据的具体存储时长如下所示：

表 1-4 支持接入的日志

云服务	日志描述	日志	日志生命周期范围
Web应用防火墙（Web Application Firewall，WAF）	攻击日志	waf-attack	7~30 天
	访问日志	waf-access	
安全云脑（SecMaster）	合规基线日志	secmaster-baseline	7~10 天
入侵防御系统（Intrusion Prevention System，IPS）	攻击日志	nip-attack	7~30 天
威胁检测服务（Managed Threat Detection，MTD）	告警日志	mtd-alarm	7~30 天
主机安全服务（Host Security Service，HSS）	主机安全告警	hss-alarm	7~30 天
	主机漏洞扫描结果	hss-vul	7天
	主机安全日志	hss-log	7~15 天
云审计服务（Cloud Trace Service，CTS）	云审计服务日志	cts-audit	7~30 天
云防火墙（Cloud Firewall，CFW）	访问控制日志	cfw-block	7~30 天
	流量日志	cfw-flow	7~15 天
	攻击事件日志	cfw-risk	7~30 天

2 购买咨询

2.1 安全云脑如何变更版本规格?

购买安全云脑后，如果需要升级版本、增加资产配额或追加增值包功能，即需要升级版本、扩充“主机配额”或新增“增值包”。

须知

- 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和专业版。
- 增值包中的“安全大屏”、“智能分析”、“安全编排”为标准版和专业版额外选购付费项目，如需使用，请先购买标准版或专业版。

- 升级版本：详细操作请参见**升级版本**。
- 购买增值包：详细操作请参见**购买增值包**。
- 增加配额：详细操作请参见**增加资产配额**。

2.2 购买安全云脑时提示权限不足怎么办?

当您在购买安全云脑时，页面提示权限不足时，请参照以下步骤进行处理。

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“管理与监管 > 统一身份认证服务 IAM”，进入统一身份认证服务管理控制台。

步骤3 （可选）创建用户组。

如果已创建“SecMaster_ops”用户组，请跳过此步骤。

1. 在左侧导航栏选择“用户组”，进入用户组页面后，单击右上角“创建用户组”。

2. 在创建用户组页面，设置用户组名称和描述信息。
   - 用户组名称：请设置为“SecMaster_ops”。
   - 描述：自定义描述信息即可。
3. 单击“确定”。

步骤4 添加权限。

1. 添加全局级权限。
   a. 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”。
   b. 配置策略。
      - 策略名称：自定义。
      - 策略配置方式：选择“JSON视图”。
      - 策略内容：请直接复制粘贴以下内容。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:permissions:checkRoleForAgency",
                "iam:agencies:listAgencies",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:agencies:createAgency",
                "iam:permissions:grantRoleToAgency",
                "iam:permissions:grantRoleToAgencyOnProject"
            ]
        }
    ]
}
```

   c. 单击“确定”。
2. 添加项目级权限。
   a. 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”。
   b. 配置策略。
      - 策略名称：自定义。
      - 策略配置方式：选择“JSON视图”。
      - 策略内容：请直接复制粘贴以下内容。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "bss:order:pay",
                "bss:unsubscribe:update",
                "bss:order:view",
                "bss:balance:view",
                "bss:order:update",
                "ecs:cloudServers:list",
                "bss:renewal:view",
                "bss:renewal:update",
                "secmaster:*:*"
            ],
            "Effect": "Allow"
```



```
    }
  ]
}
```

c. 单击“确定”。

步骤5 给用户组授权。

1. 在左侧导航栏选择“用户组”，进入用户组页面后，单击“SecMaster_ops”，进入用户组详情页面。
2. 在“授权记录”页签中，单击“授权”。
3. 在选择策略页面，搜索并选中**步骤4**添加的权限后，单击“下一步”。
4. 设置最小授权范围，请选择“所有资源”，设置完成后，单击“确定”。
5. 添加成功后显示如下：

步骤6 将操作账号用户添加到用户组中。

1. 在左侧导航栏选择“用户组”，进入用户组页面。
2. 在“SecMaster_ops”用户组所在行“操作”列，单击“用户组管理”。
3. 在弹出的“用户组管理”对话框中，勾选需要添加的用户。
4. 单击“确定”。

----结束

2.3 如何释放 ECS 和 VPC 终端节点资源?

在使用数据采集功能时，需要购买ECS节点（用于采集数据）、新增并配置VPC终端节点（用于连通和管理采集节点）。

- ECS购买后，系统将根据使用情况进行收费，具体收费情况请参见**ECS计费说明**。
- VPC终端节点配置后，系统将根据使用情况进行收费，具体收费情况请参见**VPC终端节点计费说明**。

如果不再使用数据采集功能或退订安全云脑后，需要手动释放创建的ECS资源和VPC终端节点资源，避免继续计费。具体操作步骤如下：

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，选择区域和项目。

步骤3 释放用于采集数据的ECS资源。

1. 在页面左上角单击，选择“计算 > 弹性云服务器”，进入弹性云服务器管理控制台。
2. 在资源列表中找到用于采集数据ECS资源，并在目标ECS资源所在行“操作”列的“更多 > 退订”或“更多 > 删除”。

图 2-1 退订 ECS

3. 在弹出的确认框中，根据界面提示进行退订/删除ECS资源处理，完成ECS资源释放操作。

步骤4 释放用于连通和管理采集节点的VPC终端节点资源。

1. 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。
2. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。
3. 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。
4. 注销节点。
   a. 在节点管理页面中，单击目标节点所在行“操作”列的“注销”。
   b. 在弹出的确认框中，单击“确认”。
5. 删除VPC终端节点。
   a. 在节点管理页面中，单击“新增”，并在弹出新增节点页面中，选择网络节点。
   b. 在网络通道列表中，单击“删除”。

图 2-2 删除节点

   c. 在弹出的确认框中，单击“确认”。
6. 查看是否还有安全云脑创建的用于数据采集的未释放的VPC终端节点。
   a. 在页面左上角单击 ☰，选择“网络 > VPC终端节点”，进入VPC终端节点管理控制台。
   b. 在终端节点搜索框中，输入“isap”，并按“Enter”，搜索与安全云脑数据采集相关的VPC终端节点。
   c. 查看是否还有安全云脑创建的用于数据采集的未释放的VPC终端节点。
      - 无：继续执行**步骤4.7**。

图 2-3 删除 VPCEP

- 有：确认需删除后，单击目标VPC终端节点所在行“操作”列的“删除”，并在弹出的确认框中单击“是”。

图 2-4 删除 VPCEP

删除完成后，继续执行**步骤4.7**。

7. 查看是否还有安全云脑相关的VPC终端节点仍在计费。
   - 有：请联系华为云技术支持进行处理。
   - 无：处理完毕。

----结束

2.4 如何将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。

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”，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 2-5 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 > 安全云脑 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**安全云脑介绍文档**。

----结束

3 数据采集故障排查

3.1 组件控制器安装失败

数据采集时，需要在ECS上安装组件控制器（isap-agent），当出现安装失败等问题时，请参照本章节进行排查处理：

排查过程中，常用命令请参见**组件控制器常用命令**。

可能原因

组件控制器（isap-agent）安装失败的可能原因如下：

- 待安装组件控制器（isap-agent）的ECS服务器与存储Agent的OBS桶之间网络不通
- ECS服务器的磁盘空间不足
- 调用iamtoken请求，获取iamtoken失败
- workspaceId校验失败
- 组件控制器（isap-agent）已经安装，系统仍将重复安装

原因排查及解决方法

- **待安装组件控制器（isap-agent）的ECS服务器与存储Agent的OBS桶之间网络不通**

  图 3-1 主机与 OBS 网络不通

  解决方法：

  - （可选）方法一：将ECS主机与OBS的网络连通。
  - （可选）方法二：手动将安装脚本以及安装包下载到本地后，再将安装包上传到主机的“/opt/cloud”路径下。

    i. 登录OBS管理控制台。

ii. 在左侧导航栏选择“桶列表”，并单击目标桶名称，进入桶对象管理页面。

iii. 单击目标桶对象名称，进入桶对象详情页面后，下载安装脚本和安装包。

iv. 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。

v. 将安装包上传到主机的“/opt/cloud”路径下。

- **ECS主机的磁盘空间不足**

  图 3-2 磁盘空间不足

  解决方法：

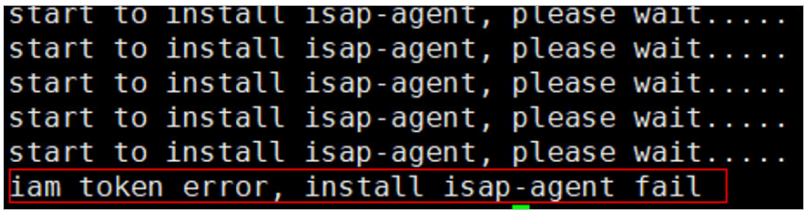
  清理磁盘，预留足够空间。

- **调用iamtoken请求，获取iamtoken失败**

  - **问题现象**

    当日志出现如下图所示信息时，则表示调用iamtoken请求，获取iamtoken失败。

    图 3-3 获取 iamtoken 失败

  - **排查步骤和解决方法**

    i. 确认执行命令中的IAM账号或用户名是否有误。

    图 3-4 IAM 用户名和密码

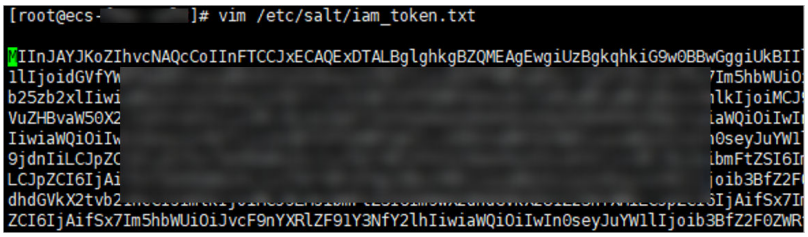
    

    - 有误，修改命令中的IAM账号或用户名后再次执行安装命令。
    - 无误，继续执行**ii**。

    ii. 执行**vim /etc/salt/iam_token.txt**命令，查看“/etc/salt/iam_token.txt”文件检查是否存在。

    - 当出现如下图信息时，则表示存在，继续执行**iii**。

图 3-5 检查文件



- 如果提示文件不存在，请联系技术支持进行处理。

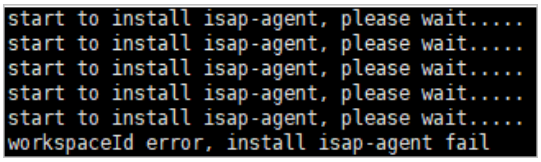
iii. 执行**ping** 命令，检查主机是否可以连通网络地址，如果不通，用户需要打通网络。

图 3-6 检查网络

- **workspaceId校验失败**
  - **问题现象**

    当日志出现如下图所示信息时，则表示Workspace ID校验失败。

图 3-7 workspaceId 校验失败



  - **解决方法**

    i. 登录安全云脑管理控制台。

    ii. 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。

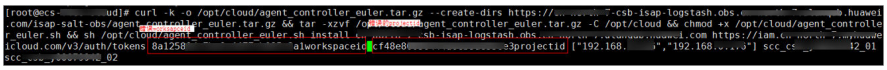
    iii. 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点名称。

    iv. 查看执行命令中的workspaceId和projectId。

图 3-8 控制台中的参数信息

    v. 查看实际运行命令中的workspaceId和projectId，是否与**iv**中的一致。

图 3-9 命令中的参数信息

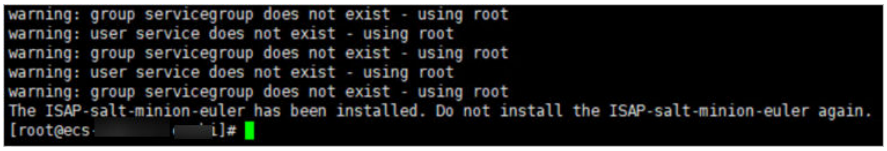


vi. 修改实际执行命令中的workspaceId和projectId。

- **组件控制器（isap-agent）已经安装，系统仍将重复安装**
  - **问题现象**

    当日志出现如下图所示信息时，则表示Agent已经安装。

    图 3-10 Agent 重复安装

  - **解决方法**

    i. （可选）方法一：通过管理控制台注销该节点。

    1) 登录安全云脑管理控制台。
    2) 在左侧导航栏选择“工作空间 > 空间管理”，并在工作空间列表中，单击目标工作空间名称，进入目标工作空间管理页面。
    3) 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，单击目标节点所在行“操作”列的“注销”。
    4) 在弹出的确认框中，单击“确认”。

    ii. （可选）方法二：通过脚本命令卸载组件控制器（isap-agent）。

    1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
    2) 执行**sh /opt/cloud/agent_controller_euler.sh uninstall**命令，卸载组件控制器。

    iii. 检查是否已完成卸载。

    1) 通过远程管理工具（如：SecureFX、WinSCP）远程登录目标云服务器。
    2) （可选）方法一：执行**ls -a /opt/cloud/**查看“/opt/cloud”目录下的文件，当提示如下图所示信息（只有脚本文件）时，则表示已完成卸载。

    图 3-11 脚本文件

    3) （可选）方法二：执行**salt-minion --version**命令，当提示如下图所示信息时，则表示已卸载完成。

    图 3-12 检查 isap-agent 信息

注意

节点注销需要一定的时间，不建议执行完注销立刻安装。

3.2 采集节点或采集通道故障

问题现象

采集节点状态和采集通道健康状态采用isap-agent定时上报机制，虽然存在一定的延迟（预计一分钟），但是在采集通道下发3分钟后，采集节点和采集通道的“健康状态”依然显示为“故障”，并且该服务器的CPU使用率或内存使用率即将达到100%。

图 3-13 采集节点故障

图 3-14 采集通道故障

可能原因

用户配置的连接器或解析器在语法或者语义上存在错误，导致采集器无法正常运行，不断重启导致CPU、内存被占满。

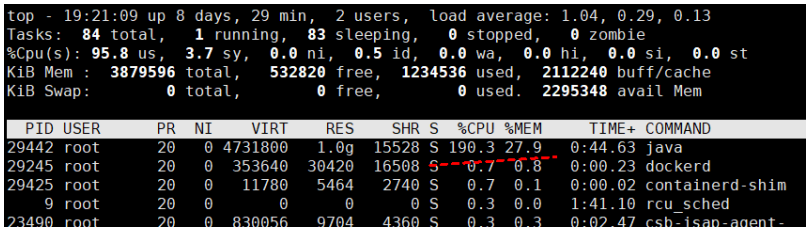
问题定位

1. 远程登录采集节点所在的ECS。
   - 您可以登录弹性云服务器控制台，在“弹性云服务器”列表中，单击“远程登录”登录主机，详细操作请参见**在云服务器控制台上登录主机**。
   - 如果您的主机已经绑定了弹性IP，您也可以使用远程管理工具（例如：PuTTY、Xshell等）登录主机，并使用root账号在主机中安装组件控制器。
2. 执行如下命令，命令查看当前系统的运行状态：

   top

   当显示如下图所示时，则表示ECS中Java进程占用了大量CPU资源。

图 3-15 运行状态

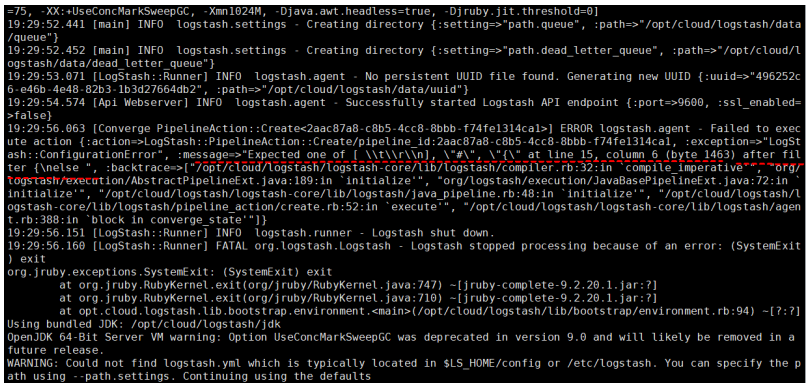


3. 执行如下命令，查看采集器运行日志：

   docker logs isap-logstash -f

   通过查看日志，定位到当前采集通道filter部分（解析器）配置有误，如下图所示：

图 3-16 采集器运行日志



4. 执行以下命令，进入采集通道配置文件所在路径。

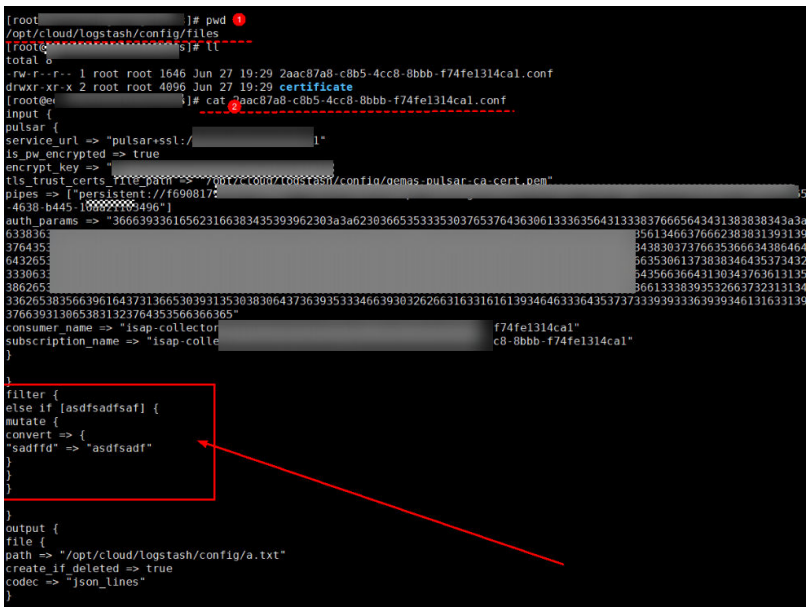
   cd /opt/cloud/logstash/config/files

5. 执行以下命令，查看filter部分是否存在异常。

   cat *配置文件名*

   当出现如下图所示内容时，则表示当前filter部分存在异常：

图 3-17 filter 部分存在异常



处理步骤

步骤1 登录安全云脑管理控制台，并进入目标工作空间。

步骤2 在左侧导航栏选择“设置 > 采集管理”，进入采集管理页面后，选择“解析器管理”页签，进入解析器管理页面。

步骤3 单击目标解析器所在行操作列的“编辑”，并在编辑页面中，删除错误配置信息，修改为正确的配置信息。

图 3-18 问题解析器配置

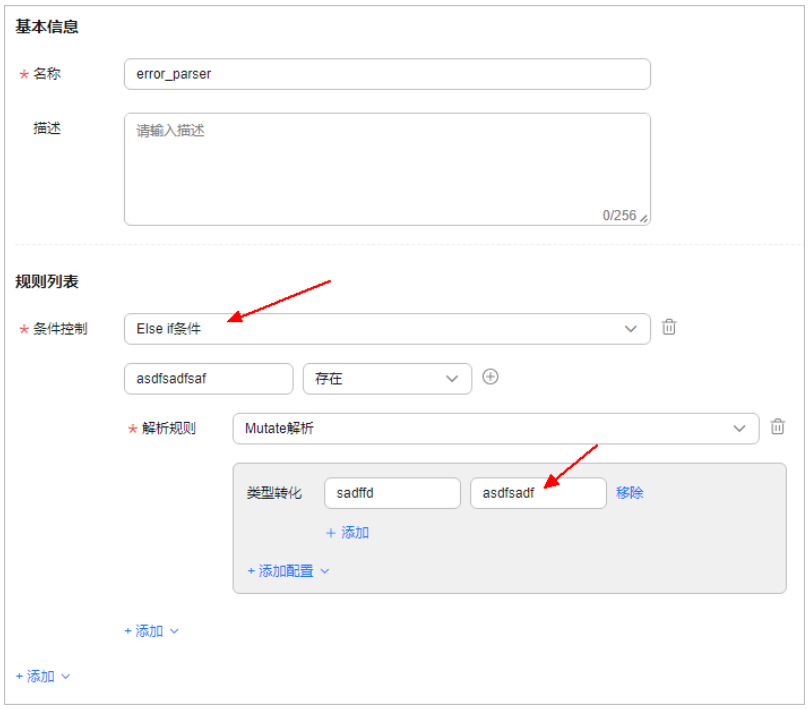
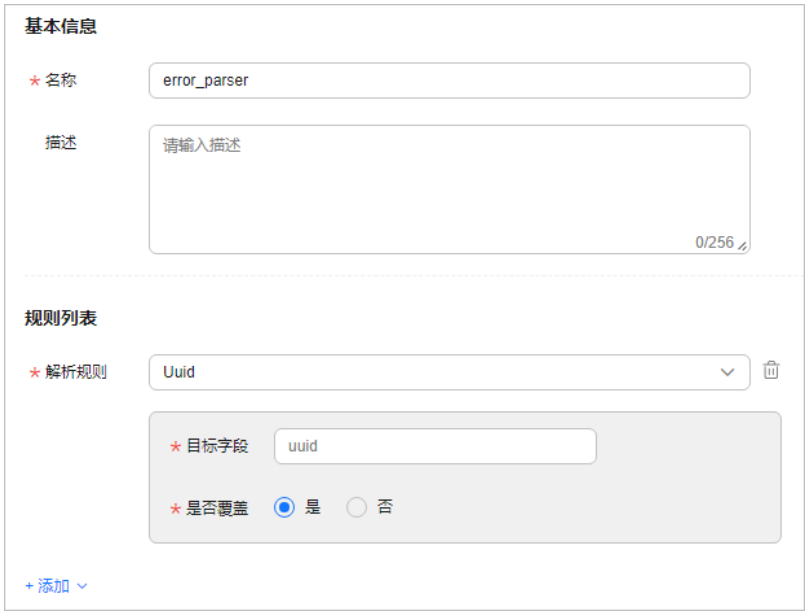


图 3-19 修改解析器配置



步骤4 单击“确定”。

步骤5 编辑完成后，在上方选择“采集通道管理”页签，并单击目标采集通道操作列的“重启”，重启采集通道。

图 3-20 重启采集通道

步骤6 检查采集通道和采集节点状态。

- 重启完成后，在“采集通道管理”页面中，检查目标采集通道的健康状态。

  图 3-21 采集通道健康状态

- 在上方选择“采集节点管理”页签，页面，检查目标采集节点的健康状态。

  图 3-22 采集节点健康状态

当采集通道和采集节点的“健康状态”均显示为“正常”时，则表示问题处理成功。

----结束

3.3 组件控制器常用命令

如果组件控制器（isap-agent）安装失败，在故障排查过程中，可能需要使用命令进行处理，其中，常用命令如下：

- 重启

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh restart

  说明：使用此命令将先停止isap-agent进程，并重新启动该进程。此命令用于isap-agent启动失败，或者节点因为机器故障导致的进程不存在情况。

- 启动

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh start

  说明：当isap-agent因为机器宕机，容灾自拉起时间未到，用户可使用此命令启动isap-agent。

- 停止

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh stop

  说明：此命令用于停止isap-agent，使用此命令将自动清理定时自拉起检测，使得isap-agent进程停止。

- 查看进程

  ps -ef|grep isap-agent

  说明：此命令用于查看当前机器上isap-agent是否存在。

- 查看日志

  tail -100f /opt/cloud/isap-agent/log/run.log

  说明：用于查看isap-agent服务，最近100行日志，用于通过日志定位agent异常问题。

- 磁盘分区

  sh /opt/cloud/isap-agent/action/agent_controller_linux.sh partition

  说明：用于在节点安装采集器，手动挂载磁盘，并进行磁盘分区的场景。

4 区域与可用区

4.1 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4-1阐明了区域和可用区之间的关系。

图 4-1 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?

在欧洲地区有业务的用户，可以选择“欧洲-都柏林”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。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。
  - 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“南非-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”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**。

4.2 为什么 Global 级项目有 region 级的选择框显示?

安全云脑属于Global级项目，但是，在控制台上还是有Region级的选择框提示：

图 4-2 region 选择框

具体原因如下：

- 方便切换区域

  如果您进入的region未部署安全云脑，可以在此处切换至已部署区域。

- 统一管理数据

  为了统一管理数据，安全云脑将区域（Region）划分了合规分区。在相同合规分区内的数据可以聚合在一起，不同合规区内的数据无法聚合在一起。安全云脑中的具体合规分区如下：

  表 4-1 合规分区

region名称	所属安全云脑合规分区
华北-北京四	国内站
华北-乌兰察布一	
华东-上海一	
华东-上海二	
华南-广州	
华南-深圳	
西南-贵阳一	
华北-乌兰察布-汽车一	华北-乌兰察布-汽车一
中国-香港	中国-香港
亚太-曼谷	亚太-曼谷
亚太-新加坡	亚太-新加坡
亚太-雅加达	亚太-雅加达
土耳其-伊斯坦布尔	欧洲站
拉美-墨西哥城二	拉美-墨西哥城二
拉美-圣保罗一	拉美-圣保罗一
中东-利雅得	中东-利雅得

