安全云脑

最佳实践

文档版本	03
发布日期	2024-11-15

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 日志接入或转出操作指导.....1
1.1 方案概述.....1
1.2 资源规划.....2
1.3 操作流程.....3
1.4 实施步骤.....4
1.4.1 （可选）步骤一：购买 ECS.....4
1.4.2 （可选）步骤二：购买数据磁盘.....6
1.4.3 （可选）步骤三：挂载数据磁盘.....8
1.4.4 步骤四：创建非管理员 IAM 账户.....9
1.4.5 步骤五：网络连通配置.....11
1.4.6 步骤六：安装组件控制器（isap-agent）.....12
1.4.7 步骤七：安装日志采集组件（Logstash）.....14
1.4.8 （可选）步骤八：创建日志存储管道.....15
1.4.9 步骤九：配置连接器.....18
1.4.10 （可选）步骤十：配置日志解析器.....22
1.4.11 步骤十一：配置日志采集通道.....24
1.4.12 步骤十二：测试验证.....26
2 凭证泄露响应方案.....29

1 日志接入或转出操作指导

1.1 方案概述

安全云脑的日志采集功能支持将安全日志接入安全云脑，同时，也支持将安全云脑日志转出至第三方系统/产品。

表 1-1 日志接入或转出场景说明

场景	操作指导
华为云日志接入安全云脑	参见**接入云服务日志**。
安全云脑日志转出至第三方系统/产品	参考本实践的操作步骤处理即可
第三方（非华为云）日志接入安全云脑	参考本实践的操作步骤处理即可

日志采集原理

日志采集器节点作为中间节点，负责在安全云脑和租户服务器之间收集、上传、下发日志。

图 1-1 安全云脑日志采集原理

基本概念

本部分介绍日志采集中涉及的基本概念的描述及其作用。

- 日志采集组件（Logstash）：用于日志采集、日志传输。
- 组件控制器（isap-agent）：用于管理日志采集组件（Logstash）等。

- **日志采集器节点：用于采集日志到云脑，以及安全云脑日志转出。**
  一台ECS，安装了安全云脑组件控制器，组件控制器中安装了日志采集组件。单个租户只需要配置安装一台日志采集器节点。

  图 1-2 日志采集器节点架构图

- 采集器：定制化的Logstash。采集器节点则是定制化的Logstash+组件控制器（isap-agent）。
- 连接器：Logstash配置的基础概念，主要包括input、output两部分，分别对应源连接器、目的连接器，用于定义采集器Logstash接受数据方式和规范。其中，安全云脑管道pipe连接器可以对接安全云脑，实现租户数据上报安全云脑，安全云脑数据转储到租户的能力。
- 解析器：Logstash配置的基础概念，主要为Logstash的filter部分，安全云脑解析器是对其filter部分的无码化封装和定制，用户只需在页面上配置解析器规则即可生成原生的filter配置脚本，从而轻松实现将原始日志转化为目标格式。
- 采集通道：采集通道等价于Logstash的pipeline，在Logstash可以配置多个pipeline，每个pipeline包括input、filter、output部分，每个pipeline为单独的作业，互不影响。在安全云脑租户采集上，可将相同的pipeline部署在多个节点上，并且配置相同的pipeline视为一个采集通道。

1.2 资源规划

账户

具有安全云脑数据采集管理权限，且非管理员的IAM账户。

ECS 规格要求

安装采集器（isap-agent + Logstash）的租户云服务器（ECS）规格要求如下表：

表 1-2 ECS 规格

CPU内核数	内存大小	系统磁盘存储大小	数据磁盘存储大小	采集器参考处理能力
4核	8G	50G	100G	4000 EPS @ 500B

CPU内核数	内存大小	系统磁盘存储大小	数据磁盘存储大小	采集器参考处理能力
8核	16G	50G	100G	10000 EPS @ 500B
16核	32G	50G	100G	20000 EPS @ 500B
32核	64G	50G	100G	40000 EPS @ 500B
64核	128G	50G	100G	80000 EPS @ 500B

规格说明：

- 4000 EPS @ 500B：日志采集器每秒可以处理4000次数据。条件：单个数据大小为500字节（500B）情况下。
- ECS规格**最低要求**：**CPU2核，内存4 GB，系统磁盘50 GB，数据磁盘100 GB**。
- 架构要求：当前日志采集组件控制器（isap-agent）仅支持运行在Linux系统和Arm64架构的ECS主机上，后续更多环境适配持续更新中。
- 操作系统（镜像）：无限制，建议Huawei Cloud EulerOS。
- 日志量应当与机器规格成比例放大，建议按表中规格比例进行放大。如果机器压力较大，建议部署多台采集器，通过采集通道来统一管理，分摊单机日志中转压力。

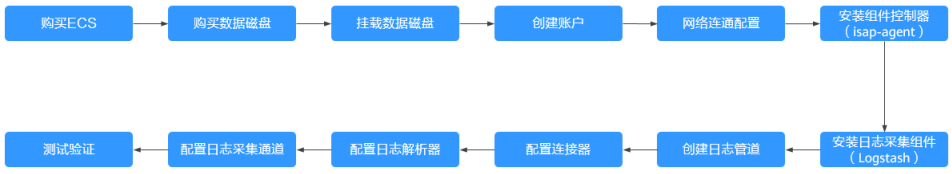
接入日志数量

无限制，可随云资源配置变化而动态扩展。

1.3 操作流程

本章节介绍如何将第三方（非华为云）安全日志接入安全云脑，同时，也支持将安全云脑日志转出至第三方系统/产品。具体流程如下：

图 1-3 日志接入或转出流程图



本章节将介绍日志数据接入或转出的操作流程进行简要说明。

表1 日志接入或转出流程说明

操作步骤	操作说明
（可选）步骤一：购买ECS	安装日志采集器。
（可选）步骤二：购买数据磁盘	保障日志采集器有足够的运行空间。
（可选）步骤三：挂载数据磁盘	保障日志采集器有足够的运行空间。
步骤四：创建非管理员IAM账户	用于租户侧日志采集器登录访问安全云脑。
步骤五：网络连通配置	实现租户VPC与云脑网络网络连通。
步骤六：安装组件控制器（isap-agent）	纳管日志采集器节点（ECS）到安全云脑。
步骤七：安装日志采集组件（Logstash）	配置日志采集进程。
（可选）步骤八：创建日志存储管道	**将非华为云日志转入安全云脑场景时，需要执行此步骤。将华为云日志转出至第三方系统或产品场景，请跳过此步骤。** 在安全云脑中创建日志存储位置（管道），用于日志存储、分析。
步骤九：配置连接器	配置日志来源、接收目的的参数信息。 请根据场景选择操作步骤： • 将第三方日志接入安全云脑 • 将安全云脑日志转出至第三方系统或产品
（可选）步骤十：配置日志解析器	格式转换，无码化将源日志转换成您需要的数据类型。
步骤十一：配置日志采集通道	完成各功能组件连接，实现安全云脑和日志采集器正常工作。
步骤十二：测试验证	测试验证日志是否接入成功。

1.4 实施步骤

1.4.1 （可选）步骤一：购买 ECS

本章节将介绍如何购买ECS，用于安装日志采集器。

采集数据需要一台用于安装日志采集的各项配置的ECS主机，且ECS的系统内存 ≥ 50 GB。若已有满足条件的ECS，则跳过此步骤。

前提条件

已获取IAM管理员账号信息。

操作步骤

步骤1 查看ECS信息。

1. 使用IAM管理员账号登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目后，单击页面左上方的 ，选择“计算 > 弹性云服务器 ECS”。
3. 在弹性云服务器ECS列表页面中，单击已有或已购ECS名称，进入ECS详情页面。
4. 查看已有或已购ECS的**可用区**、**规格**、**镜像**、**系统盘**、**数据盘**信息。

图 1-4 查看 ECS 信息

5. 确认ECS系统盘是否大于等于50GB。
   - 是：跳过步骤一：购买ECS，执行（可选）步骤二：购买数据磁盘。
   - 否：继续执行步骤2，购买弹性云服务器ECS。

步骤2 返回弹性云服务器页面，单击页面右上角的“购买弹性云服务器”。

步骤3 在购买页面配置ECS购买参数信息。

表 1-3 ECS 购买参数说明

参数名称		配置说明
基础配置		根据需要自定义配置“计费模式”和“区域”。 其中，“可用区”如果没有特殊要求，建议选择“随机分配”。
实例	CPU架构	请选择“x86计算”。 目前，日志采集器的组件控制器（isap-agent）仅支持运行在Linux系统X86_64和Arm64架构的ECS主机上，因此，此处请选择“x86计算”。
	实例筛选	最低要求**CPU 2核，内存4 GB**，根据需要选择符合要求的实例。
操作系统	镜像	建议选择“公共镜像 > Huawei Cloud EulerOS”后，根据需要选择镜像。 由于名称中带有“制作资源专用不支持密码注入”描述的镜像无法使用密码进行登录，因此**请勿选择**此类镜像。 选择镜像后，是否“开启安全防护”根据需要自定义配置。

参数名称		配置说明
存储与备份	系统盘	最低要求**系统磁盘50 GB**。 根据需要选择符合要求的系统盘。
	数据盘	最低要求**数据磁盘100 GB**。 单击“增加一块数据盘”，根据需要选择符合要求的数据盘。
	开启备份	根据需要自定义配置。
网络	虚拟私有云	根据需要自定义配置。 配置后，请**记录**此处选择的**虚拟私有云**和**主网卡**信息，方便后续使用。
	主网卡	
安全组		根据需要自定义配置。
公网访问		根据需要自定义配置。
云服务器管理		根据需要自定义配置。 配置后，请**记录**此处设置的**云服务器名称**、**用户名**、**密码**信息，方便后续使用。
高级配置		根据需要自定义配置。
购买量		根据需要自定义配置。

步骤4 确认参数配置无误后，勾选协议并单击“立即购买”。

步骤5 在订单页面，选择付款方式完成付款，完成购买操作。

----结束

1.4.2 （可选）步骤二：购买数据磁盘

本章节将介绍如何购买数据磁盘，保障日志采集器有足够的运行空间。

ECS中有用于采集管理的日志采集器的空闲数据盘，此数据磁盘需要和已有的ECS属于同一可用区，且磁盘容量 ≥ 100 GB。

如果参照**（可选）步骤一：购买ECS**时已购买且配置了数据磁盘，则请跳过该步骤。否则执行当前步骤购买数据磁盘。

操作步骤

步骤1 查看数据磁盘信息。

1. 使用IAM管理员账号登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目后，单击页面左上方的 ，选择“存储 > 云硬盘 EVS”。
3. 在磁盘列表页面中，单击已有或已购EVS名称，进入EVS详情页面。
4. 查看已有或已购EVS的**名称**、**可用区**、**容量**、**磁盘属性**信息。

图 1-5 查看数据磁盘信息

5. 确认数据磁盘是否和已有的ECS属于同一可用区，且磁盘容量 ≥ 100 GB。
   - 是：跳过该步骤，执行**（可选）步骤三：挂载数据磁盘**。
   - 否：继续执行**步骤2**，购买数据磁盘。

步骤2 返回云硬盘页面，单击页面右上角“购买磁盘”。

步骤3 在购买页面配置磁盘购买参数信息。

表 1-4 磁盘购买参数说明

参数名称	配置说明
区域	请选择与**（可选）步骤一：购买ECS**中ECS相同的区域。
可用区	请选择与**（可选）步骤一：购买ECS**中ECS相同的可用区。
挂载到云服务器	请选择“立即挂载”，并单击“选择云服务器”，再选择**（可选）步骤一：购买ECS**中已购买的ECS或当前已有的可用ECS后，单击“确定”。
计费模式	根据需要自定义配置，建议和ECS计费模式保持一致。
数据源	根据需要自定义配置。
磁盘规格	• 磁盘类型：根据需要自定义配置。 • 容量 (GiB)：最低要求**数据磁盘100 GB**。请根据需要选择符合要求的数据盘。
当前已选	展示当前已选择磁盘配置信息，无需配置。
云备份	根据需要自定义配置。
更多	根据需要自定义配置。
企业项目	根据需要自定义配置。 若无特殊要求“企业项目”建议选“default”。
磁盘名称	根据需要自定义配置。
购买量	根据需要自定义配置。

步骤4 确认参数配置无误后，单击“立即购买”。

步骤5 在订单页面，根据界面提示完成购买操作。

> **⚠ 注意**
>
> 购买完成后，不需要初始化，后续**网络连通配置**会自动进行初始化配置。

----结束

1.4.3 （可选）步骤三：挂载数据磁盘

本章节将介绍如何挂载数据磁盘到符合条件的ECS上。

需要将符合条件的数据磁盘挂载在已有的符合条件的ECS上，保障日志采集器有足够的运行空间。若满足以下任一场景则无需执行此步骤：

- 场景一：参考**（可选）步骤一：购买ECS**时已经了购买符合条件的ECS和数据磁盘，且磁盘已挂载到ECS，则无需执行此步骤。
- 场景二：已有符合条件的ECS（未参考**（可选）步骤一：购买ECS**进行购买），且参考**（可选）步骤二：购买数据磁盘**购买了符合条件的数据磁盘，购买数据磁盘时已经执行了数据磁盘挂载到云服务器ECS的操作，则无需执行此步骤。

操作步骤

步骤1 如果您已有符合条件的ECS，且有符合条件的数据磁盘，查看数据盘是否已挂载在ECS中。

1. 使用IAM管理员账号登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目后，单击页面左上方的 ☰，选择“计算 > 弹性云服务器 ECS”。
3. 在弹性云服务器页面中，单击符合条件的ECS名称，进入ECS详情页面。
4. 选择“云硬盘”页签后，在云硬盘页面中查看是否已挂载符合要求的数据盘。
   - 是：已挂载，则跳过该步骤，执行**步骤四：创建非管理员IAM账户**。
   - 否：未挂载，继续执行**步骤2**，挂载数据磁盘到ECS。

图 1-6 查看已挂载数据磁盘

步骤2 在云硬盘页面中单击“挂载磁盘”，并在挂载磁盘弹窗中，勾选符合条件的数据磁盘，单击“确定”。

图 1-7 挂载磁盘

----结束

1.4.4 步骤四：创建非管理员 IAM 账户

本章节介绍如何创建非管理员IAM账户。

租户采集的鉴权采用的是IAM鉴权，因此需要创建拥有安全云脑接口访问权限的IAM最小权限账户（机机账户），同时禁止开启MFA。该账户主要用于租户侧日志采集器登录并访问安全云脑。

操作步骤

步骤1 使用IAM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 IAM”，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“租户采集用户组”。
   - 描述：自定义描述信息即可。
3. 单击“确定”。

步骤4 添加权限。

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。
   - 策略名称：请设置为“租户采集最小权限策略”。
   - 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": [
                "secmaster:workspace:get",
                "secmaster:node:create",
                "secmaster:node:monitor",
                "secmaster:node:taskQueueDetail" ,
```



```
            "secmaster:node:updateTaskNodeStatus"
          ]
        }
      ]
    }
```

3. 单击“确定”。

步骤5 给用户组授权。

1. 在统一身份认证服务IAM管理控制台的左侧导航栏选择“用户组”，进入用户组页面后，选择并单击**步骤3**创建的用户组“租户采集用户组”名称，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“租户采集最小权限策略”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 创建用户。

1. 在统一身份认证服务IAM管理控制台的左侧导航栏选择“用户”，进入用户页面后，单击右上角“创建用户”。
2. 配置用户基本信息。

表 1-5 用户基本信息

参数名称		配置说明
用户信息		自定义配置。 设置后，记录此处IAM**用户名**信息（IAM User Name），方便后续使用。
访问方式	编程访问	勾选。
	管理控制台访问	不勾选。
凭证类型	访问密钥	勾选。
	密码	勾选。 勾选密码后，勾选“自定义”，并自定义设置密码。设置后，记录此处IAM用户**密码**信息（IAM User Password），方便后续使用。

3. 单击页面右下角“下一步”，进入加入用户组页面。
4. 搜索并选中**步骤3**创建的用户组“租户采集用户组”，单击右下角“创建用户”。

步骤7 确认用户未绑定虚拟MFA设备。

1. 在统一身份认证服务IAM管理控制台的左侧导航栏选择“用户”，进入用户页面后单击**步骤6**创建的用户的名称。
2. 选择“安全设置”页签，并确认“虚拟MFA设备”的状态为“未绑定”。

步骤8 查看IAM用户的域账号信息。

1. 将鼠标悬停至控制台右上角用户名上，并在下拉框中选择“我的凭证”。

2. 在API凭证信息中，查看并记录账号名，此信息则为后续安装isap-agent的域账号信息。

图 1-8 域账号信息

----结束

1.4.5 步骤五：网络连通配置

采集数据前，需要进行网络连通配置，以便实现租户VPC与安全云脑的网络连通。

操作步骤

步骤1 已开通付费版安全云脑服务，且已创建工作空间。

详细操作请参见**购买安全云脑**、**新增工作空间**。

步骤2 登录管理控制台。

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 1-9 进入目标工作空间管理页面

步骤5 在左侧导航栏选择“设置 > 组件管理”，默认进入节点管理页面。

图 1-10 进入节点管理页面

步骤6 在节点管理页面中，单击“新增”，页面右侧弹出新增节点页面。

步骤7 在新增节点页面中，配置通道。

图 1-11 新增节点

1. 在网络通道配置栏中，选择（可选）步骤一：购买ECS中记录的ECS所属的虚拟私有云和子网。
2. 在网络通道列表中，单击**所有通道**操作列的“配置”，并在弹出的确认框中，单击“确定”。

   当所有通道的状态为已接受时，则表示网络通道配置完成。

图 1-12 网络通道配置完成

说明

VPC终端节点（用于连通和管理采集节点）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**。

后续如果不再使用数据采集功能，需要手动释放用于连通和管理采集节点的VPC终端节点，详细操作请参见**删除终端节点**。

----结束

1.4.6 步骤六：安装组件控制器（isap-agent）

本章节介绍如何安装安全云脑组件控制器（isap-agent），将日志采集器节点（ECS）纳管到安全云脑。

操作步骤

步骤1 在**步骤五：网络连通配置**执行后的页面中，单击页面右下角“下一步”，进入“脚本安装验证”页面。

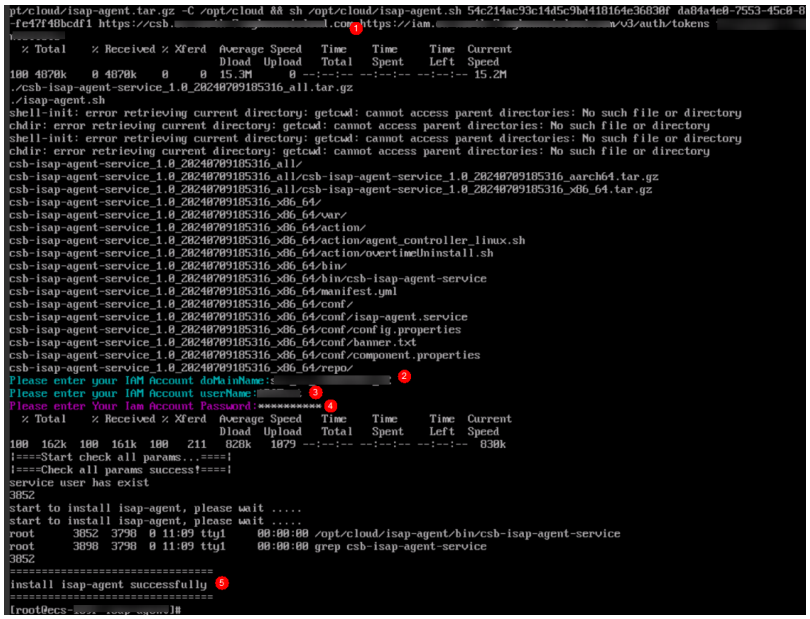
步骤2 单击 复制安装组件控制器的命令。

图 1-13 复制安装命令

步骤3 安装组件控制器。

1. 远程登录（可选）**步骤一：购买ECS**准备的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，选中目标ECS单击操作”列的“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. 粘贴**步骤2**复制的安装命令，并以root权限执行，在ECS中安装组件控制器。
3. 根据界面提示，输入**步骤四：创建非管理员IAM账户**中创建的机机账户域名、用户名、密码。
4. 如果界面回显“install isap-agent successfully”信息时，则表示组件控制器安装成功。

图 1-14 安装成功



安装过程中，如果安装失败请参考**组件控制器安装失败问题排查**进行排查处理；如果提示内存不足，请参见**磁盘分区**进行处理。

步骤4 确认已安装后，返回安全云脑的新增节点页面（即**步骤2**），单击页面右下角“确认”。

安装完成后，可以在节点管理页面查看已新增的节点。

图 1-15 已新增节点

----结束

1.4.7 步骤七：安装日志采集组件（Logstash）

本章节将介绍如何安装安全云脑日志采集组件（Logstash），配置日志采集进程。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-16 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 组件管理”，进入节点管理页面后，选择“组件管理”页签，进入组件管理页面。

图 1-17 进入组件管理页面

步骤5 在组件管理页面中，单击待查看组件右上角“编辑配置”，右侧将弹出该组件的配置管理页面。

步骤6 在配置管理界面的节点配置栏中，单击节点列表左上角“添加”，并在弹出的“添加节点”框中选择（可选）步骤一：购买ECS购买/准备的节点后，单击“确认”。

步骤7 在配置管理界面，单击页面右下角“保存并应用”。

等待一段时间，当组件配置状态为“应用完成”时，表示在当前ECS节点上采集器Logstash已经安装完成。

图 1-18 配置完成

----结束

1.4.8 （可选）步骤八：创建日志存储管道

本章节将介绍如何在安全云脑中创建日志存储位置（管道），用于日志存储、分析。

将非华为云日志转入安全云脑场景时，需要执行此步骤。将华为云日志转出至第三方系统或者产品场景，请跳过此步骤。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-19 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

图 1-20 进入安全分析页面

步骤5 新增数据空间。

1. 在数据空间列表左上角，单击“新增”，系统从右侧弹出新增数据空间界面。

图 1-21 新增数据空间

2. 在新增数据空间页面中，配置新建数据空间参数，参数说明如表1-6所示。

表 1-6 新增数据空间

参数名称	参数说明
数据空间	输入数据空间名称。命名规则如下： – 名称长度取值范围为5-63个字符。 – 可包含英文字母、数字和-。其中，-不能出现在开头和结尾，且不能连续出现。 – 名称须为全局（整个华为云上）唯一，不能与其他数据空间名称相同。

参数名称	参数说明
描述	可选参数，设置该数据空间的备注信息。

3. 单击“确定”。

步骤6 在左侧数据空间导航栏中，单击**步骤5**新增的数据空间名称右侧的，并在下拉选项中选择的“创建管道”，系统从右侧弹出创建管道页面。

图 1-22 创建管道

步骤7 在创建管道页面中，配置管道参数，参数说明如**表1-7**所示。

表 1-7 创建管道

参数名称	参数说明
数据空间	该管道所属的数据空间，系统默认生成。
管道名称	自定义管道的名称。命名规则如下： ● 名称长度取值范围为5-63个字符。 ● 可包含英文字母、数字和-。其中，-不能出现在开头和结尾，且不能连续出现。 ● 名称须为数据空间中的唯一，不能与数据空间中其他管道名称相同。
Shard数	该管道的Shard数量。取值范围为：1-64。 索引可以存储数据量超过1个节点硬件限制的数据。为满足这样的需求，Elasticsearch提供了一个能力，将一个索引拆分为多个，称为Shard。当您创建一个索引时，您可以根据实际情况指定Shard的数量。每个Shard托管在集群中的任意一个节点中，且每个Shard本身是一个独立的、全功能的“索引”。
生命周期	该管道内数据的生命周期。取值范围为：7-180。
描述	可选参数，设置该管道的备注信息。

步骤8 单击“确定”。

创建成功后，可单击数据空间名称，展开查看已创建的管道。

----结束

1.4.9 步骤九：配置连接器

本章节将介绍如何配置日志来源、接收目的的参数信息。请根据场景选择操作步骤：

- **将第三方日志接入安全云脑**
- **将安全云脑日志转出至第三方系统或产品**

将第三方日志接入安全云脑

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-23 进入目标工作空间管理页面

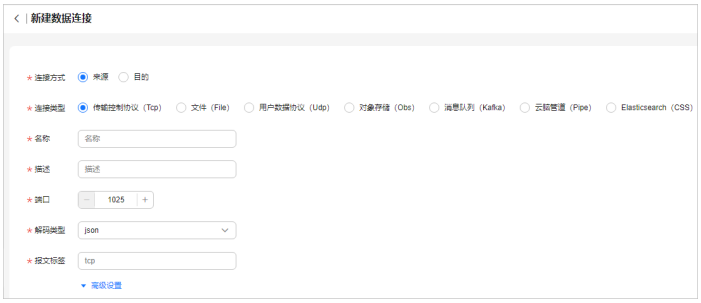
步骤4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 1-24 进入连接管理页面

步骤5 新增数据连接来源。

1. 在“连接管理”页面中，单击“新增”，默认进入选择数据连接来源页面。
2. 配置数据连接来源参数。

图 1-25 来源



此处以日志数据来源类型为UDP、TCP为例进行介绍，更多连接类型介绍请参见**连接器规则说明**。

- 连接类型 UDP

  表 1-8 日志来源

参数名称	配置说明
连接方式	选择“来源”。
连接类型	选择“用户数据协议（Udp）”。
名称	自定义设置数据连接来源名称。
描述	自定义设置数据来源描述信息。
端口	保持缺省值即可。
解码类型	保持缺省值即可。
高级设置	无需配置。

- 连接类型 TCP

  表 1-9 日志来源

参数名称	配置说明
连接方式	选择“来源”。
连接类型	选择“传输控制协议（Tcp）”。
名称	自定义设置数据连接来源名称。
描述	自定义设置数据来源描述信息。
端口	保持缺省值即可，未与其他来源使用的端口号重复即可。
解码类型	如果原始日志格式不是Json，则建议选择Plain。
报文标签	无需配置。

3. 设置完成后，单击页面右下角“确认”。

步骤6 新增数据连接目的。

1. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。
2. 配置数据连接目的参数。

图 1-26 目的

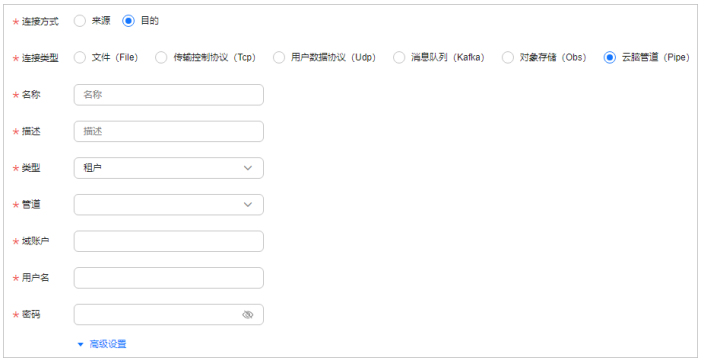


表 1-10 日志目的

参数名称	配置说明
连接方式	选择“目的”。
连接类型	选择“云脑管道（Pipe）”。
名称	自定义设置数据连接目的名称。
描述	自定义设置日志数据目的描述信息。
类型	自定义设置日志目的类型。
管道	选择**（可选）步骤八：创建日志存储管道**创建的管道。
域账户	输入当前登录Console的IAM账号的域账户信息。
用户名	输入当前登录Console的IAM账号的用户信息。
密码	输入当前登录Console的IAM账号的密码。
高级设置	无需配置。

3. 设置完成后，单击页面右下角“确认”。

----结束

将安全云脑日志转出至第三方系统或产品

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-27 进入目标工作空间管理页面

步骤4 在左侧导航栏选择“设置 > 采集管理”，默认进入连接管理页面。

图 1-28 进入连接管理页面

步骤5 新增数据连接来源。

1. 在“连接管理”页面中，单击“新增”，进入选择数据连接页面。
2. 配置数据连接来源参数。

图 1-29 数据来源

表 1-11 日志来源

参数名称	配置说明
连接方式	选择“来源”。
连接类型	选择“云脑管道（Pipe）”。
名称	自定义设置数据连接目的名称。
描述	自定义设置日志数据目的描述信息。
类型	自定义设置日志目的类型。
管道	选择（可选）步骤八：创建日志存储管道创建的管道。
域账户	输入当前登录Console的IAM账号的域账户信息。

参数名称	配置说明
用户名	输入当前登录Console的IAM账号的用户信息。
密码	输入当前登录Console的IAM账号的密码。
高级设置	无需配置。

3. 设置完成后，单击页面右下角“确认”。

步骤6 新增数据连接目的。

在“连接管理”页面中，单击“新增”，并配置数据连接目的参数。

请根据实际情况进行填写，更多连接类型介绍请参见**连接器规则说明**。

----结束

1.4.10（可选）步骤十：配置日志解析器

本章节将介绍如何配置日志解析器，以便将日志数据进行格式转换，实现无码化，将源日志转换成用户需要的数据类型。

安全云脑提供模板日志解析器（规则），可以直接使用模板进行配置。当模板日志解析器（规则）无法满足日志转换的情况下，可自定义新增日志解析器（规则）。

- **方式一：使用模板进行创建**
- **方式二：自定义新增解析器**

方式一：使用模板进行创建

此处以“安恒WAF日志解析”为例进行介绍。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-30 进入目标工作空间管理页面

步骤4 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。

图 1-31 进入解析器管理页面

步骤5 在解析器管理页面中，选择“模板列表”页签。

步骤6 在模板列表页面中，单击“安恒WAF日志解析”所在行“操作”列的“由模板创建”。

步骤7 在新增解析器页面中，进行参数配置。

表 1-12 新增解析器

参数名称		参数说明
基本信息	名称	解析器名称，系统已根据模板自动生成，可进行修改。
	描述	解析器描述信息，系统已根据模板自动生成，可进行修改。
规则列表		解析器解析规则，系统已根据模板自动生成，可进行修改。 如需添加规则，可以单击“添加”，选择规则类型，并根据选择的规则配置对应的参数信息。 • 解析规则：选择解析器的解析规则，详细参数说明请参见**解析器规则说明**。 • 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。

步骤8 设置完成后，单击页面右下角“确定”。

----结束

方式二：自定义新增解析器

模板日志解析器（规则）无法满足日志转换的情况下，可自定义新增日志解析器（规则）。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-32 进入目标工作空间管理页面

步骤4 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。

图 1-33 进入解析器管理页面

步骤5 在解析器列表管理页面中，单击“新增”，进入新增解析器页面。

步骤6 在新增解析器页面中，进行参数配置。

表 1-13 新增解析器

参数名称		参数说明
基本信息	名称	设置解析器名称。
	描述	输入解析器描述信息。
规则列表		设置解析器解析规则。操作步骤如下： 1. 单击“添加”，并选择规则类型。 – 解析规则：选择解析器的解析规则，详细参数说明请参见**解析器规则说明**。 – 条件控制：选择解析器的条件控制原则，支持选择“if条件”、“else条件”、“else if条件”。 2. 根据选择的规则配置对应的参数信息。

步骤7 设置完成后，单击页面右下角“确定”。

----结束

1.4.11 步骤十一：配置日志采集通道

本章节将介绍如何配置日志采集通道，完成各功能组件连接，实现安全云脑和日志采集器正常工作。

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 > 安全云脑 SecMaster”，进入安全云脑管理页面。

步骤3 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 1-34 进入目标工作空间管理页面

步骤4 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“采集通道管理”页签，进入采集通道管理页面。

图 1-35 进入采集通道管理页面

步骤5 新增日志采集通道分组。

1. 在采集通道管理页面中，单击“分组列表”右侧的⊕。
2. 自定义输入分组名称，并单击✔，完成新增。

步骤6 新建日志采集通道。

1. 在采集通道管理页面的分组列表右侧，单击“新增”，进入新增采集通道页面。
2. 在“基础配置”页面中，配置基础信息。

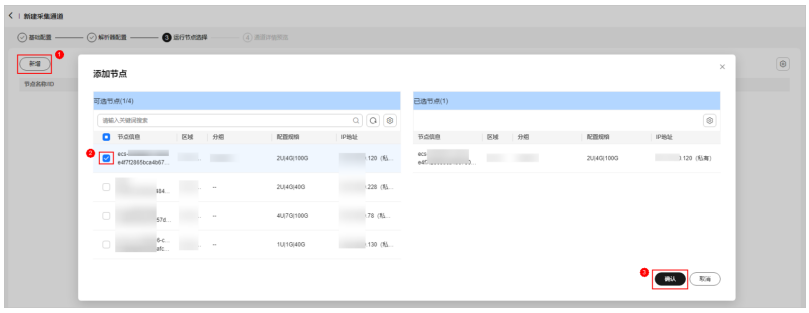
表 1-14 基础配置参数说明

参数名称		参数说明
基础信息	名称	自定义采集通道名称。
	通道分组	选择**步骤5**创建的分组。
	（可选）描述	自定义填写采集通道描述信息。
来源配置	源名称	选择**步骤九：配置连接器**新增的日志来源名称。 选择后系统将自动生成已选择来源的相关信息。
目的配置	目的名称	选择**步骤九：配置连接器**新增的日志目的名称。 选择后系统将自动生成已选择目的相关信息。

3. 单击页面右下角“下一步”，进入“解析器配置”页面。
4. 在“解析器配置”页面中，选择（可选）步骤十：配置日志解析器配置的解析器，并单击页面右下角“下一步”，进入“运行节点选择”页面。

   如果未配置解析器，可以选择“快速接入”，将原始日志直接接入采集通道列表中。
5. 在“运行节点选择”页面中，单击“新增”，并在弹出的添加节点框中选择（可选）步骤一：购买ECS购买的ECS节点后，单击“确认”。

图 1-36 选择运行节点



步骤7 单击页面右下角“下一步”，进入“通道详情预览”页面。

步骤8 在“通道详情预览”页面确认配置无误后，单击“保存并执行”。

在采集通道管理页面，当采集通道的健康状态列显示为“正常”，表示当前采集通道下发已经全部成功。

图 1-37 采集通道配置完成

----结束

1.4.12 步骤十二：测试验证

本章节介绍将非华为云日志接入安全云脑后，如何在安全云脑中测试验证日志是否接入成功。

表 1-15 测试验证场景说明

场景	验证方法
华为云日志接入安全云脑	请在“安全分析”中查看是否存在已接入云服务日志。
安全云脑日志转出至第三方系统/产品	请在第三方系统/产品侧确认日志是否接收成功。
第三方（非华为云）日志接入安全云脑	参考本章节进行验证。

操作步骤

步骤1 手动触发生成日志。

1. 远程登录（可选）步骤一：购买ECS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，选择目标ECS并单击操作”列的“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. 执行以下命令，手动触发生成日志。

   echo ”asdfsadfsadf” > /dev/udp/0.0.0.0/1025

步骤2 在安全云脑控制台的采集通道中查看数据。

1. 登录管理控制台。
2. 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。
3. 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 1-38 进入目标工作空间管理页面

4. 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“采集通道管理”页签，进入采集通道管理页面。

图 1-39 进入采集通道管理页面

5. 在采集通道页面中，单击表格右上角的设置按钮，勾选“接收数量”和“发送数量”。

图 1-40 配置表格参数

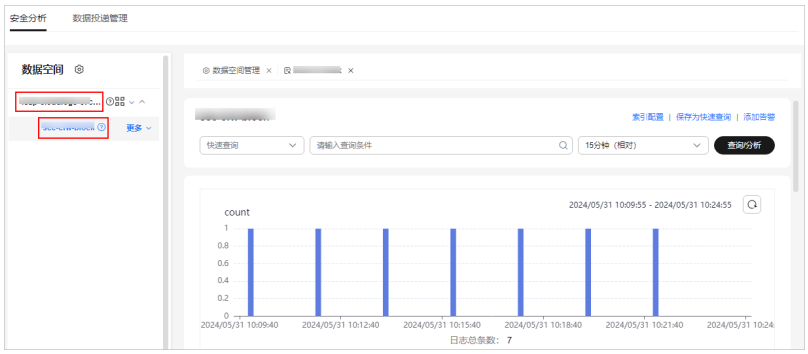
6. 在表格中，查看对应采集通道监控，有接收数量和发送数量，说明日志接入成功。

图 1-41 查看日志接入情况

步骤3 在安全云脑控制台的安全分析日志管道中查看数据。

步骤4 在左侧数据空间导航栏中，单击数据空间名称，展开数据管道列后，再单击**操作步骤**创建的管道名称，右侧将显示管道数据的检索页面。

图 1-42 管道数据页面



步骤5 日志管道有数据，说明日志接入成功。

----结束

2 凭证泄露响应方案

事件类型：凭证泄露

凭证泄露指的是个人或组织在使用各种服务（如云服务、社交媒体、电子邮件等）时，其身份验证信息（如用户名、密码、API密钥、访问令牌等）被未经授权的第三方获取或泄露。这种情况可能通过多种方式发生，包括但不限于网络钓鱼、恶意软件、社交工程、系统漏洞等。一旦凭证被泄露，攻击者可能会利用这些信息来访问敏感数据、进行非法交易或破坏系统，对业务造成严重影响。

事件响应方案

针对以上问题，华为云推出了安全云脑（SecMaster）服务。它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。

事件响应流程

步骤1 识别身份凭证是否受损或泄露。

1. 如果您收到如下提示信息，您需要排查并识别您的身份凭证是否受损或泄露：
   - 来自华为云服务（例如，华为云证书管理服务CCM、安全云脑SecMaster、云审计服务CTS等）、外部监控系统的告警或指标；
   - 来自承包商或第三方服务提供商的提示信息；
   - 通过内部或外部安全研究人员的排查信息；
   - 内部系统信息；
   - 匿名举报信息；
   - 其他途径的信息。例如，攻击者通过被泄露的凭证，窃取您的数据，并修改您面向公众的资源。
2. 确认已针对该事件提交工单或案例。如果没有，请手动提交。
3. 确定并记录问题对最终用户的影响。

   无论此类场景是否造成直接的用户影响，都请将调查结果记录在与此事件相关的工单或案例中。

4. 对于自动创建的工单或案例，确定哪些告警或指标是存在问题的。

   例如触发告警或指标可能是CTS服务指标指示您的IAM配置某些方面不合规，或者IAM服务警报表明可能存在凭证泄露。也可能是一个计费警报，当您的计费成本已超过预定阈值，触发告警或通知。

5. 确定已泄露的凭证集。
   - 如果已创建工单或案例，请检查该工单或案例中是否记录了用户/角色名称、用户或角色ID或访问密钥ID。
   - 如果告警来自安全云脑基线检查，您可以在控制台查看基线检查结果，找到受影响凭证的访问密钥ID。具体操作请参见**查看基线检查结果**。
   - 如果告警来自CTS服务，您可以在控制台事件列表，查看结果。“资源名称”为访问密钥，Credential字段则包含“access_key_id”、“account_id”、“user_name”和其他信息。
6. 确定凭证可能被破坏或泄露的时间。在该时间后进行的任何API操作应被视为恶意操作，在该时间后创建的任何资源应被视为被泄露。
7. 如果您的应用程序发生服务中断，需确定造成中断的可能事件。如果中断事件与凭证泄漏无关，需检查部署管道以确定在事件发生之前是否进行了任何更改。您可以通过CTS服务，协助查看所有账户活动的日志。
8. 事件沟通：
   - 根据组织的事件响应计划确定利益相关方的角色。
   - 通知相关干系人，包括法务人员、技术团队和开发人员，并确保他们被添加到工单和作战室中，以进行持续更新。
9. 外部沟通：
   - 确保您的法律顾问了解情况，并将其纳入内部利益相关者的状态更新，特别是外部沟通的状态更新。
   - 将负责公共或外部沟通的同事添加到工单中，以便他们可以定期接收到有关事件的状态更新，并履行其沟通职责。
   - 如果您所在辖区有法规要求报告此类事件，请确保贵组织中负责通知当地或联邦执法机构的人员也收到有关该事件的通知/被添加到工单中。请咨询您的法律顾问、执法部门，以获取有关收集和保存证据和监管局的指导。即使法规没有要求，向开放数据库、政府机构或非政府组织报告，您的报告也可能有助于分析类似的活动或帮助其他人。

步骤2 控制事件。

您可以通过禁用受损凭证或撤销与这些凭证相关的权限，从而阻止使用受损凭证调用API。

1. 禁用**步骤1**识别到的受损凭证。
   a. 如果是永久IAM用户凭证，请在IAM控制台，删除用户凭证，具体操作请参见**删除IAM用户**。
   b. 如果是通过IAM获取的临时安全凭证，则会关联到IAM角色。您可以通过如下方法禁用这些功能：
      i. 撤销所有当前角色会话。如果攻击者获取新的临时安全凭证，并继续攻击，跳转到**步骤2.1.b.ii**。
      ii. 删除添加到该角色的所有IAM策略，修改已有策略以阻止所有访问，或者修改角色的策略以防止攻击者承担该角色。

      由于凭证在颁发后的指定时间段内仍然有效，因此请务必注意，修改信任策略后，凭证在有效期内将被允许继续使用。**步骤2.1.b.i**和**步骤**

2.1.b.ii将阻止所有用户使用通过承担角色获得的凭证，包括任何合法用户或应用程序。

2. 您可以在30分钟左右的时间内通过CTS服务控制台查看持续使用的凭证，无论是访问密钥、IAM用户还是角色，确认受损凭证已被禁用。

步骤3 消除事件。

您需要排查凭证在受损后执行了哪些API操作，创建、删除或修改了哪些资源，并采取相应措施，消除影响。

1. 使用您的首选监控工具，访问CTS服务，并采集受损凭证执行的所有API操作，日志采集时间为受损时间到当前时间。
   - 如果您使用的是第三方工具（如Splunk或其他工具）采集云审计服务日志，请按照从该工具获取日志信息的正常过程进行操作。
   - 如果您不使用第三方工具，而是将日志发送到华为云对象存储服务（OBS），您可以使用华为云日志服务LTS采集、查询和存储日志。
2. 在日志服务LTS控制台，查询凭证在受损或泄露后的日期/时间采取的所有API操作。
3. 从结果列表中，确定哪些API调用：
   - 访问敏感数据，例如，OBS Object。
   - 创建新的华为云资源，例如数据库、云服务器等。
   - 创建资源的服务，包括ECS弹性伸缩组等。
   - 创建或修改权限，同时，还应排查包括（但不限于）以下API方法：CreateUser、CreateRole、AssumeRole*、Get*Token、Attach*Policy、*Image*、*Provider、Tag*、Create*、Delete*、Update*等。
   - 删除现有华为云资源。
   - 修改现有华为云资源。
4. 根据上一步的结果，确定是否有任何应用程序可能受到影响。如果有，获取受影响的每个资源的ID或标记信息，并通知资源的所有者。
5. 基于以上结果，如果创建了额外的凭证获取资源（IAM用户、角色等），根据步骤2.1，禁用和删除这些资源的所有凭证。
6. 重复步骤3.1到步骤3.5，排查是否仍存在额外发现的凭证，直到全部处置完成。

步骤4 从事故中恢复。

1. 恢复被修改的资源：
   - 如果资源可以被销毁和替换，则添加新的资源。
   - 如果资源无法被替换，请执行以下任一操作：
     - 从备份还原资源。
     - 准备新资源并将其配置到应用程序的基础架构中，同时隔离受损资源并将其从应用程序的基础架构中移除。
     - 销毁受损资源，或继续将其隔离以备取证。
   - 恢复删除的资源：
     i. 通过排查确定资源所属的应用程序。如果资源标签未在CTS服务条目中列出，且华为云配置支持该资源，则检查华为云的配置。

ii. 如果删除的资源可以从备份中恢复，请直接恢复；如果删除的资源无法从备份中恢复，请查阅CMDB以获取资源的配置，重新创建资源并将其配置到应用程序的基础架构中。

步骤5 事故后活动。

- 针对某些受损资源进行调查取证，分析攻击者对受损资源使用了哪些攻击手段，并确定是否需要针对相关资源或应用程序采取额外的风险缓解措施。
  a. 对于任何已隔离以供进一步分析的受损资源，对这些资源执行取证活动，并将调查结果纳入事后报告。
  b. 确保正确更新CMDB以反映受影响的所有资源和应用程序的当前状态。
- 审查事件本身和对它的响应，确定哪些措施起作用，哪些措施不起作用，根据这些信息更新改进流程，并记录调查结果。

----结束

