安全云脑

# 最佳实践

文档版本 07

发布日期 2024-12-09

华为云计算技术有限公司

**版权所有 © 华为云计算技术有限公司 2024。 保留一切权利。**

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 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



 版权所有 © 华为云计算技术有限公司 

 版权所有 © 华为云计算技术有限公司 

# 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。


版权所有 © 华为云计算技术有限公司

- **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。

## 日志接入或转出支持的传输协议类型以及日志格式

**表 1-2** 日志接入或转出支持的传输协议类型以及日志格式

| 场景 | 支持的传输协议类型 | 支持的日志格式 |
| --- | --- | --- |
| 日志接入安全云脑 | 传输控制协议 TCP | json、syslog、plain |
| | 用户数据协议 UDP | json、syslog、plain |
| | 对象存储 OBS | json、plain |
| | 消息队列 Kafka | json、plain |
| | 云脑管道 Pipe | json、plain |
| | ElasticSearch CSS | json、plain |
| 日志从安全云脑转出 | 传输控制协议 TCP | json |
| | 用户数据协议 UDP | json |


版权所有 © 华为云计算技术有限公司

| 场景 | 支持的传输协议类型 | 支持的日志格式 |
| --- | --- | --- |
| | 消息队列 Kafka | json |
| | 对象存储 OBS | json |
| | 云脑管道 Pipe | json |

# 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 1-3** 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 |
| 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。

 版权所有 © 华为云计算技术有限公司 

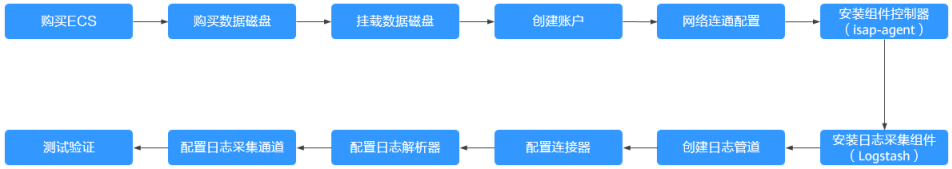
### 接入日志数量

**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。**<br>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。<br>请根据场景选择操作步骤：<br>• 将第三方日志接入安全云脑<br>• 将安全云脑日志转出至第三方系统或产品 |


版权所有 © 华为云计算技术有限公司

| 操作步骤 | 操作说明 |
| --- | --- |
| （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

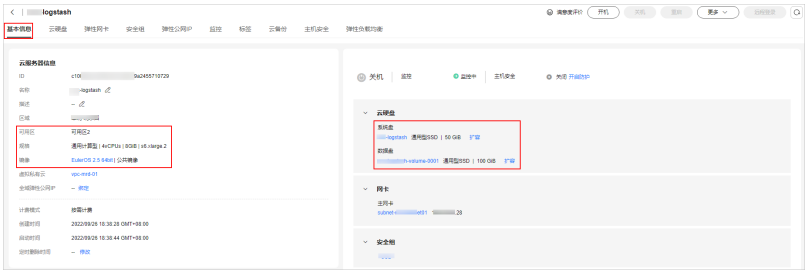
已获取IAM管理员账号信息。

### 购买 ECS

**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”。


版权所有 © 华为云计算技术有限公司

**步骤3** 在购买页面配置ECS购买参数信息。

**表 1-4** 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”。<br>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”。<br>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。<br>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。<br>选择镜像后，是否“开启安全防护”根据需要自定义配置。 |
| 存储与备份 | 系统盘 | 最低要求**系统磁盘50 GB**。<br>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**。<br>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。<br>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。<br>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”。

 版权所有 © 华为云计算技术有限公司 

**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。

### 购买数据磁盘

**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 1-5** 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。 |


版权所有 © 华为云计算技术有限公司

| 参数名称 | 配置说明 |
| --- | --- |
| 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。<br>• 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。<br>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。

### 挂载数据磁盘

**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”。


版权所有 © 华为云计算技术有限公司

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。

### 创建非管理员 IAM 账户

**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”。


版权所有 © 华为云计算技术有限公司

**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 1-6** 用户基本信息

| 参数名称 | | 配置说明 |
| --- | --- | --- |
| 用户信息 | | 自定义配置。<br>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。 |


版权所有 © 华为云计算技术有限公司

| 参数名称 | | 配置说明 |
| --- | --- | --- |
| | 密码 | 勾选。<br>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。

### 网络连通配置

**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



版权所有 © 华为云计算技术有限公司

**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



版权所有 © 华为云计算技术有限公司

**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。

### 安装组件控制器

**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

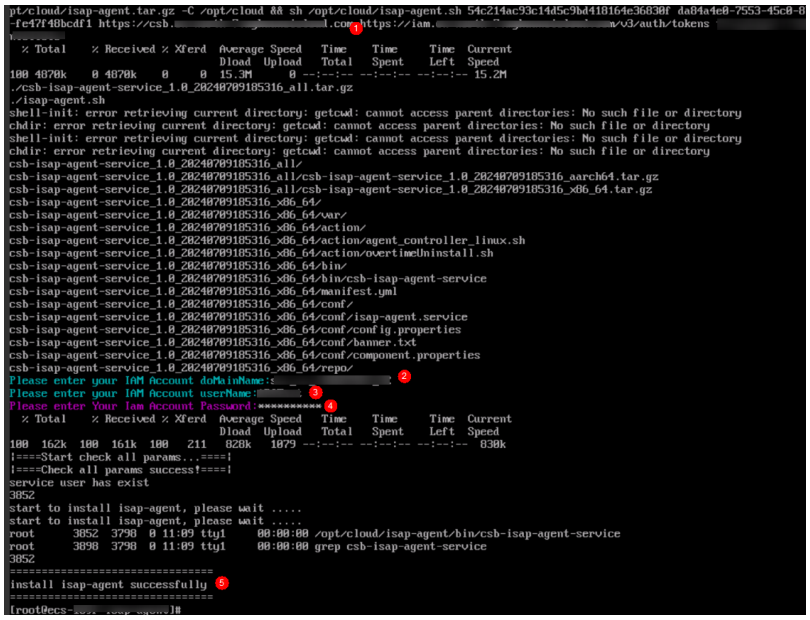

**步骤3** 安装组件控制器。

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。

 版权所有 © 华为云计算技术有限公司 

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。

### 安装日志采集组件

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角单击 ☰，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面。

 版权所有 © 华为云计算技术有限公司 

**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。

 版权所有 © 华为云计算技术有限公司 

**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。**

## 创建日志存储管道

**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1-7所示。


版权所有 © 华为云计算技术有限公司

**表 1-7** 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：<br>– 名称长度取值范围为5-63个字符。<br>– 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。<br>– 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。 |
| 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1-8**所示。

**表 1-8** 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：<br>● 名称长度取值范围为5-63个字符。<br>● 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。<br>● 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。<br>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。 |


版权所有 © 华为云计算技术有限公司

**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。

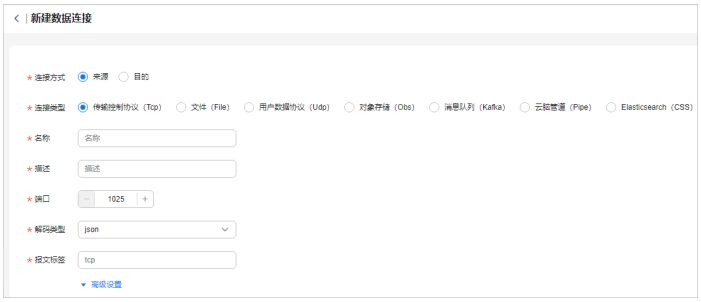
**图 1-24** 进入连接管理页面

**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。

 版权所有 © 华为云计算技术有限公司 

**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 1-9** 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“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 1-10** 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。 |

 版权所有 © 华为云计算技术有限公司 

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

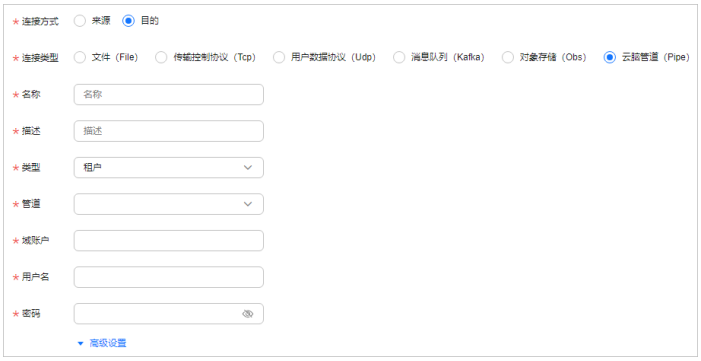



**表 1-11** 日志目的

| 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。

 版权所有 © 华为云计算技术有限公司 

**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 1-12** 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。 |

 版权所有 © 华为云计算技术有限公司 

| 参数名称 | 配置说明 |
| --- | --- |
| 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”。

**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。

 版权所有 © 华为云计算技术有限公司 

**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 1-13** 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。<br>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。<br>• 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**。<br>• 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。

 版权所有 © 华为云计算技术有限公司 

**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 1-14** 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：<br>1. 单击“添加”，并选择规则类型。<br>– 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**。<br>– 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”。<br>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。

### 配置日志采集通道

**步骤1** 登录管理控制台。

 版权所有 © 华为云计算技术有限公司 

**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 1-15** 基础配置参数说明

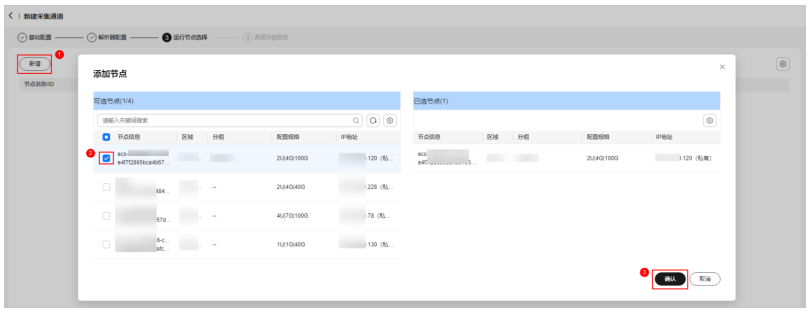
| 参数名称 | | 参数说明 |
| --- | --- | --- |
| 基础信息 | 名称 | 自定义采集通道名称。 |
| | 通道分组 | 选择**步骤5**创建的分组。 |
| | （可选）描述 | 自定义填写采集通道描述信息。 |
| 来源配置 | 源名称 | 选择**步骤九：配置连接器**新增的日志来源名称。<br>选择后系统将自动生成已选择来源的相关信息。 |
| 目的配置 | 目的名称 | 选择**步骤九：配置连接器**新增的日志目的名称。<br>选择后系统将自动生成已选择目的相关信息。 |

 版权所有 © 华为云计算技术有限公司 

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 1-16** 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。 |


版权所有 © 华为云计算技术有限公司

## 测试验证

**步骤1** 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。

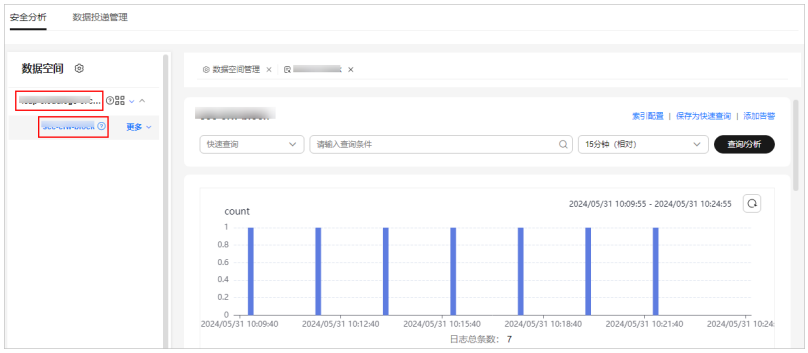
**图 1-41** 查看日志接入情况

**步骤2** 在安全云脑控制台的安全分析日志管道中查看数据。

**步骤3** 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**创建日志存储管道**创建的管道名称，右侧将显示管道数据的检索页面。


版权所有 © 华为云计算技术有限公司

**图 1-42** 管道数据页面




**步骤4** 日志管道有数据，说明日志接入成功。

**----结束**

 版权所有 © 华为云计算技术有限公司 

# 2 安全云脑护网/重保最佳实践

## 2.1 场景说明

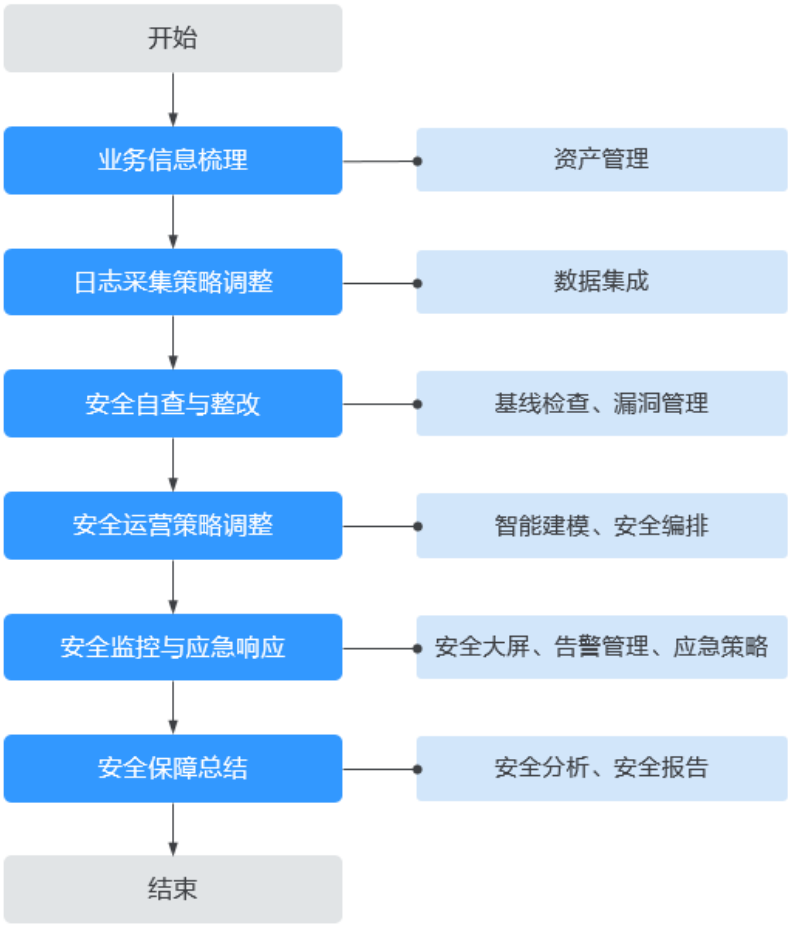
安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力。

安全云脑支持在重大保障及防护演练前，全面地进行资产脆弱性盘点；在攻防演练期间，高强度7*24的安全保障，侧重于防攻击，保障业务可用性不因安全攻击受影响，侧重于防入侵，保障不因入侵失分被问责。能够更智能、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。

本场景将介绍在护网、重保场景中安全云脑的使用，具体流程如下图所示：

 版权所有 © 华为云计算技术有限公司 

**图 2-1** 使用流程




# 2.2 步骤一：业务信息梳理

护网/重保前，需要对整体护网信息进行盘点，全面梳理可能针对云上业务系统的攻击路径，构建安全防护架构。

安全云脑纳管了网站、弹性云服务器、数据库、IP、VPC等资产，并关联对应的安全服务，护网、重保期间立志于从网络层、应用层、主机层、数据层等多方面构建整体网络防护架构，全面保障用户业务系统的安全稳定。

**说明**

如果资产信息未在安全云脑中显示，则可以通过**设置资产订阅**同步资产信息；如果需要导入云下资产，请参考**导入资产**进行处理。

## 梳理网站资产

Web业务是企业最为重要和广泛使用的业务之一，也是最容易受到攻击的业务之一，因此，护网/重保前需要先进行Web资产的梳理。

针对网站域名，支持通过Web应用防火墙（Web Application Firewall，WAF）服务对网站业务流量进行全方位检测和防护，智能识别恶意请求特征和防御未知威胁，避免源站被黑客恶意攻击和入侵，防止核心资产遭窃取，为网站业务提供安全保障。


版权所有 © 华为云计算技术有限公司

安全云脑的资产管理功能会自动将WAF中已录入的域名同步过来，可以在安全云脑中进行统一管理。**护网/重保期间需要保证所有网站均已接入WAF并开启防护，以提高网站安全性**。

查看方法如下：

1. 登录安全云脑控制台，并进入目标工作空间管理页面。
2. 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面后，选择“网站”页签，查看网站防护状态。

**图 2-2** 查看网站防护状态

网站防护状态说明如下表所示：

**表 2-1** 网站防护状态说明

| 网站防护状态 | 说明 |
| --- | --- |
| 未防护 | 网站域名未在WAF中开启防护。<br>为防止网站被各种恶意流量攻击，建议您将网站接入WAF，才能对HTTP(S)请求进行检测，保障业务核心数据安全，详细操作请参见网站接入WAF。<br>开启防护后，建议优化如下网站防护配置，护网期间请采用严格的安全防护模式：<br>**Web基础防护（拦截模式），CC攻击防护（阻断模式），精准访问防护（阻断模式），IP黑白名单设置（拦截模式），地理位置访问控制（拦截模式）**<br>防护配置详细操作请参见网站防护配置建议。 |
| 已防护 | 已购买WAF，且已在WAF中接入网站域名并开启防护。 |
| -- | 对应的安全防护产品(WAF)在该region不支持使用。 |

## 梳理主机资产

安全云脑的资产管理功能会自动完成弹性云服务器（Elastic Cloud Server，ECS）资产的梳理，包括资产名称、镜像、IP等信息。

针对ECS主机资产，支持通过企业主机安全（Host Security Service，HSS）服务，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

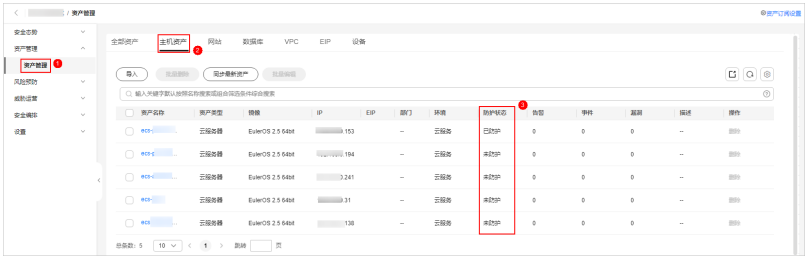
**护网/重保期间需要保证所有ECS主机均接入HSS，尤其是绑定了EIP、以及Web业务所在ECS，以提高主机安全风险防御能力**。

 版权所有 © 华为云计算技术有限公司 

查看方法如下：

1. 登录安全云脑控制台，并进入目标工作空间管理页面。
2. 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面后，选择“主机资产”页签，查看主机防护状态。

**图 2-3** 查看主机资产防护状态



主机资产防护状态说明如下表所示：

**表 2-2** 主机资产防护状态说明

| 主机防护状态 | 说明 |
| --- | --- |
| 未防护 | ECS主机未开启防护，被威胁入侵的风险较高，建议您尽快为主机开启防护。开启防护步骤如下：<br>1. **购买防护配额**。<br>2. **安装Agent**。<br>3. **开启主机防护**。<br>开启防护后，建议优化主机防护配置，开启恶意软件云查，并通过精细化策略配置，提升主机防护能力，详细操作请参见**优化主机安全防护配置**。 |
| 已防护 | 主机已开启防护。企业主机安全会持续优化迭代Agent版本，请及时参考**升级Agent**将Agent升级为最新版。 |
| -- | 对应的安全防护产品(HSS)在该region不支持使用。 |

**说明**

目前，安全云脑暂未接入容器资产信息，如果您的资产为容器资产，请在HSS服务控制台上进行容器资产安全防护梳理，详细操作请参见**查看容器节点防护状态**。

## 梳理数据库资产

梳理数据库资产的目的主要是在安全运营过程中，相关告警会自动关联数据库资产。

安全云脑的资产管理功能会自动完成云数据库（Relational Database Service，RDS）资产的梳理。针对数据库资产，支持通过数据库安全服务（Database Security Service，DBSS）服务来保障云上数据库的安全。

**护网/重保期间需要保证所有RDS资产均已开启数据库安全审计，以保障云上数据库的安全。**


版权所有 © 华为云计算技术有限公司

查看方法如下：

1. 登录安全云脑控制台，并进入目标工作空间管理页面。
2. 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面后，选择“数据库”页签，查看数据库防护状态。

**图 2-4** 查看数据库防护状态

数据库防护状态说明如下表所示：

**表 2-3** 数据库防护状态说明

| 数据库防护状态 | 说明 |
| --- | --- |
| 未防护 | RDS资产未在DBSS中配置并开启防护。<br>为防止数据库被攻击，建议您开通并使用数据库安全审计，详细操作请参见**审计RDS关系型数据库（安装Agent）**或**审计RDS关系型数据库（免安装Agent）**。 |
| 已防护 | RDS资产已在DBSS中配置并开启防护。 |
| -- | 对应的安全防护产品(DBSS)在该region不支持使用。 |

**说明**

RDS通过DBSS纳管审计防护，还需要在DBSS中进行告警设置，将DBSS日志数据同步到安全云脑，从而监控到DBSS告警数据，详细操作请参见**设置告警通知**，设置时，请将所有DBSS实例所有告警风险等级的告警均开启告警通知。

## 梳理虚拟私有云资产

虚拟私有云（Virtual Private Cloud，VPC）是您在云上的私有网络，为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。

安全云脑的资产管理功能会自动完成云VPC资产的梳理。针对VPC资产，支持通过云防火墙（Cloud Firewall，CFW）服务来提供云上互联网边界和VPC边界的防护，VPC边界防火墙支持两个VPC之间通信流量的访问控制，实现内部业务互访活动的可视化与安全防护。

**护网/重保期间需要保证所有VPC资产均已使用CFW防护，以保障云上互联网边界和VPC边界的安全。**

查看方法如下：

1. 登录安全云脑控制台，并进入目标工作空间管理页面。
2. 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面后，选择“VPC”页签，查看VPC防护状态。


版权所有 © 华为云计算技术有限公司

**图 2-5** 查看 VPC 防护状态

VPC防护状态说明如下表所示：

**表 2-4** VPC 防护状态说明

| VPC防护状态 | 说明 |
| --- | --- |
| 未防护 | VPC资产未在CFW中配置并开启防护。<br>为有效检测和统计VPC间的通信流量数据，建议您使用并配置VPC边界防火墙，详细操作请参见**配置VPC边界云防火墙**。 |
| 已防护 | VPC资产已在CFW中配置并开启防护。 |
| -- | 对应的安全防护产品(CFW)在该region不支持使用。 |

## 梳理弹性公网 IP 资产

弹性公网IP（Elastic IP，EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。为资源配置弹性公网IP后，可以直接访问Internet，如果资源只配置了私网IP，就无法直接访问Internet。弹性公网IP可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。

安全云脑的资产管理功能会自动完成云EIP资产的梳理。针对EIP资产，支持通过Anti-DDoS通过对互联网访问公网IP的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS为用户生成监控报表，清晰展示网络流量的安全状况。

**护网/重保期间需要保证所有EIP资产均已使用Anti-DDoS进行流量清洗，以保障云上公网流量的基础安全。**

查看方法如下：

1. 登录安全云脑控制台，并进入目标工作空间管理页面。
2. 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面后，选择“EIP”页签，查看EIP防护状态。

**图 2-6** 查看 EIP 防护状态


版权所有 © 华为云计算技术有限公司

EIP防护状态说明如下表所示：

**表 2-5** EIP 防护状态说明

| EIP防护状态 | 说明 |
| --- | --- |
| 未防护 | EIP资产未在Anti-DDoS中配置并开启防护。<br>为有效对互联网访问公网IP进行检测，清洗攻击流量，建议您使用并配置Anti-DDoS，购买了公网IP后，系统自动开启Anti-DDoS默认防护。 |
| 已防护 | EIP资产已在Anti-DDoS中配置并开启防护。 |
| -- | 对应的安全防护产品(Anti-DDoS)在该region不支持使用。 |

**说明**

除了使用Anti-DDoS进行流量清洗，还推荐使用CFW对公网IP进行防护，保证所有业务流量均经过云防火墙，通过CFW日志数据即可对整体业务进行监控或设置其他运营策略进行有效防护，详细操作请参见**开启弹性公网IP防护**。

# 2.3 步骤二：日志采集策略调整

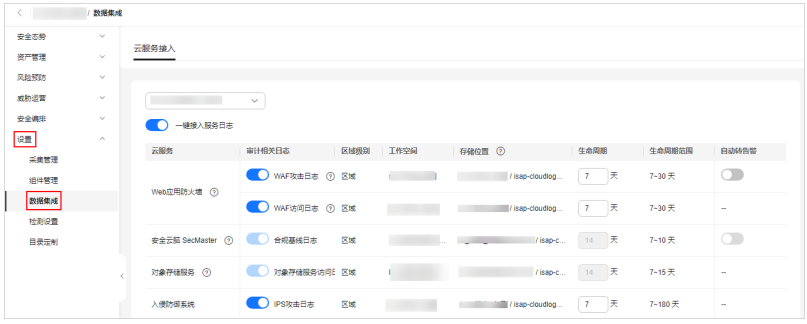
日志作为安全运营提供重要数据支撑，**护网/重保期间推荐使用一键接入功能接入全部日志**，并调整自动转告警功能，结合模型和安全服务攻击日志，通过“告警管理”统一进行跟踪监控。

## 日志采集策略调整

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“设置 > 数据集成”，进入云服务日志接入页面。

**图 2-7** 数据集成页面



**步骤3** 护网期间，推荐接入当前region所有云产品日志，请直接单击“一键接入服务日志”前的 按钮，一键接入当前region所有云服务日志。

**步骤4** 在“主机漏洞扫描结果”、“DDoS攻击日志”、“数据库安全服务告警”的“自动转告警”列，单击 ，开启自动转告警功能。


版权所有 © 华为云计算技术有限公司

**步骤5** 单击“保存”，并在弹出的配置保存框中，单击“确定”。

**----结束**

# 2.4 步骤三：安全自查与整改

## 2.4.1 基线检查

安全云脑支持根据基线检查计划检查您的服务基线配置是否存在风险，提供了“安全上云合规检查1.0”、“等保2.0三级要求”、“护网检查”、“华为云安全配置基线”几大风险类别遵从包。

**护网/重保期间推荐使用“安全上云合规检查1.0”和“护网检查”两个规范。**

检查之后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。

所有检查项检查完成之后进入详情页面，不合格检查项按照加固建议进行修复，特别是**靶标，通过资产搜索，清零不合格检查项**。同时，配置检查计划，每天定时扫描刷新结果。

### 设置基线检查计划

检查计划是规范和时间组合形成的，也就是设置的定时扫描任务。通过配置检查计划自动的定期的对资产进行检查，保证检查结果的即时性。

护网/重保期间推荐对“护网检查规范”配置对应检查计划，配置策略周期为每天检查一次。

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“风险预防 > 基线检查”，进入基线检查页面后，选择“安全遵从包”页签，并在安全遵从包页面中，选择“检查计划”页签，进入检查计划管理页面。

**图 2-8** 进入检查计划页面

**步骤3** 在检查计划页面中，单击“创建计划”，系统右侧弹出新建检查计划页面。

**步骤4** 在新建检查计划页面中，配置检查计划。

**表 2-6** 新建检查计划

| 参数名称 | | 参数说明 |
| --- | --- | --- |
| 基本信息 | 计划名称 | 自定义检查计划的名称。 |

 版权所有 © 华为云计算技术有限公司 

| 参数名称 | | 参数说明 |
| --- | --- | --- |
| | 检查时间 | 建议设置为每隔1天00:00~06:00进行检查。 |
| 选择遵从包 | | 此处请选择“护网检查”。 |

**步骤5** 单击“确定”。

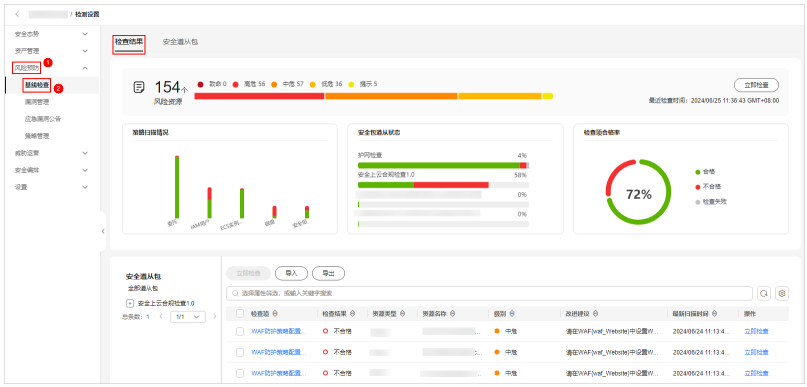
**----结束**

## 立即执行全量基线检查

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“风险预防 > 基线检查”，默认进入检查结果管理页面。

**图 2-9** 进入基线检查结果页面



**步骤3** 在检查结果页面中，单击“立即检查”，并在弹出的确认框中，单击“确认”。

等待一段时间之后刷新页面，如果“最近检查时间”刷新为手动单击检查的时间，则页面显示结果为最新扫描结果。

**----结束**

## 清理加固基线检查风险项

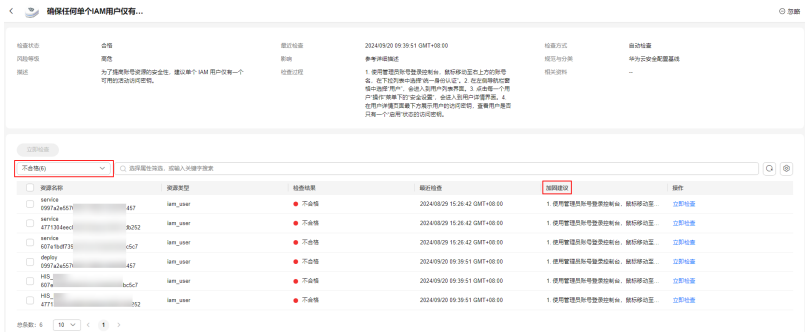
基线检查分为手动检查项和自动检查项。针对自动检查项，执行基线检查后，需要对不合格检查项按照加固建议进行修复；针对手动检查项，需要用户自主排查对应检查项，针对不合格检查项进行手动整改，结果反馈到安全云脑中。

- **自动检查项**
  - 通过安全遵从包进行清理加固
    i. 在检查结果页面中，查看子检查项的风险状态。如果检查状态显示为不合格，则单击目标子检查项名称，进入检查项目详情页面。
    ii. 筛选“不合格”的检查项，并根据“加固建议”修复风险点。

    如果加固建议中提供了跳转链接，可以直接单击链接，跳转至对应页面进行处理。

 版权所有 © 华为云计算技术有限公司 

**图 2-10** 检查项加固建议



iii. 修改之后单击操作列“立即检查”对修改结果进行验证。

**部分关键风险项清理加固建议如下表所示**:

**表 2-7** 加固建议

| 检查项名 | 加固建议 |
| --- | --- |
| 安全组入方向规则控制检查 | 安全组入方向规则应满足最小化访问控制原则。<br>一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。 |
| 项目服务中的委托权限配置检查 | 请在IAM委托设置中删除对应委托权限（Security Administrator，Tenant Administrator），提高账号安全性。<br>高危操作！请根据您的需要谨慎处理。 |
| 全局服务中的委托权限配置检查 | 请在IAM委托设置中删除对应委托权限（Security Administrator，Tenant Administrator），提高账号安全性。<br>高危操作！请根据您的需要谨慎处理。 |
| 管理员账号AK/SK启用检查 | 访问密钥（AK/SK，Access Key ID/Secret Access Key）是账号的长期身份凭证。<br>由于管理员具有IAM用户管理权限，且具有大范围的操作权限。为了避免因AK/SK泄露带来的安全隐患，建议管理员账号不启用AK/SK身份凭证。 |
| 主机弱密码检查 | HSS提供基线检查功能，主动检测主机中口令复杂度策略，给出修改建议，帮助用户提升口令安全性。<br>如果提示需要修改，请根据修改建议进行修改，防止账户口令被轻易猜解。<br>高危操作！请根据您的需要谨慎处理。 |


版权所有 © 华为云计算技术有限公司

| 检查项名 | 加固建议 |
| --- | --- |
| 委托账号检查 | 通过创建委托，可以将资源共享给其他账号，或委托更专业的人或团队来代为管理资源。被委托方使用自己的账号登录后，切换到委托方账号，即可管理委托方委托的资源，避免委托方共享自己的安全凭证（密码/密钥）给他人，确保账号安全。<br>在云服务环境中，如果创建委托给个人账号，可能会导致不可信，因此不建议委托给个人账号，建议删除个人委托账号。<br>高危操作！请根据您的需要谨慎处理。 |
| 主机高危端口暴露检查 | HSS提供资产管理功能，主动检测主机中的开放端口，及时发现主机中含有风险的各项资产。<br>如果检测到开放了危险端口或者开放了不必要的端口，需要排查这些端口是否是正常业务使用，如果不是正常业务端口，建议关闭端口。对于危险端口建议进一步检查程序文件，如果存在风险建议删除或者隔离源文件。<br>高危操作！请根据您的需要谨慎处理。 |
| 检查主机是否存在Sudo漏洞 | HSS提供漏洞管理功能，检测Linux软件漏洞，通过与漏洞库进行比对，检测出系统和官方软件（非绿色版、非自行编译安装版，例如：SSH、OpenSSL、Apache、MySQL等）存在的漏洞，帮助用户识别出存在的风险。<br>请在HSS漏洞管理页面，对Sudo漏洞进行修复处理。 |
| OBS桶服务端加密检查 | OBS服务端加密是在上传对象到桶时，将数据在服务端加密成密文后存储。再次下载加密对象时，存储的密文会先在服务端解密为明文，再反馈给用户。将数据加密后存储到OBS桶中，提高数据的安全性。<br>请在OBS中开启服务端加密。 |
| CTS启用检查 | 云审计服务（Cloud Trace Service，CTS）可以将当前账户下所有的操作记录在追踪器中，通过查询和审计操作记录，实现安全分析、资源变更、合规审计、问题定位等。<br>请启用CTS检查，并配置追踪器。 |

- **手动检查项**

  a. 在基线检查页面的检查结果中，选择护网检查遵从包，并筛选手动检查的规范。

  **图 2-11** 手动检查项

  b. 单击目标子检查项所在行的“操作”列的“查看详情”，进入检查项目详情页面。


版权所有 © 华为云计算技术有限公司

c. 查看检查描述和检查过程，确认是否满足。

如果业务涉及对应检查项资源，根据检查过程进行资源自查；如果资源自查结果不满足检查项规则，可自主按照相关资料指南整改加固，加固完成之后通过检查结果页面将结果反馈到安全云脑。如果直接满足检查项规则，直接反馈结果到安全云脑即可。

d. 检查完成后，返回检查规范页面，单击目标检查项“操作”列的“反馈结果”。

e. 在弹出的确认框中，勾选检查结果，并单击“确定”。

## 2.4.2 漏洞管理

漏洞是攻击者入侵企业系统的主要手段之一，攻击者可以利用漏洞获取系统权限、窃取敏感信息或者破坏系统功能。完成漏洞整改可以有效地提高系统的安全性，预防潜在的攻击。

安全云脑提供漏洞修复帮助用户针对配置隐患和系统漏洞进行排查。安全云脑的漏洞管理分为Linux漏洞、Windows漏洞、Web-CMS漏洞、应用漏洞进行管理。

- Linux漏洞：内含常见Linux系统以及组件的各类漏洞，如内核漏洞、组件漏洞等。
- Windows漏洞：内含Windows系统最新漏洞以及补丁。
- Web-CMS漏洞：内含常见web-cms框架漏洞信息，如phpmyadmin等。
- 应用漏洞：内含常见应用类型漏洞，如fastjson、log4j2等。

### 修复说明

- **Linux、Windows漏洞**
  - 如下是近两年在攻防演练中被红队利用最频繁且对企业危害较高的系统漏洞，HSS漏洞库支持扫描该漏洞，如果使用HSS扫描时发现该漏洞，请优先排查修复。
    - Linux DirtyPipe权限提升漏洞（CVE-2022-0847）
  - 如果漏洞影响的软件未启动或启动后无对外开放端口，则实际风险较低，可滞后修复。
- **应用漏洞**
  - HSS不支持扫描如用友、金蝶等商用软件的漏洞，因此商用软件漏洞您需要自行排查。
  - 如果Web服务器的应用漏洞无法修复，您可以通过配置安全组规则，限制只可内网访问，或使用WAF防护（只能降低风险，通过内网渗透或规则绕过依然有被入侵的风险）。
  - 如下是近两年在攻防演练中被红队利用最频繁且对企业危害较高的应用漏洞，HSS漏洞库支持扫描这些漏洞，如果使用HSS扫描时发现这些漏洞，请优先排查修复。
    - nginxWebUI远程命令执行漏洞
    - Nacos反序列化漏洞
    - Apache RocketMQ命令注入漏洞（CVE-2023-33246）
    - Apache Kafka远程代码执行漏洞（CVE-2023-25194）

 版权所有 © 华为云计算技术有限公司 

- Weblogic远程代码执行漏洞（CVE-2023-21839）
- Atlassian Bitbucker Data Center远程代码执行漏洞（CVE-2022-26133）
- Apache CouchDB远程代码执行漏洞（CVE-2022-24706）
- F5 BIG-IP命令执行漏洞（CVE-2022-1388）
- Fastjson 1.2.8反序列化漏洞（CVE-2022-25845）
- Atlasssian Confluence OGNL注入漏洞（CVE-2022-26134）
- Apache Log4j2远程代码执行漏洞（CVE-2021-44228）

## 前提条件

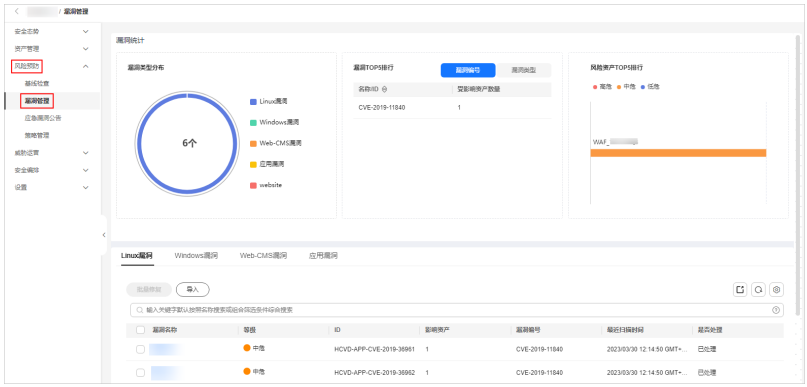
请确保修复漏洞时，您的业务处于低峰期或特定的变更时间窗。

## 修复漏洞操作步骤

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在安全云脑管理页面选择“风险预防 > 漏洞管理”，进入漏洞管理页面。

**图 2-12** 进入漏洞管理页面



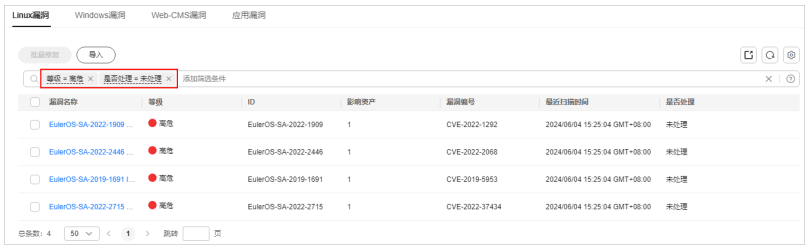
**步骤3** 筛选“等级”为“高危”、“是否已处理”为“未处理”的Linux漏洞、Windows漏洞和应用漏洞，优先进行修复。

**须知**

在进行漏洞修复前，需提前和您的业务相关人员确认漏洞修复是否会对业务造成影响。


版权所有 © 华为云计算技术有限公司

**图 2-13** 筛选漏洞



**步骤4** 修复漏洞。

- 修复Linux、Windows漏洞

  单击目标漏洞名称，在右侧弹出漏洞信息页面中，选择“受影响资产”页签，并在资产列表中，单击待处理资产所在行“操作”列的“修复”，系统提示修复操作触发成功。

---

**⚠ 注意**

执行主机漏洞修复可能存在漏洞修复失败导致业务中断，或者中间件及上层应用出现不兼容等风险，并且无法进行回滚。为了防止出现不可预料的严重后果，建议您通过云服务器备份（CSBS）为ECS创建备份，详细操作请参见**创建云服务器备份**。然后，使用空闲主机搭建环境充分测试，确认不影响业务正常运行后，再对主机执行漏洞修复。

---

- 修复Web-CMS漏洞、应用漏洞

  单击目标漏洞名称，在右侧弹出漏洞信息页面中，查看**修复建议**，并根据修复建议按照如下步骤，对“受影响资产”进行修复：

**图 2-14** 查看漏洞修复建议

a. 登录漏洞影响的主机，手动修复漏洞。

   漏洞修复有可能影响业务的稳定性，为了防止在修复漏洞过程影响当前业务，建议参考以下两种方案，选择其中一种执行漏洞修复：

   - **方案一：创建新的虚拟机执行漏洞修复**

     1) 为需要修复漏洞的ECS主机创建镜像，详细操作请参见**通过云服务器创建整机镜像**。

     2) 使用该镜像创建新的ECS主机，详细操作请参见**通过镜像创建云服务器**。


版权所有 © 华为云计算技术有限公司

3) 在新启动的主机上执行漏洞修复并验证修复结果。
4) 确认修复完成之后将业务切换到新主机。
5) 确定切换完成并且业务运行稳定无故障后，可以释放旧的主机。如果业务切换后出现问题且无法修复，可以将业务立即切换回原来的主机以恢复功能。

- **方案二：在当前主机执行修复**
  1) 为需要修复漏洞的ECS主机创建备份，详细操作请参见**创建云服务器备份**。
  2) 在当前主机上直接进行漏洞修复。
  3) 如果漏洞修复后出现业务功能问题且无法及时修复，立即使用备份恢复功能将主机恢复到修复前的状态，详细操作请参见**使用备份恢复服务器**。

**说明**

- 方案一适用于第一次对主机漏洞执行修复，且不确定漏洞修复的影响。新创建的ECS主机建议采用按需计费的方式创建，待业务切换完成后可以根据需要转换为包周期计费模式。如果漏洞修复不成功可以随时释放以节省开销。
- 方案二适用于已经有同类主机执行过修复，漏洞修复方案已经比较成熟可靠的场景。

**----结束**

# 2.5 步骤四：安全运营策略调整

## 2.5.1 启用安全模型

在智能建模页面安全云脑内置了基于应用、网络、主机多维度的安全分析模型，自动化的完成数据汇聚、分析和报警。

**护网/重保期间建议使用全量内置的模板创建告警模型并启用模型。**

通过模型汇聚分析筛选告警，降低误报率，提升值班人员分析处理效率。同时，也可以结合用户场景编辑模型进行模型调整，适配不同用户场景，降噪告警。

### 启用安全模型

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

**图 2-15** 模型模板页面


版权所有 © 华为云计算技术有限公司

**步骤3** 在模型模板列表中，选择未创建模型的模板，单击目标模板所在行“操作”列的“详情”，右侧弹出模板详情页面。

**步骤4** 在模板详情页面，单击右下角“创建模型”，进入新建告警模型页面。

**步骤5** 在新增告警模型页面中，配置告警模型信息。

- 管道名称：选择该告警模型的执行管道。

  模型对应管道可以从模型描述中的使用约束中获取，须与约束中的管道信息保持一致，也可以参考**执行管道**进行填写。

  **图 2-16** 基础配置


- 其他参数、设置保持默认值即可。

**步骤6** 设置完成后，单击“确定”，完成创建。

**步骤7** 重复**步骤3**-**步骤6**为其他模板创建告警模型。

**----结束**

## 执行管道

**表 2-8** 模型的执行管道

| 模型名称 | 管道 | 是否开启 | 状态 | 备注 |
| --- | --- | --- | --- | --- |
| 应用-分布式url遍历攻击 | sec-waf-access | 推荐开启 | 开箱即用已开启 | -- |
| 应用-源ip对域名进行爆破攻击 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 应用-源ip进行url遍历 | sec-waf-access | 推荐开启 | 开箱即用已开启 | -- |


版权所有 © 华为云计算技术有限公司

| 模型名称 | 管道 | 是否开启 | 状态 | 备注 |
| --- | --- | --- | --- | --- |
| 应用-WAF关键攻击告警 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 主机-虚拟机横向连接 | sec-hss-log | 推荐开启 | 开箱即用已开启 | -- |
| 网络-高危端口对外暴露 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 网络-登录爆破告警 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 主机-异常网络连接 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 网络-源ip对多个目标进行攻击 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| IPS告警去重 | sec-nip-attack | 按需开启 | -- | -- |
| 网络-命令注入告警 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 网络-恶意外联 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 主机-rootkit事件 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 主机-反弹shell | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | 已升级，需更新模型 |
| 主机-异地登录 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 主机-异常shell | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 主机-弱口令 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 主机-恶意程序 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 主机-暴力破解成功 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | -- |
| 主机-高危命令检测 | sec-hss-alarm | 推荐开启 | 开箱即用已开启 | 已升级，需更新模型 |
| 网络-检测异常连接行为 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 网络-检测黑客工具攻击 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |


版权所有 © 华为云计算技术有限公司

| 模型名称 | 管道 | 是否开启 | 状态 | 备注 |
| --- | --- | --- | --- | --- |
| 网络-恶意软件 [蠕虫、病毒、木马] | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 网络-僵尸网络 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 网络-后门 | sec-nip-attack | 推荐开启 | 开箱即用已开启 | -- |
| 应用-疑似存在源码泄露风险 | sec-waf-access | 推荐开启 | 开箱即用已开启 | -- |
| 身份-IAM账号爆破 | sec-iam-audit | 推荐开启 | 开箱即用已开启 | -- |
| 应用-疑似存在log4j2漏洞 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 身份-创建IAM委托 | sec-iam-audit | 推荐开启 | 开箱即用已开启 | -- |
| 身份-创建联邦登录 | sec-iam-audit | 推荐开启 | 开箱即用已开启 | -- |
| 身份-IAM账户添加子用户 | sec-iam-audit | 推荐开启 | 开箱即用已开启 | -- |
| 运维-挂载网卡 | sec-cts-audit | 推荐开启 | 开箱即用已开启 | -- |
| 运维-创建peering对等连接 | sec-cts-audit | 推荐开启 | 开箱即用已开启 | -- |
| 运维-资源绑定EIP | sec-cts-audit | 推荐开启 | 开箱即用已开启 | -- |
| 应用-疑似存在fastjson漏洞 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 应用-疑似存在 Java框架通用代码执行漏洞 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 应用-疑似存在Shiro漏洞 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 网络-CFW异常外联 | sec-cfw-risk | 推荐开启 | 开箱即用已开启 | -- |
| 网络-疑似存在DOS攻击 | sec-cfw-block | 按需开启 | 开箱即用已开启 | -- |
| 应用-登录爆破攻击 | sec-waf-attack | 推荐开启 | 开箱即用已开启 | -- |
| 主机-异常文件属性修改 | sec-hss-log | 推荐开启 | 开箱即用已开启 | -- |

 版权所有 © 华为云计算技术有限公司 

| 模型名称 | 管道 | 是否开启 | 状态 | 备注 |
| --- | --- | --- | --- | --- |
| 主机-恶意定时任务写入 | sec-hss-log | 推荐开启 | 开箱即用已开启 | -- |
| 主机-进程和端口信息隐匿 | sec-hss-log | 推荐开启 | 开箱即用已开启 | -- |
| 主机-异常文件权限修改 | sec-hss-log | 推荐开启 | 开箱即用已开启 | -- |
| 网络-疑似存在远程代码执行漏洞 | sec-nip-attack | 推荐开启 | -- | -- |
| 网络-存在敏感文件泄露 /目录遍历漏洞 | sec-nip-attack | 推荐开启 | -- | -- |
| 应用-疑似存在openfire鉴权绕过漏洞 | sec-waf-access | 推荐开启 | -- | -- |
| 应用-疑似存在 nginxWebUI 远程命令执行漏洞 | sec-waf-access | 推荐开启 | -- | -- |
| 应用-疑似存在 MinIO 信息泄露 | sec-waf-access | 推荐开启 | -- | -- |
| 应用-疑似存在 F5 BIG-IP 命令执行漏洞 | sec-waf-access | 推荐开启 | -- | -- |
| 应用-存在Spring Actuator信息泄露 | sec-waf-access | 推荐开启 | -- | -- |
| 主机-计划任务异常 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-疑似注册启动信息修改 | sec-hss-log | 推荐开启 | -- | -- |
| 主机-疑似发现webshell木马 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-疑似使用内网扫描工具 | sec-hss-log | 推荐开启 | -- | -- |
| 主机-挖矿行为检测 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-异常脚本调用 | sec-hss-log | 推荐开启 | -- | -- |
| 主机-勒索软件 | sec-hss-alarm | 推荐开启 | -- | -- |
| 应用-疑似人为WEB恶意入侵攻击 | sec-waf-attack | 推荐开启 | -- | -- |
| 网络-目录遍历攻击 | sec-ndr-risk | 按需开启 | -- | -- |


版权所有 © 华为云计算技术有限公司

| 模型名称 | 管道 | 是否开启 | 状态 | 备注 |
| --- | --- | --- | --- | --- |
| 网络-文件读写执行 | sec-ndr-risk | 按需开启 | -- | -- |
| 网络-绕过 | sec-ndr-risk | 按需开启 | -- | -- |
| 网络-代码执行 | sec-ndr-risk | 按需开启 | -- | -- |
| 网络-检测后门 | sec-ndr-risk | 按需开启 | -- | -- |
| 网络-log4j漏洞攻击 | sec-ndr-risk | 按需开启 | -- | -- |
| 网络-提权 | sec-ndr-risk | 按需开启 | -- | -- |
| 网络-检测恶意外联 | sec-ndr-risk | 按需开启 | -- | -- |
| 主机-异常权限提升 | sec-hss-alarm | 推荐开启 | -- | -- |
| 应用-疑似泛微 e-cology9登录漏洞 | sec-waf-access | 推荐开启 | -- | -- |
| 主机-信息破坏 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-网络异常行为 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-用户异常行为 | sec-hss-alarm | 推荐开启 | -- | 已升级，需更新模型 |
| 主机-容器异常 | sec-hss-alarm | 推荐开启 | -- | -- |
| 应用-waf 告警恶意ip攻击 | sec-waf-attack | 推荐开启 | -- | -- |
| 主机-系统异常变更 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-漏洞利用 | sec-hss-alarm | 推荐开启 | -- | 已升级，需更新模型 |
| 主机-集群异常行为 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-异常进程 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-黑客工具检测 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-扫描侦查 | sec-hss-alarm | 推荐开启 | -- | -- |
| 主机-关键文件路径变更 | sec-hss-alarm | 推荐开启 | -- | 新增 |


版权所有 © 华为云计算技术有限公司

| 模型名称 | 管道 | 是否开启 | 状态 | 备注 |
| --- | --- | --- | --- | --- |
| 主机-异常外联行为 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-文件/目录变更 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-尝试暴力破解 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-可疑进程异常访问文件 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-容器异常启动 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-非可信进程运行 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-Crontab可疑任务 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 主机-用户账号变更 | sec-hss-alarm | 推荐开启 | -- | 新增 |
| 网络-CFW恶意外部攻击 | sec-cfw-risk | 推荐开启 | -- | 新增 |
| 应用-疑似存在目录爆破 | sec-nginx-access | 按需开启 | -- | -- |
| 应用-疑似存在dos攻击风险 | sec-nginx-access | 按需开启 | -- | -- |
| 应用-python恶意爬虫 | sec-nginx-access | 按需开启 | -- | -- |
| 应用-用户异常登录疑似爆破 | sec-nginx-access | 按需开启 | -- | -- |
| 应用-疑似撞库攻击 | sec-nginx-access | 按需开启 | -- | -- |
| 网络-主机非法探测 | sec-vpc-flow | 按需开启 | -- | -- |
| 网络-端口非法扫描 | sec-vpc-flow | 按需开启 | -- | -- |

## 2.5.2 启用流程和剧本

### 操作场景

数据采集后，针对云上安全事件提供了安全编排剧本，实现安全事件的高效、自动化响应处置。


版权所有 © 华为云计算技术有限公司

安全云脑内置的流程默认已启用，无需再进行手动启用；内置的剧本已激活默认版本，仅需启用对应剧本即可。建议启用以下剧本：

**表 2-9** 启用剧本

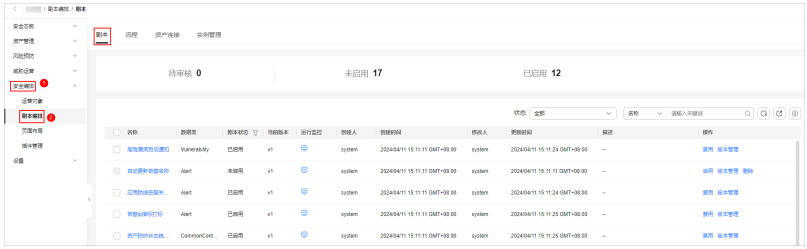
| 剧本名称 | 描述 |
| --- | --- |
| **重复告警自动关闭** | 将近7日内第二次及第二次以上出现的告警状态置为关闭，并关联7日内同名告警 |
| **高危告警自动通知** | 对威胁级别为High或者Fatal的告警进行邮件或者短信通知 |

### 启用流程和剧本

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“安全编排 > 剧本编排”，默认进入剧本管理页面。

**图 2-17** 进入剧本管理页面



**步骤3** 在剧本页面中，分别筛选“重复告警自动关闭”和“高危告警自动通知”剧本，如果剧本未启用，单击剧本所在行“操作”列的“启用”。

**步骤4** 在弹出启用确认信息框中，选择最新的剧本版本，并单击“确认”。

**说明**

“高危告警自动通知”流程需要使用消息通知服务（Simple Message Notification，SMN）来创建安全云脑告警通知主题，并完成订阅即可接收到告警通知。请参考**如何创建并订阅主题**配置护网过程中需要进行告警通知的人员。

**----结束**

# 2.6 步骤五：安全监控与应急响应

## 2.6.1 值班监控

### 操作场景

安全云脑提供了4+1个大屏，一个是综合态势感知大屏，其他四个大屏是值班响应大屏、资产大屏、威胁态势大屏和脆弱性大屏。

**护网开始之前我们已经完成了自查整改，清零了所有未处理的运营数据。**


版权所有 © 华为云计算技术有限公司

**护网及重保期间，安全值班人员需要重点关注“值班响应大屏”的数据信息，当有告警冒泡出来的时候，及时进行告警处理，清零全部告警数据。**

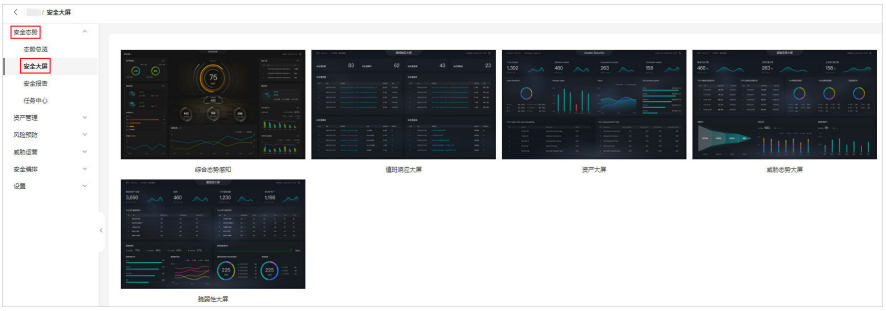
**通过告警详情页数据进行告警分析，如果需要结合其他日志数据，可通过安全分析在对应数据管道进行查询统计溯源。误报告警直接关闭，有风险告警可通过“一键阻断”能力应急阻断。**

## 值班监控

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“安全态势 > 安全大屏”，进入安全大屏页面。

**图 2-18** 进入安全大屏页面



**步骤3** 单击“值班响应大屏”图片，进入值班响应大屏信息页面后，在“未处理告警”模块中，单击告警描述，页面跳转到“告警详情”页面。

**图 2-19** 值班响应大屏


**步骤4** 分析告警。

告警详情页面可以查看告警总览、上下文、关系图和评论信息。

- **总览**页面可以看到告警摘要、处理建议、相关基础信息和涉及的详情信息等。
- **上下文**页面可以看到告警的上下文关键信息和全文信息。
- **关系图**页面中是告警关联的其他运营数据。
- **评论**页面中，可以查看评论信息，评论信息中是告警所有的处置和评论历史信息。

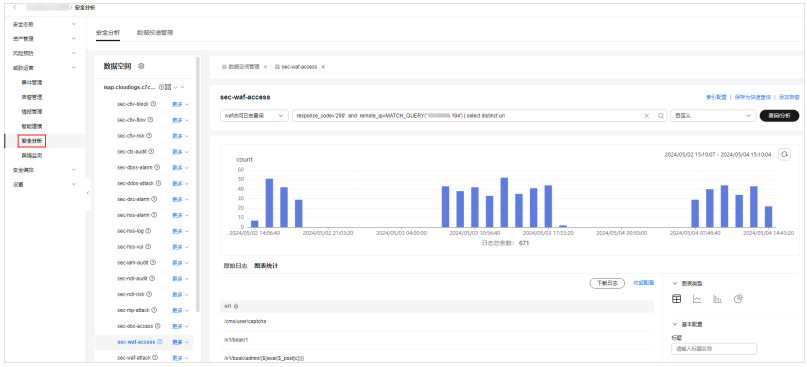
不同的告警结合不同的信息进行分析，可以通过告警关联信息，告警payload，告警详情分析。


版权所有 © 华为云计算技术有限公司

**图 2-20** 告警详情示例

如果需要结合历史或者其他日志进行分析的，也可以使用安全分析进行统计分析，进一步判断告警是否有风险。

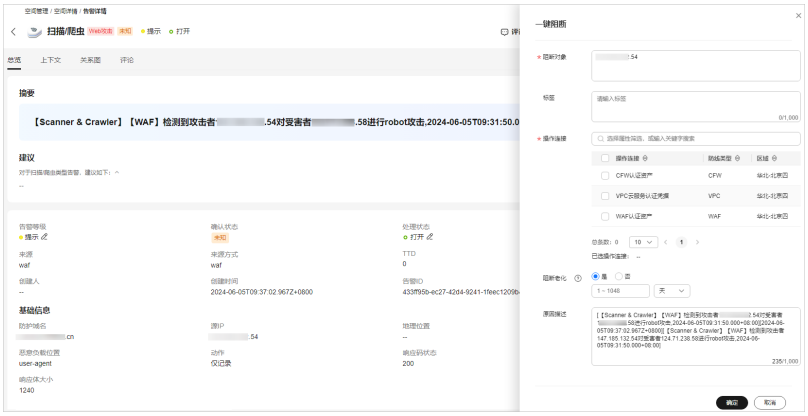
**图 2-21** 安全分析示例



**步骤5** 应急处置告警。

1. 通过告警详情页面数据并结合安全分析，分析出告警有风险，就可以通过告警详情页面，单击右上角“一键阻断”，对攻击IP进行阻断。
2. 配置阻断信息。

**图 2-22** 一键阻断




版权所有 © 华为云计算技术有限公司

**表 2-10** 一键阻断

| 参数名称 | 参数说明 |
| --- | --- |
| 阻断对象 | 告警攻击IP。 |
| （可选）标签 | 自定义应急策略的标签。 |
| 操作连接 | 选择该策略的操作连接，具体请参见**表2-11**。 |
| 阻断老化 | 确认是否老化该条阻断。<br>建议设置老化时间为护网/重保周期时间，护网/重保结束之后封堵失效。 |
| 原因描述 | 自定义该策略的描述信息。 |

**表 2-11** 推荐阻断策略

| 告警类型 | 对应防线 | 推荐阻断策略 | 阻断效果 |
| --- | --- | --- | --- |
| HSS告警 | 主机防线 | 建议优先采用VPC策略阻断 | 下发策略主机访问控制封堵攻击IP |
| WAF告警 | 应用防线 | 建议优先采用WAF策略阻断 | 下发策略WAF黑名单控制攻击IP |
| CFW告警 | 网络防线 | 建议优先采用CFW策略阻断 | 下发策略CFW黑名单控制攻击IP |
| IAM告警 | 身份防线 | 建议优先采用IAM策略阻断 | 下发策略停用IAM用户 |
| OBS/DBSS告警 | 数据防线 | 当前可根据实际攻击场景和调查结果考虑使用VPC策略阻断/CFW策略阻断，隔绝防护资产和攻击源的网络通信等 | 下发策略对资源访问控制封堵攻击IP/下发策略CFW黑名单控制攻击IP |

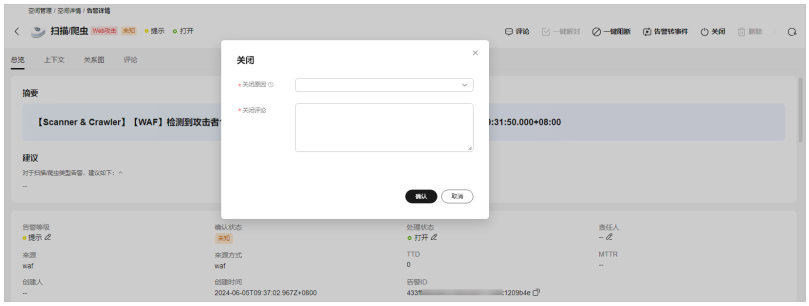
3. 单击“确认”。

**步骤6** 关闭告警。

1. 如果分析之后判断告警误报，可以通过告警详情页面，单击右上角“关闭”
2. 在弹出的确认框中，选择关闭原因并输入评论信息后，单击“确认”，关闭告警。


版权所有 © 华为云计算技术有限公司

**图 2-23** 关闭告警



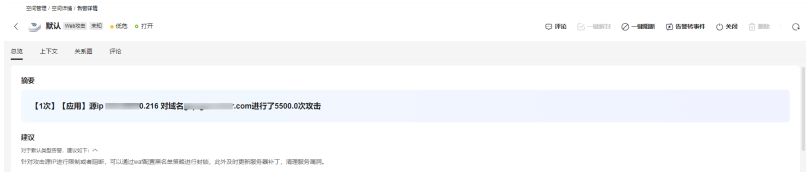

**----结束**

## 告警处置举例

此处以“【应用】源ip xx.xx.xx.xx 对域名demo.host.com进行了xx次攻击”告警为例进行说明。

- **收到告警**:

**图 2-24** 告警示例



- **分析思路**:

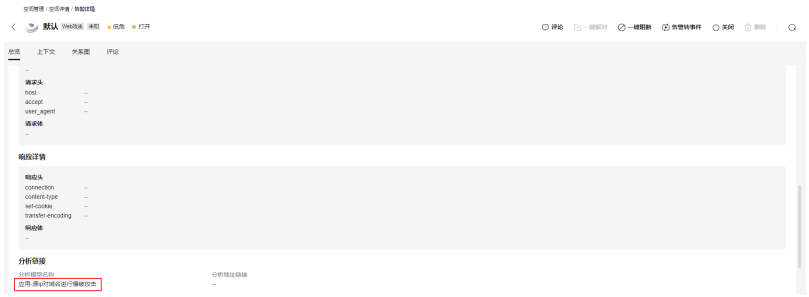
  源IP对域名进行爆破攻击，会对可能的子域名产生大量的枚举和测试。

  安全云脑通过分析Web应用防火墙的告警，统计1小时内的攻击次数，过滤出次数超过阈值的攻击进行告警。

- **查看告警**:

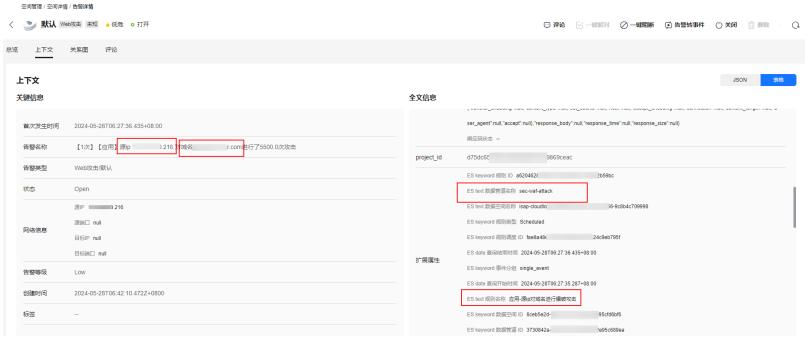
  告警详情页面可以看到告警攻击IP、攻击域名，分析模型是“应用-源ip对域名进行爆破攻击”数据管道名称为“sec-waf-attack”。

**图 2-25** 查看总览信息




版权所有 © 华为云计算技术有限公司

**图 2-26** 查看上下文信息



因为是统计类模型告警，可以结合WAF日志进行安全分析。单个源IP对域名进行多次攻击，虽然已经被WAF阻断，但是由于攻击次数较多，存在绕过WAF的风险，将多次攻击的行为冒泡出来。

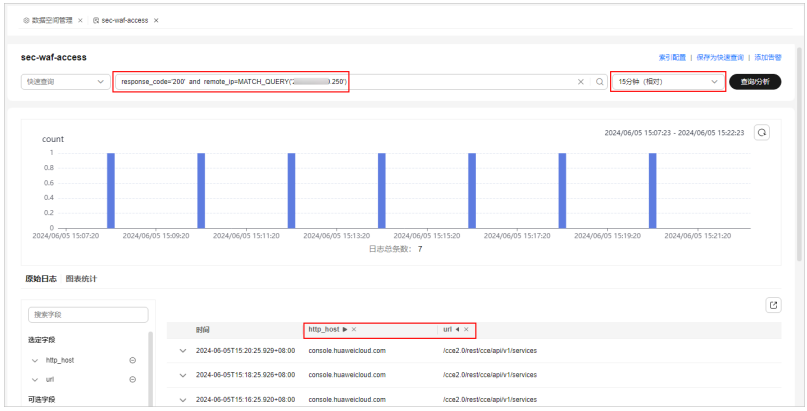
- **分析/处理告警**：

  a. 进入安全分析页面，打开sec-waf-access日志。

  b. 输入查询语句，筛选查询时间，并单击“查询/分析”。

  ```
  response_code='200' and remote_ip=MATCH_QUERY('xx.xx.xx.xx')
  ```

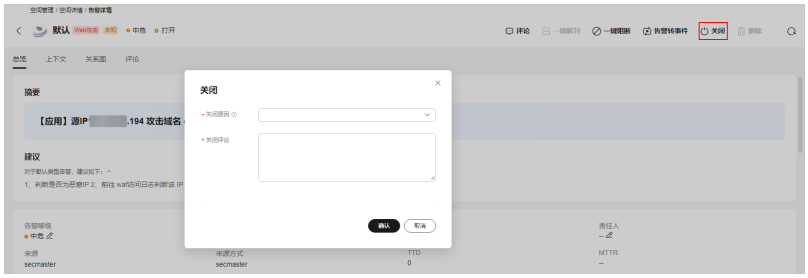
**图 2-27** 分析告警



  c. 根据查询结果，分析查询该IP有没有成功的访问请求。

  - 通过分析，如果该攻击ip请求成功的都是非敏感url，不存在攻击成功或绕过WAF检测的风险，直接在告警详情页面，单击“关闭”，并根据提示关闭告警。

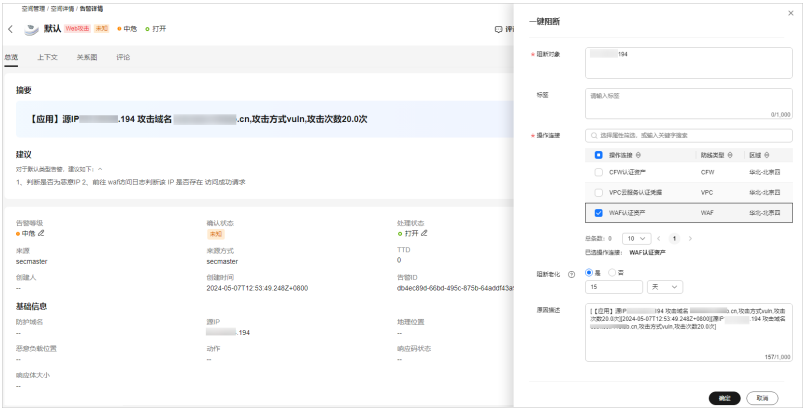
**图 2-28** 关闭告警




版权所有 © 华为云计算技术有限公司

- 如果是有风险url访问成功，直接在告警详情页面，单击“一键阻断”，填写风险IP，选择WAF防线，阻断老化15天，进行危险IP封堵。

**图 2-29** 一键阻断



## 典型告警处理指导

**表 2-12** 典型告警处理指导

| 告警类型 | 安全防线 | 依赖数据源 | 云脑智能模型 | 护网推荐处理建议 |
| --- | --- | --- | --- | --- |
| 侦察阶段典型告警 | 网络防线 | NIP攻击日志 | 网络-高危端口对外暴露 | 排查源IP对系统中的高危端口连接是否为业务需要。如果为业务需要，可修改模型脚本将该源IP过滤掉；如果非业务需要，则可修改相应安全组入方向规则，禁止高危端口暴漏公网，或者对源ip进行封堵拦截。同时为保证系统安全，尽量关闭不必要的端口。 |
| 侦察阶段典型告警 | 应用防线 | WAF攻击日志 | 应用-源ip进行url遍历 | 应急处理可以记录所有的访问请求和响应，及时发现攻击行为，针对攻击源IP进行限制或者阻断，可以通过配置黑名单策略进行封锁。 |
| 侦察阶段典型告警 | 应用防线 | WAF访问日志 | 应用-疑似存在源码泄露风险 | 应急处理可以记录所有的访问请求和响应，及时发现攻击行为，针对攻击源IP进行限制或者阻断，可以通过配置黑名单策略进行封锁。 |


版权所有 © 华为云计算技术有限公司

| 告警类型 | 安全防线 | 依赖数据源 | 云脑智能模型 | 护网推荐处理建议 |
| --- | --- | --- | --- | --- |
| 尝试攻击典型告警 | 应用防线 | WAF攻击日志 | 应用-WAF关键攻击告警、应用-疑似存在Shiro漏洞、应用-疑似存在log4j2漏洞、应用-疑似存在Java框架通用代码执行漏洞、应用-疑似存在fastjson漏洞 | 需要联系业务责任人，排查Web服务器是否存在相关漏洞，确认是否攻击成功。如果存在漏洞，应及时修改漏洞并加固安全；如果攻击成功，可结合威胁情报对攻击IP进行拦截。 |
| 尝试攻击典型告警 | 网络防线 | NIP攻击日志 | 网络-检测黑客工具攻击、网络-登录爆破告警 | 请确认该操作是否为正常业务人员的行为，如果不是，可以参考以下处置建议：<br>1. 切断网络连接：立即停止受攻击的设备或系统与网络的连接，以防止攻击者继续进行攻击或窃取数据。<br>2. 收集证据：记录攻击发生的时间、攻击者使用的IP地址、攻击类型和受影响的系统等信息，这些信息可能有助于后续的调查和追踪。 |
| 尝试攻击典型告警 | 网络防线 | CFW访问控制日志 | 网络-疑似存在DOS攻击 | 请确认该操作是否为正常业务人员的行为，如果不是，可在相关网络设备上进行IP拦截或封堵。 |
| 入侵成功典型告警 | 网络防线 | NIP攻击日志 | 网络-命令注入告警 | 如果发现源端口或目的端口为4444、8686、7778等非常用端口（可疑端口一般为4个数字），需联系责任人确认业务场景。如果不是正常业务行为，可能是黑客正在进行命令注入攻击，需要结合业务及主机日志查看是否被成功入侵，同时也可以对攻击ip采取拦截封堵等措施。 |
| 入侵成功典型告警 | 网络防线 | NIP攻击日志 | 网络-恶意软件[蠕虫、病毒、木马] | 首先应该立即断开与互联网的连接，防止恶意软件进一步传播或者窃取您的敏感信息。之后可通过系统还原，杀毒软件等方式扫描和清除恶意软件。 |


版权所有 © 华为云计算技术有限公司

| 告警类型 | 安全防线 | 依赖数据源 | 云脑智能模型 | 护网推荐处理建议 |
| --- | --- | --- | --- | --- |
| 入侵成功典型告警 | 主机防线 | 主机安全告警日志 | 主机-暴力破解成功、主机-异常shell、主机-异地登录 | 请确认该事件是否攻击成功，如果攻击成功，表明该主机已经失陷，需要进行主机隔离，防止风险扩散，之后对失陷的主机进行加固。 |
| 入侵成功典型告警 | 主机防线 | 主机安全日志 | 主机-进程和端口信息隐匿、主机-异常文件属性修改 | 及时判断是否是内部人员操作，是否为误操作。如果是异常进程，或文件存在恶意行为，执行相关命令结束进程。 |
| 防御绕过典型告警 | 主机防线 | 主机安全告警日志 | 主机-rootkit事件 | 立即确认该Rootkit安装是否正常业务引起。如果是非正常业务引起的，建议您立即登录系统终止该Rootkit安装行为，利用主机安全告警信息全面排查系统风险，避免系统遭受进一步破坏。 |
| 权限维持典型告警 | 主机防线 | 主机安全告警日志 | 主机-反弹shell、主机-恶意程序 | 联系所属主机的责任人，登录到主机上停止恶意程序并删除恶意文件，同时进一步排查是否存在可疑进程，是否开放了可疑端口，是否有可疑连接等，并进一步检查自启动项，避免遗留，此外可以结合其他方式进行综合判断。 |
| 权限维持典型告警 | 网络防线 | NIP攻击日志 | 网络-检测异常连接行为 | 首先需要确认是否为真实的异常行为，而非误报或误判。可以通过多个方法进行确认，例如，查看日志记录、使用网络监控工具等。一旦确认存在异常连接行为，需要立即采取措施切断该异常连接，消除恶意软件，以避免进一步安全问题的发生。 |
| 横向移动典型告警 | 主机防线 | 主机安全日志 | 主机-虚拟机横向连接 | 建议通过堡垒机等审计记录查看该命令是程序执行还是人为操作，如果为人为操作，需联系对应操作人确定，风格为非正常业务人员操作，需尽快确定该行为是否为异常恶意行为，是否危害到对应虚拟机，及时采取措施，保护计算机和系统的安全。 |
| 持久化控制典型告警 | 网络防线 | NIP攻击日志 | 网络-后门 | 首先应该立即断开与互联网的连接，防止后门进一步传播或者窃取您的敏感信息。可以使用杀毒软件进行扫描和清除后门，并查找和删除可疑文件，确保系统的安全性。 |

 版权所有 © 华为云计算技术有限公司 

| 告警类型 | 安全防线 | 依赖数据源 | 云脑智能模型 | 护网推荐处理建议 |
| --- | --- | --- | --- | --- |
| 持久化控制典型告警 | 主机防线 | 主机安全日志 | 主机-恶意定时任务写入 | 请确认是否为正常业务任务，如果不是，可以停用计划任务。 |

## 2.6.2 风险控制

### 操作场景

支持通过应急策略功能进行风险控制。

**安全云脑的应急策略功能可以联动CFW/WAF/VPC安全组对源IP进行封堵和解封。**

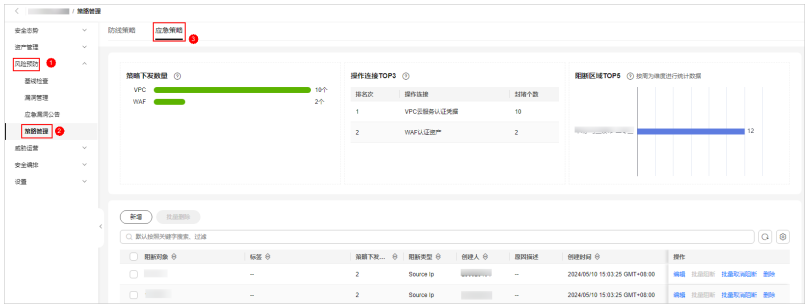
当护网和重保过程中有情报需要进行单个IP或多个IP进行批量阻断时候，可以通过该功能进行全策略封堵。

### 风险控制

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“风险预防 > 策略管理”，进入策略管理页面后，选择“应急策略”页签，进入应急策略管理页面。

**图 2-30** 进入应急策略管理页面



**步骤3** 在应急策略管理页面中，单击“新增”，右侧弹出新增应急策略页面。

**步骤4** 在新增策略页面中，配置策略信息。

**表 2-13** 新增应急策略

| 参数名称 | 参数说明 |
| --- | --- |
| 阻断对象 | 输入需要阻断的单个（或多个）IP地址或IP地址段，如有多个IP地址或地址段，请使用英文逗号隔开。 |
| 标签 | 自定义应急策略的标签。 |
| 操作连接 | 选择该策略的操作连接。 |
| 阻断老化 | 确认是否老化该条阻断。 |


版权所有 © 华为云计算技术有限公司

| 参数名称 | 参数说明 |
| --- | --- |
| 原因描述 | 自定义该策略的描述信息。 |

**步骤5** 单击“确定”。

**----结束**

# 2.7 步骤六：安全保障总结

## 2.7.1 安全报告

事后对攻防过程中重要攻击或防守成果进行溯源分析，对于过程中暴露的安全能力风险、应急处理流程缺失、安全意识薄弱等问题进行梳理，输出复盘报告。

**安全云脑报告可以在护网期间每天输出报告，也可以自定义基于护网整个周期统计安全报告。**

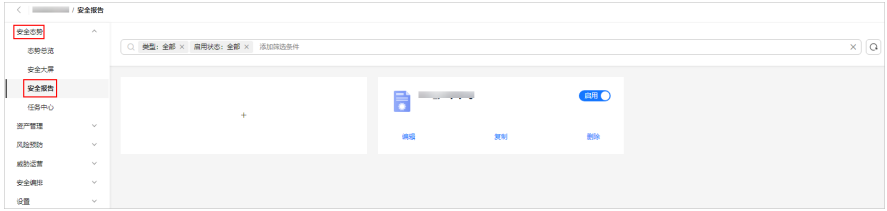
报告中可以涵盖统计周期内安全评分、运营数据统计（涵盖资产安全、脆弱性、安全响应等），也可基于不同维度（资产、威胁、响应等）进行详细报告展示。

### 创建安全报告

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

**步骤2** 在左侧导航栏选择“安全态势 > 安全报告”，进入安全报告页面。

**图 2-31** 进入安全报告页面



**步骤3** 在安全报告页面中单击 + 按钮，进入配置报告基本信息页面。

**步骤4** 配置报告基本信息。

**表 2-14** 报告基本信息参数说明

| 参数名称 | 参数说明 |
| --- | --- |
| 报告名称 | 自定义报告名称。 |
| 报告类型 | 选择“自定义”报告类型。 |
| 报告发送频次 | 根据根据护网周期，选择安全报告的发送频次。 |
| 发送规则 | 根据根据护网周期，设置报告的发送时间以及统计范围。<br>最多可添加5个发送规则。 |


版权所有 © 华为云计算技术有限公司

| 参数名称 | 参数说明 |
| --- | --- |
| 邮件标题 | 设置报告发送邮件的标题信息。 |
| 报告接收人邮箱 | 添加接收人邮箱地址。<br>• 最多可添加100个邮箱地址。<br>• 有多个邮箱地址，请使用英文分号隔开。例如：test01@example.com;test02@example.com |
| （可选）抄送 | 添加抄送人邮箱地址。<br>• 最多可添加100个邮箱地址。<br>• 有多个邮箱地址，请使用英文分号隔开。例如：test03@example.com;test04@example.com |
| （可选）备注 | 自定义安全报告的备注信息。 |

**步骤5** 单击右上角“下一步：报告选择”，进入报告选择页面。

**步骤6** 在报告选择页面的左侧已有报告布局中，选择已有报告布局。

选择完成后，可以在右侧页面中预览报告样式。

（可选）如果涉及巡检或者响应处置等，请在报告的“Top5 应急响应”中，需要根据实际情况进行填写。

**步骤7** 单击右下角“完成”。

**----结束**

## 2.7.2 分析溯源

事后对攻防过程中重要攻击或防守成果进行溯源分析，针对过程中暴露的安全能力风险、应急处理流程缺失、安全意识薄弱等问题进行梳理，输出复盘报告。

**安全分析能力提供原始日志数据查询统计能力，可以针对原始数据进行溯源分析。**

### 分析溯源

**步骤1** 登录安全云脑控制台，并进入目标工作空间管理页面。

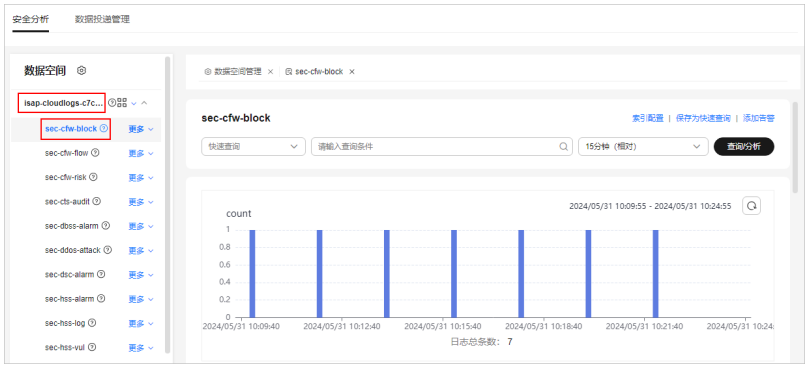
**步骤2** 在左侧导航栏选择“威胁运营 > 安全分析”，进入安全分析页面。

**图 2-32** 进入安全分析页面


**步骤3** 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，再单击管道名称，右侧将显示管道数据的检索页面。


版权所有 © 华为云计算技术有限公司

**图 2-33** 管道数据页面

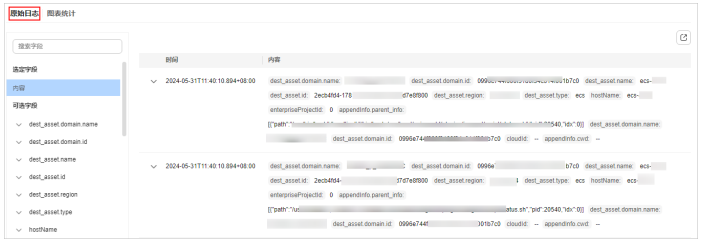



**步骤4** 在管道数据检索页面，选择查询分析时间，设置查询条件或直接输入查询语句进行溯源分析。

设置查询条件或直接输入查询语句操作参考**查询语法**。

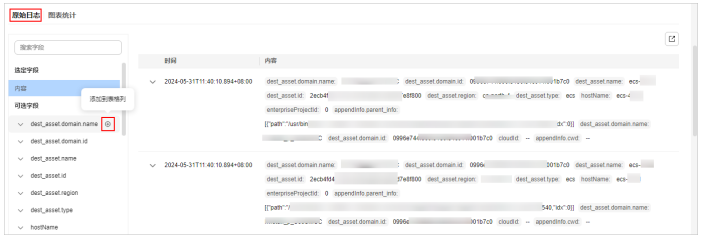
查询之后通过原始日志看到详细日志数据，如**图2-34**所示。

**图 2-34** 原始日志




同时，也可以通过显示字段，进行字段筛选显示查看分析，如**图2-35**所示。

**图 2-35** 选中显示字段




**----结束**


版权所有 © 华为云计算技术有限公司

## 常用查询语句

**表 2-15** 常用查询语句

| 需求 | 管道 | 查询语句 |
| --- | --- | --- |
| 某IP访问查询 | sec-waf-access | **x_forwarded_for='*x.x.x.x*' or remote_ip='*x.x.x.x*' and response_code='200' \| select x_forwarded_for,remote_ip,http_host,url,response_code** |
| url关键词访问查询 | sec-waf-access | **url like '**actuator**' and response_code='200' \| select *,count(x_forwarded_for) as num group by x_forwarded_for,remote_ip,http_host,url** |
| 某域名访问iptop | sec-waf-attack | **http_host=MATCH_QUERY('*www.xx.com*') \| select *,count(remote_ip) as num group by http_host,remote_ip** |
| 某IP攻击查询 | sec-waf-attack | **sip='*x.x.x.x*' and not attack='custom_whiteblackip' and not attack='custom_custom' \| select attack,sip,http_host,uri,hit_data,status** |
| 某域名被攻击查询 | sec-waf-attack | **http_host='*www.aa.com*' and not attack='custom_whiteblackip' and not attack='custom_custom' and not attack='robot' \| select attack,sip,http_host,uri,hit_data,status** |
| 某主机执行命令查询 | sec-hss-log | **(dest_asset.name='*aa*' or ipList='*x.x.x.x*') and alarmKey='proc_report_2' \| select dest_asset.name,ipList,appendInfo.cmdline,appendInfo.path** |
| 某主机登录查询 | sec-hss-log | **alarmKey like 'login_check_*' and ipList='*x.x.x.x*' \| select ipList,appendInfo.service_type,appendInfo.service_port,appendInfo.login_ip ,hostIp** |
| 某主机告警查询 | sec-hss-alarm | **(dest_asset.name='*hostname*' or ipList='*x.x.x.x*' ) \| select dest_asset.name,ipList,appendInfo.event_name,appendInfo.file_info,appendInfo.process_info** |


版权所有 © 华为云计算技术有限公司

| 需求 | 管道 | 查询语句 |
| --- | --- | --- |
| 某主机登录查询 | sec-hss-alarm | **appendInfo.event_type=4007 and (ipList='***x.x.x.x***' or appendInfo.forensic_info.login_ip='***x.x.x.x***') \| select appendInfo.forensic_info.login_ip,appendInfo.forensic_info.service_type,appendInfo.forensic_info.user_name,appendInfo.event_name,ipList** |


版权所有 © 华为云计算技术有限公司

# 3 使用安全云脑纳管华北-北京一 Region 资源

## 场景说明

由于“华北-北京一”region已转存量维护局点，存在无资源部署的问题。在此情况下，可以通过安全云脑实现资源纳管，支撑用户使用安全云脑进行安全运营。

支持纳管以下资源：

- 资产：

  主机、网站、数据库、VPC、EIP

- 日志：

  HSS安全日志、告警日志、漏洞扫描日志、基线日志；WAF攻击日志、访问日志；APIG请求日志；CTS服务日志；DCS告警日志；IAM审计日志；安全云脑基线日志

本场景介绍如何在“华北-北京四”region的安全云脑中完成操作，实现纳管“华北-北京一”region中云服务资源。

## 步骤一：在“华北-北京四”region 购买安全云脑

此步骤在“华北-北京四”region，以包周期购买1个月的1个配额的专业版安全云脑为例进行介绍。

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. 在总览页面中，单击“购买安全云脑”。
4. （可选）首次购买需要进行访问授权。

   在弹出的访问授权页面中，勾选同意授权并单击“确认”。
5. 在购买安全云脑页面，配置购买参数。

   **表 3-1** 购买安全云脑

| 参数名称 | 取值样例 | 参数说明 |
| --- | --- | --- |
| 计费模式 | 包周期 | 选择计费模式。 |


版权所有 © 华为云计算技术有限公司

| 参数名称 | 取值样例 | 参数说明 |
| --- | --- | --- |
| 区域 | 华北-北京四 | 根据待查看的云上资源所在的区域就近选择购买安全云脑的区域。 |
| 版本 | 专业版 | 选择安全云脑的版本，不同版本提供的功能存在差异。 |
| 主机配额 | 1 | 请根据当前账户下所有ECS主机资产总数设置配额数。 |
| 增值包 | • 安全大屏：开通<br>• 智能分析配额：1 GB/天<br>• 安全编排：1万次/天 | 根据需要选购安全大屏、智能分析配额、安全编排。 |
| 标签 | -- | 如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下选择同一标签，建议在TMS中创建预定义标签，也可以直接在此处创建标签。 |
| 购买时长 | 1个月 | 选择安全云脑购买时长。 |

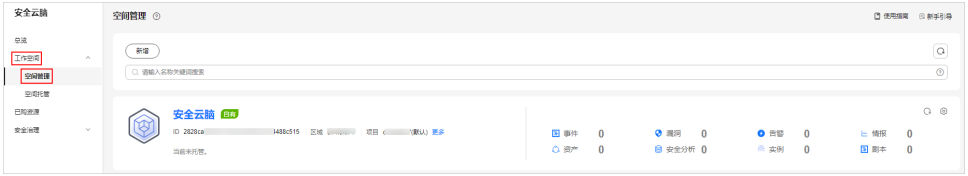
6. 确认参数配置无误后，在页面右下角单击“立即购买”。
7. 确认订单详情无误后，阅读并勾选《安全云脑服务(SecMaster)免责声明》，单击“去支付”。
8. 在支付页面，选择付款方式完成付款，完成购买操作。
9. 单击“返回安全云脑控制台”，返回安全云脑控制台页面。

## 步骤二：在“华北-北京四”region 创建工作空间

此步骤以在“华北-北京四”region，创建一个名称为“纳管北京一”工作空间为例进行介绍。

1. 在左侧导航栏选择“工作空间 > 空间管理”，进入工作空间管理页面。

**图 3-1** 工作空间管理页面




2. 创建首个工作空间。
   a. （可选）委托授权。

      首次使用时需要授权安全云脑访问您账号下的资源信息，便于统一查看并管理资源。

      i. 在空间管理页面上方单击“服务委托授权-当前租户”，右侧弹出授权页面。


版权所有 © 华为云计算技术有限公司

ii. 在授权页面中，默认已勾选所需全部权限，请勾选权限下方的“同意授权”，并单击“确认”。

b. 在工作空间管理页面中，单击“新增”，系统从右侧弹出新增工作空间页面。

c. 配置新建工作空间参数，参数说明如下表所示：

- 区域：根据待查看的云上资源所在的区域就近选择创建工作空间的区域。此处示例选择“华北-北京四”。
- 项目：选择工作空间所属的项目，此处示例选择“default”。
- 工作空间名称：自定义工作空间的名称。
- 其他参数：请根据需要进行配置。

d. 单击“确定”。

3. 重复2，再创建一个的用于纳管北京一云服务数据的工作空间。

由于每个Region的首个工作空间可自动加载当前Region所有数据与资产，并启用预置模型与剧本。后续新增的用于自定义运营的工作空间，不会自动加载数据与资产，需要用户自定义接入。因此，纳管北京一云服务需要再创建一个空间。

- 区域：此处示例选择“华北-北京四”。
- 工作空间名称：此处示例工作空间名称为“纳管北京一”。
- 其他参数：请根据需要进行配置。

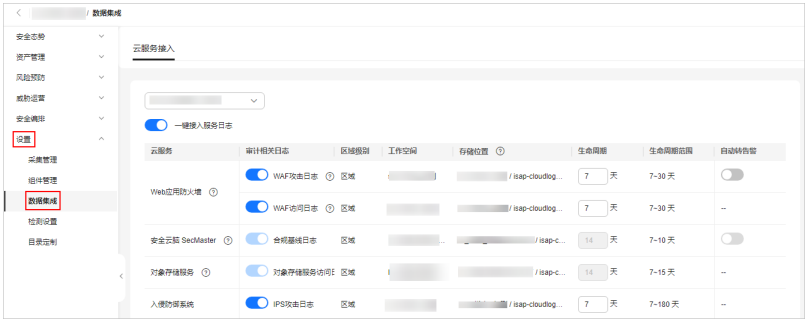
## 步骤三：接入“华北-北京一”region 日志、告警和漏洞数据

在已创建的用于纳管“华北-北京一”region的工作空间中接入“华北-北京一”region的日志、告警和漏洞数据。

此步骤以接入WAF、HSS日志、告警和漏洞数据为例进行介绍。

1. 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“纳管北京一”工作空间名称，进入工作空间管理页面。
2. 在左侧导航栏选择“设置 > 数据集成”，进入数据集成页面。

**图 3-2** 数据集成页面




3. 选择“华北-北京一”region，并在待接入云产品的“审计相关日志”列，单击  ，开启接入的云服务日志。

此处示例，接入WAF（攻击、访问日志）和HSS（告警、漏洞、安全日志）的所有类型日志。

 版权所有 © 华为云计算技术有限公司 

在安全云脑的“漏洞管理”页面可以接入主机漏洞扫描结果，如果数据集成操作时接入了主机漏洞扫描结果，但是未开启自动转告警，则在“漏洞管理”将不会展示主机相关的漏洞扫描情况。

4. 在待设置云产品的“自动转告警”列，单击  ，开启接入的云服务日志满足告警条件时，自动转为告警，并且在“告警管理”页面中进行展示。

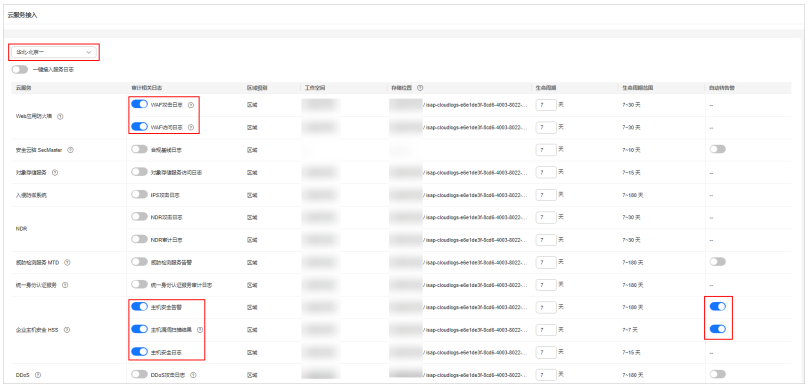
   此处示例，开启HSS“主机安全告警”、“主机漏洞扫描结果”转告警设置。

   如果此处未开启自动转告警，在对应日志满足告警条件时，将不会转为告警，也不会在“告警管理”页面中进行展示。

5. 单击“保存”，并在弹出的配置保存框中，单击“确定”。

   操作成功后，日志数据订阅预计在十分钟内生效。

**图 3-3** 接入日志数据



## 步骤四：订阅“华北-北京一”region 资产

在已创建的用于纳管“华北-北京一”region的工作空间中订阅“华北-北京一”region资产

1. 在左侧导航栏选择“资产管理 > 资产管理”，进入资产管理页面后，单击页面右上角“资产订阅设置”。
2. 在资产订阅页面中，开通“华北-北京一”资产订阅，并单击“确定”。

**图 3-4** 资产订阅


## 步骤五：在纳管“华北-北京一”的空间中创建告警模型

安全云脑支持利用模型对管道中的日志数据进行监控，如果数据信息在模型范围内容，将产生告警提示。此步骤以通过“应用-WAF关键攻击告警”模型创建告警为例进行介绍。

 版权所有 © 华为云计算技术有限公司 

请根据需要创建告警模型，详细操作请参见**创建告警模型**。

1. 在左侧导航栏选择“威胁运营 > 智能建模”，进入智能建模页面后，选择“模型模板”页签，进入模型模板页面。

**图 3-5** 模型模板页面

2. 在模板列表中，单击“应用-WAF关键攻击告警”模板所在行“操作”列的“详情”，右侧弹出模板详情页面后，单击右下角“创建模型”。
3. 在新增告警模型页面中，配置告警模型基础信息。
   - 管道名称：选择该告警模型的执行管道。此处示例选择“sec-waf-attack”。
   - 其他参数保持缺省值即可。
4. 设置完成后，单击页面右下角“下一步”，进入设置模型逻辑页面。
5. 在模型逻辑设置页面，无需进行配置，保持缺省值即可，单击页面右下角“下一步”，进入模型详情预览页面。
6. 预览确认无误后，单击页面右下角“确定”。

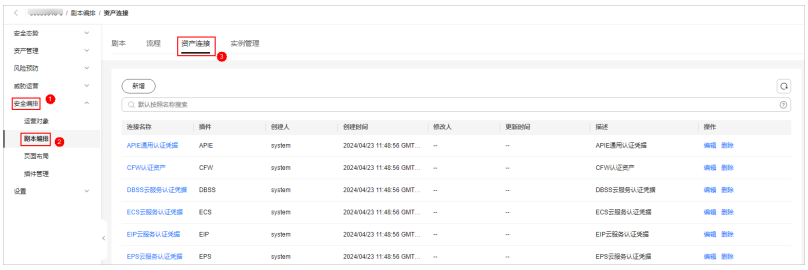
## 步骤六：创建连接器，连接“华北-北京一”云服务

在已创建的用于纳管“华北-北京一”region的工作空间中创建连接器，连接“华北-北京一”region云服务。

本步骤以创建HSS资产连接器为例进行介绍。

1. 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“资产连接”页签，进入资产连接管理页面。

**图 3-6** 资产连接管理页面



2. 在资产连接管理页面中，单击“新增”，右侧弹出新增资产连接面板。
3. 在新增资产连接面板中，配置资产连接参数。
   - 连接名称：输入资产连接名称。此处示例设置为“HSS-北京一”。
   - 插件：选择资产连接所需的插件。此处示例选择为“HSS”。
   - 连接类型：选择资产连接的类型。此处示例选择为“其它”。

 版权所有 © 华为云计算技术有限公司 

- 凭证信息：
  - endPoint：填写北京一endpoint信息，不同服务不同区域的终端节点不同，您可以从**地区和终端节点**中查询服务的终端节点。
    此处示例填写为：https://hss.cn-north-1.myhuaweicloud.com
  - iamEndpoint：填写北京一IAMendpoint信息，https://iam.cn-north-1.myhuaweicloud.com
  - 其他参数信息请根据实际情况进行填写。

4. 单击“确认”，返回资产列表，即可查询已经创建的资产连接信息。

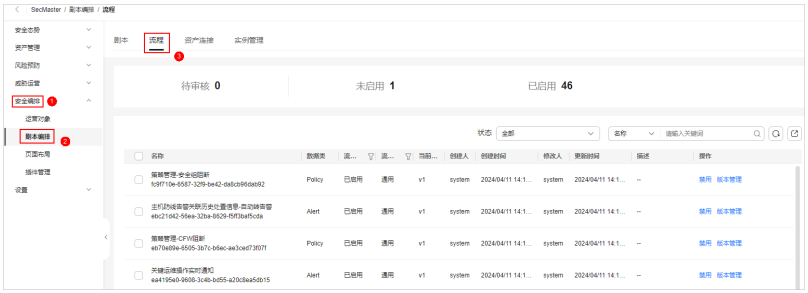
## 步骤七：创建响应剧本，联动“华北-北京一”region 云服务自动化处置

在已创建的用于纳管“华北-北京一”region的工作空间中创建响应剧本，联动“华北-北京一”region云服务自动化处置。

此步骤以修改“HSS文件隔离查杀”流程为例进行介绍。

1. 在左侧导航栏选择“安全编排 > 剧本编排”，进入剧本管理页面后，选择“流程”页签，进入流程管理页面。

**图 3-7** 流程管理页面



**复制流程版本**

2. 在“HSS文件隔离查杀”流程“操作”列，单击“版本管理”，弹出流程版本管理页面。
3. 在**流程版本管理**页面中，单击“版本信息”栏中v1版本所在行的“操作”列的“复制”。

**图 3-8** 复制流程版本

4. 在弹出的确认框中，单击“确定”。

**编辑并提交流程版本**

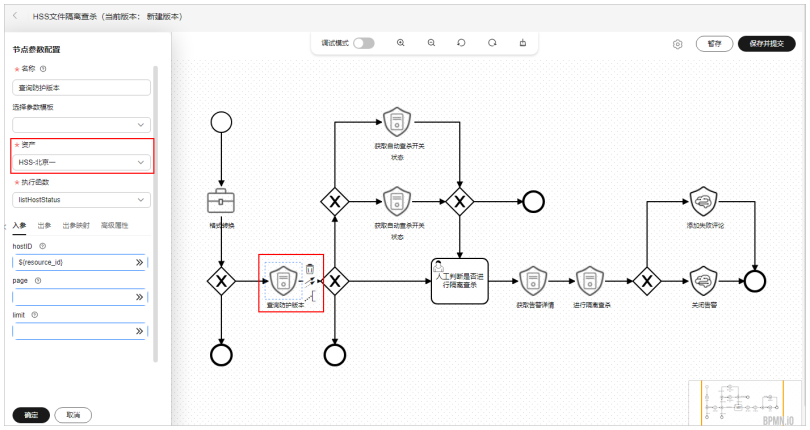
5. 在**流程版本管理**页面中，单击“版本信息”栏中草稿版本所在行的“操作”列的“编辑”。

 版权所有 © 华为云计算技术有限公司 

**图 3-9** 编辑流程

6. 在流程图绘制页面中，单击**所有节点排查**，将节点参数中的“资产”修改为新增的“HSS-北京一”。

**图 3-10** 修改节点参数



7. 单击右上角“保存并提交”，并在弹出的流程自动校验框中，单击“确定”。

**审核流程版本**

8. 编辑并提交流程版本后，页面返回流程管理页面。在**流程管理**页面中，单击“HSS文件隔离查杀”流程“操作”列“版本管理(1)”，右侧弹出流程版本管理页面。
9. 在**流程版本管理**页面中，单击v2版本所在行的“操作”列的“审核”。

**图 3-11** 审核流程版本

10. 在审核确认框中，选择“审核意见”为“通过”，并单击“确定”。

**激活流程版本**

11. 在**流程版本管理**页面中，单击“版本信息”栏中v2版本所在行的“操作”列的“激活”。


版权所有 © 华为云计算技术有限公司

**图 3-12** 激活流程版本

12. 在弹出确认框中，单击“确定”。

**启用流程**

“HSS文件隔离查杀”流程自动启用，无需手动操作。

**启用剧本**

13. 在剧本编排页面中，选择剧本页签，并单击“HSS文件隔离查杀”剧本所在行“操作”列的“启用”。

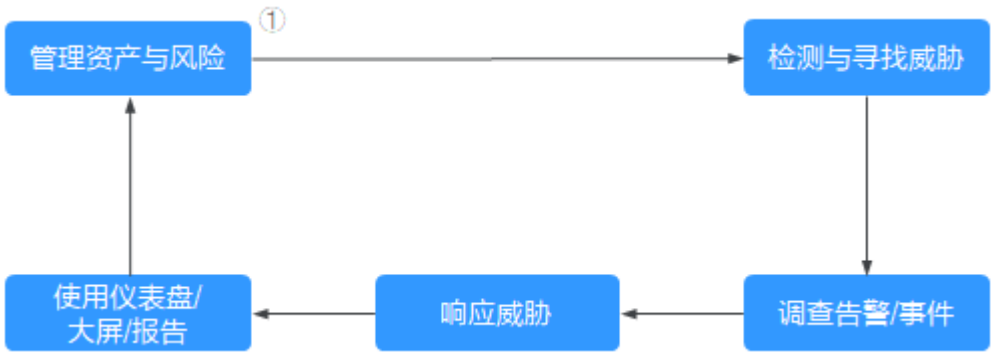
**图 3-13** 启用剧本

14. 在弹出的确认框中，选择v2版本，并单击“确认”。

## 安全运营

以上操作完成后，即可在“华北-北京四”region的指定工作空间中对“华北-北京一”region的云服务进行运营。

**图 3-14** 安全运营




- **管理资产与风险**

  安全运营的本质指安全风险管理，根据ISO的定义，其三要素包括“资产”，“脆弱性”和“威胁”。因此，梳理您要防护的资产，是安全运营的业务流起点。

  - **梳理资产**

    安全云脑可以帮助您：


版权所有 © 华为云计算技术有限公司

- 将云上资产从不同租户、不同Region汇集到一个视图中。
- 将云外资产导入到安全云脑中，并标记其所属的环境。
- 将资产的风险情况标识出来，例如：是否有不安全的配置、是否有OS或者应用漏洞、是否存在疑似入侵的告警、是否覆盖了对应的防护云服务（例如：ECS上应该安装HSS的Agent、域名应纳入到WAF的防护策略中）。

更多详细介绍及操作请参见**资产管理**。

- **检查并清理不安全的配置**

  在安全运营过程中，最常见的“脆弱性”是不安全的配置。安全云脑基于安全合规经验，形成自动化检查的基线，按照业界通用的规范标准，提供基线检查包。

  - 提供了多种基线标准。法规类标准，如：ISO系列标准、PCI DSS；隐私保护类，如：某国家或地区的隐私保护基线。
  - 云服务中的配置可以自动检查。如：IAM是否按角色进行授权分数、VPC的安全组中是否存在完全放通的策略、WAF的防护策略是否开启等。您可以根据“详情”中建议的方法，对配置进行加固。

  更多详细介绍及操作请参见**安全治理**、**基线检查**。

- **发现并修复漏洞**

  在修复配置类风险之后，安全云脑还可以帮助您，发现并修复安全漏洞。支持检测Linux软件漏洞、Windows系统漏洞、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。

  更多详细介绍及操作请参见**漏洞管理**。

- **检测与寻找威胁**

  数据源连接到安全云脑后，我们已经清点了要保护的资产，并查找及修复了不安全的配置和漏洞，接下来就是识别可疑活动和威胁。

  安全云脑可提供多种内置的由安全专家和分析团队根据已知威胁、常见攻击媒介和可疑活动上报链设计的模板，使您能够执行某些对应操作时收到此类威胁的通知。启用这些模板后，它们将自动在整个环境中搜索可疑活动。同时，可以根据需要自定义模板，以搜索或筛选出活动。

  同时，还支持云服务安全日志数据检索、分析功能，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。

  更多详细介绍及操作请参见**模型模板**、**安全分析**。

- **调查告警与事件**

  - 调查告警

    威胁检测模型分析大量的安全云服务日志，找到疑似入侵的行为，即告警。安全云脑中的告警包含如下字段：名称、等级、发起可疑行为的资产/威胁、遭受可疑行为的资产。安全值班人员，需要在较短的时间内对告警做出判定。如果风险较低，则关闭告警（如：重复告警、运维操作）；如果风险较高，需要单击“转事件”，将告警转为事件。

    更多详细介绍及操作请参见**查看告警信息**、**告警转事件**。

  - 调查事件

    告警转成事件后，就可以在事件管理中查看到生成的事件，事件生成后可以进行调查分析。您可以在事件上关联与可疑行为相关的实体：资产（如：

 版权所有 © 华为云计算技术有限公司 

VM）、情报（如：攻击源IP）、账号（如：泄露的账号）、进程（如：木马）等；也可以关联历史上相似的其他告警或事件。

更多详细介绍及操作请参见**查看事件信息**、**编辑事件**。

- **响应威胁**

  利用实时自动化，您可以通过对重复类型的告警实现常规响应自动化来减少告警研判工作量。同时，也可以利用自动化的剧本，完成自动化止血操作。

  更多详细介绍及操作请参见**安全编排**。

- **使用总大屏、报告**
  - **安全大屏**
    - 综合态势感知：可以还原攻击历史，感知攻击现状，预测攻击态势，呈现安全运营的全局指标情况。
    - 值班响应大屏：可以查看未处理告警、事件、漏洞、基线等需要处理的安全风险事项。
    - 资产大屏：可以查看资产总数、受攻击资产数、未防护资产数等需要处理的资产以及资产视角的风险情况。
    - 威胁态势大屏：可以查看DDoS攻击次数、网络攻击次数、应用拦截次数、主机层拦截次数等威胁攻击趋势及其防御、检测情况。
    - 脆弱性大屏：可以查看脆弱性资产、漏洞、基线、未防护资产等脆弱性配置或资产的趋势及分布。

    更多详细介绍及操作请参见**安全大屏**。
  - **安全报告**

    展示安全评分、基线检查结果、安全漏洞、策略覆盖等信息，您可以通过创建安全报告，及时掌握资产的安全状况数据。

    更多详细介绍及操作请参见**安全报告**。

 版权所有 © 华为云计算技术有限公司 

# 4 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。

 版权所有 © 华为云计算技术有限公司 

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**

 版权所有 © 华为云计算技术有限公司 

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。

 版权所有 © 华为云计算技术有限公司 

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**

 版权所有 © 华为云计算技术有限公司 