安恒信息
DAS-security 安全中国

明御®综合日志审计平台

V3.0

用户手册

文档版本：01

发布日期：2020-05-06

文档说明

产品名称	明御®综合日志审计平台
适用平台/版本	V3.0

修订记录

日期	修订版本	修改记录	修改人
2020-06-02	01	初次发布	

目 录

前言

感谢您选择安恒信息的网络安全产品。本手册对安恒信息明御®综合日志审计平台（以下简称“平台”或“DAS-Logger”）进行了简单介绍，并对平台的使用方法进行了详细描述。主要包括快速入门、Web 配置页面简介、首页、资产管理、事件管理、性能监控、规则库、弱点管理、审计概要、统计报表、系统管理、权限管理和系统日志。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于使用 DAS-Logger 的人员，包括系统管理员、权限管理员、操作管理员等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP、Syslog、HTTP、FTP、NFS、Samba 等基础网络通讯协议
- 数据库、服务器、网络安全设备、路由器、交换机等常见设备（系统）的基本工作原理和配置
- 网络安全相关知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段
- Syslog 协议的基本工作原理和配置

格式约定

本手册内容格式约定如下：

内容	说明
粗体字	Web 界面上的菜单、页签、页面名称、窗口名称、对话框名称，例如：“在菜单栏中选择**系统状态**进入**系统状态**页面，选择**接口状态**页签。”
< >	Web 界面上的按钮名称、复选框名称、文本框名称、选项名称等。例如：“微信认证失败，点击<**我要上网**>不弹出微信认证界面”。
➢	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等），例如：“在菜单栏选择‘**策略配置➢认证管理➢认证策略**’查看是否开启了认证策略”。

本手册图标格式约定如下：

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn/获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1. 快速入门

1.1 产品简介

明御®综合日志审计平台作为信息资产的综合性管理平台，通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件。为管理人员提供全局的视角，确保客户业务的不间断运营安全。通过采集网络资产设备上报的日志，实时监视网络各类操作行为及攻击信息。根据设置的规则，智能判断出各种风险行为，对风险行为进行报警。

DAS-Logger 分为硬件版和云上版两种版本。两种版本的功能基本相同，用户可根据需要进行购买。

1.1.1 产品功能

平台由采集器、通信服务器、关联引擎及平台管理器组成。主要功能如下：

1、 全面日志采集

全面支持 Syslog、SNMP、OPSec、XML、FTP 及本地文件等协议，可以覆盖主流硬件设备、主机及应用，保障日志信息的全面收集。实现信息资产（网络设备、安全设备、主机、应用及数据库）的日志获取，并通过预置的解析规则实现日志的解析、过滤及聚合。同时可将收集的日志通过转发功能转发到其它网管平台。

2、 大规模安全存储

内置 TB 级别存储设备，可以选配各种 RAID 级别进行数据冗余和安全保障。系统拥有多项自主知识产权的存储加密机制和查询机制，十分合适等保、密保等行业的应用要求。

3、 智能关联分析

实现全维度、跨设备、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，可轻松实现各资产间的关联分析。

4、 脆弱性管理

能够收集和管理来自各种 Web 漏洞扫描工具、主机漏洞扫描工具、网络漏洞扫描工具产生的扫描结果，并实时和用户资产收到的攻击危险进行风险三维关联分析。

5、 数据挖掘和数据预测

支持对历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。系统自带多种数据统计预测算法，可以根据历史数据的规律对未来的数据发生情况进行有效预测。

6、 可视化展示

实现对信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。通过各种事件的归化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力。事后的合规性统计分析处理，可对数据进行二次挖掘分析。

7、 分布式部署和管理

平台支持分布式部署，可以在中心平台管理规则、配置策略自动分发、远程自动升级等，极大地降低了分布式部署的难度，提高了可管理性。

8、 灵活的可扩展性

提供多种定制接口，实现强大的二次开发能力以及与第三方平台对接和扩展的能力。

1.1.2 产品特点

1、全面的智能收集功能

- 不间断的连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控。
- 可配置过滤和聚合功能以消除无关数据、合并重复的资产日志。
- 强大的数据压缩功能可节省带宽成本。

2、标准化日志

- 可采集各种安全事件日志（攻击、入侵、异常）。
- 可采集各种行为事件日志（内控、违规）。
- 可采集各种弱点扫描日志（弱点、漏洞）。
- 可采集各种状态监控日志（可用性、性能、状态）。
- 安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类。

3、创新的日志解析功能

- 解析规则激活：仅当接收到对应的日志后，规则才会被激活。
- 支持未识别日志水印处理，采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理。
- 支持多种解析方法（如正则表达式、分隔符、MIB 信息映射配置等）。
- 日志解析性能与接入的日志设备数量无关。

4、先进的关联算法

平台的关联分析引擎是产品的最大亮点之一。关联分析引擎采用了 In-Memory 的设计方式，全内存运算方式保证了事件分析较高的效率和实时性。相对于一般的日志审计产品通过 SQL 查询方式提供关联分析能力，平台在分析速度、分析维度、灵活性、IO 抗压能力方面都具有较大优势。

此外，在关联算法方面，平台有如下独到之处：

- 标准化之上的关联规则，适应性强。
- 可定制性强，几乎可根据通用事件的任何字段进行关联。
- 基于逻辑表达式，可以进行复杂关联。
- 时序宽容，无惧乱序。

5、可维护性及可扩展性

- 平台具有对自身的维护配置功能，例如：系统参数设置、系统日志管理等。
- 硬件系统采用模块化结构，保证系统内存、CPU 及储存容量可扩展。
- 硬件配置的升级不会引起软件的修改和开发。
- 每个组件都可以横向扩展，通过增加设备满足业务需求。

6、采用通用的安全事件标准

产品人员根据多年的网络安全经验，总结出了通用标准的安全事件归一化格式和分类体系结构。平台可以以标准方式处理以下元素：

- 各种安全事件日志（攻击、入侵、异常）
- 各种行为事件日志（内控、违规）
- 各种弱点扫描日志（弱点、漏洞）
- 各种状态监控日志（可用性、性能、状态）
- 安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击归类、检测设备归类

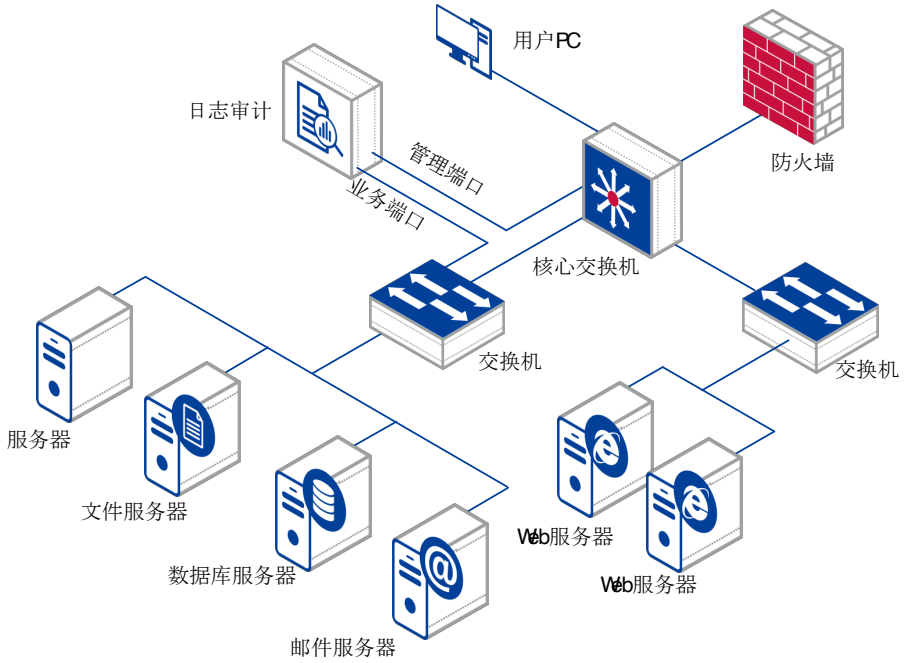
7、分布式设计

- 平台采用分布式设计，分为采集器、通讯服务器、关联分析引擎和管理中心四个部分。四个部分可以分布式部署，也可以组合部署，最大程度上兼顾了系统的可扩展性和灵活性。
- 基于 HTTPS 的通讯模式，使跨互联网部署成为了可能，异地监控不再需要昂贵的专线。可以适用于从简单网络环境到大型电信级网络环境。

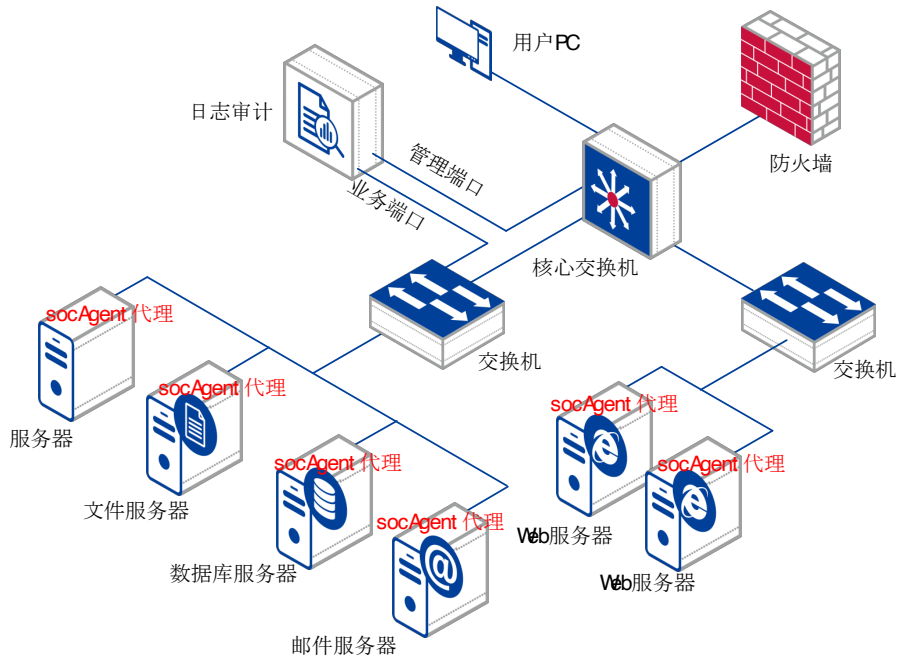
1.1.3 典型应用场景

DAS-Logger 支持两种不同的日志采集方式：

◆ 资产以 Syslog 等协议方式上传日志至平台（仅 Linux 服务器可以直接配置 Syslog 等协议）。组网方式如下图所示。



◆ 在资产上安装 socAgent，通过 socAgent 向平台发送日志。平台支持采集主机、网络设备、安全设备、应用等资产的日志信息。组网方式如下图所示。



1.2 角色与权限说明

不同角色的用户具有的权限不同，权限管理员可自定义角色，具体请以实际情况为准。系统默认的角色及权限可参考下表。

角色	权限
系统管理员	资产管理、规则库维护、事件管理、系统配置、安全知识库维护、弱点库管理、数据维护、安全知识导入、弱点导入、查看首页、审 计概要、性能监控与统计报表。
操作审计员	查看平台所有用户的操作记录。
权限管理员	对平台的用户、角色进行管理，并对登录安全进行设置。

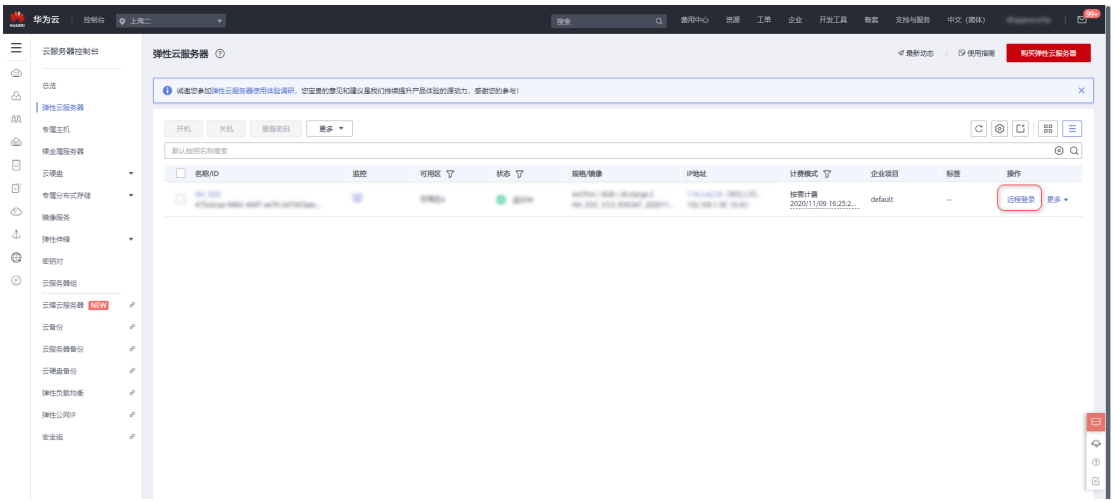
1.3 SSH 登录华为云安恒综合日志审计后台

由于安恒综合日志审计华为云镜像安全策略 SSH 服务设置了 root 用户不能直接 SSH 登录，必须需要先创建普通用户登录 SSH 后再 su - root 切成 root 用户

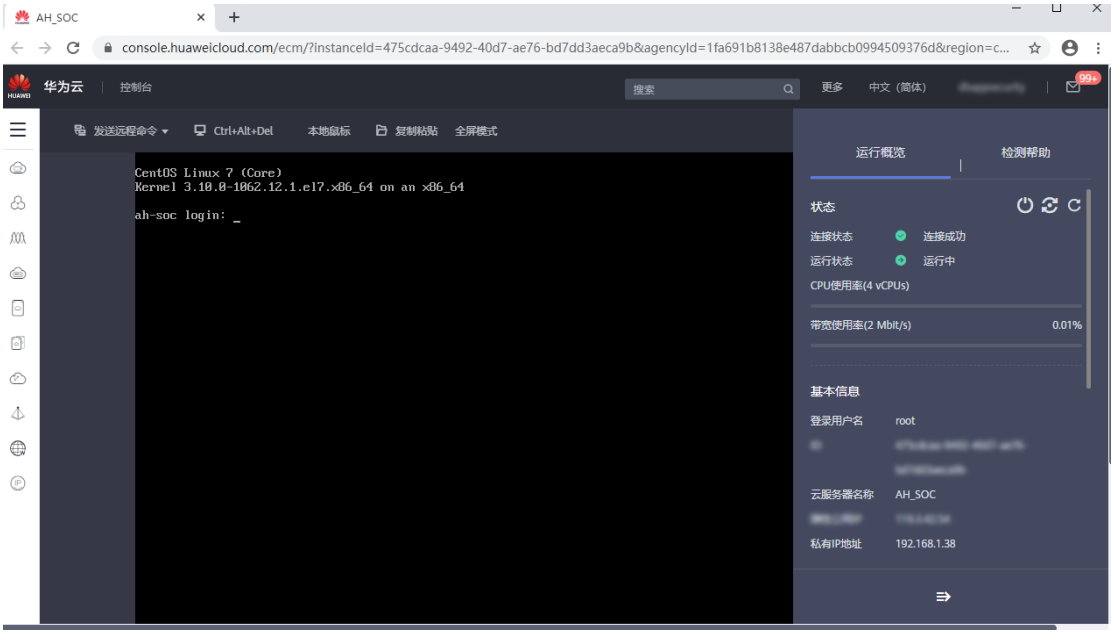
操作方法

1、 登录云服务器控制台，使用控制台提供的 VNC 方式登录

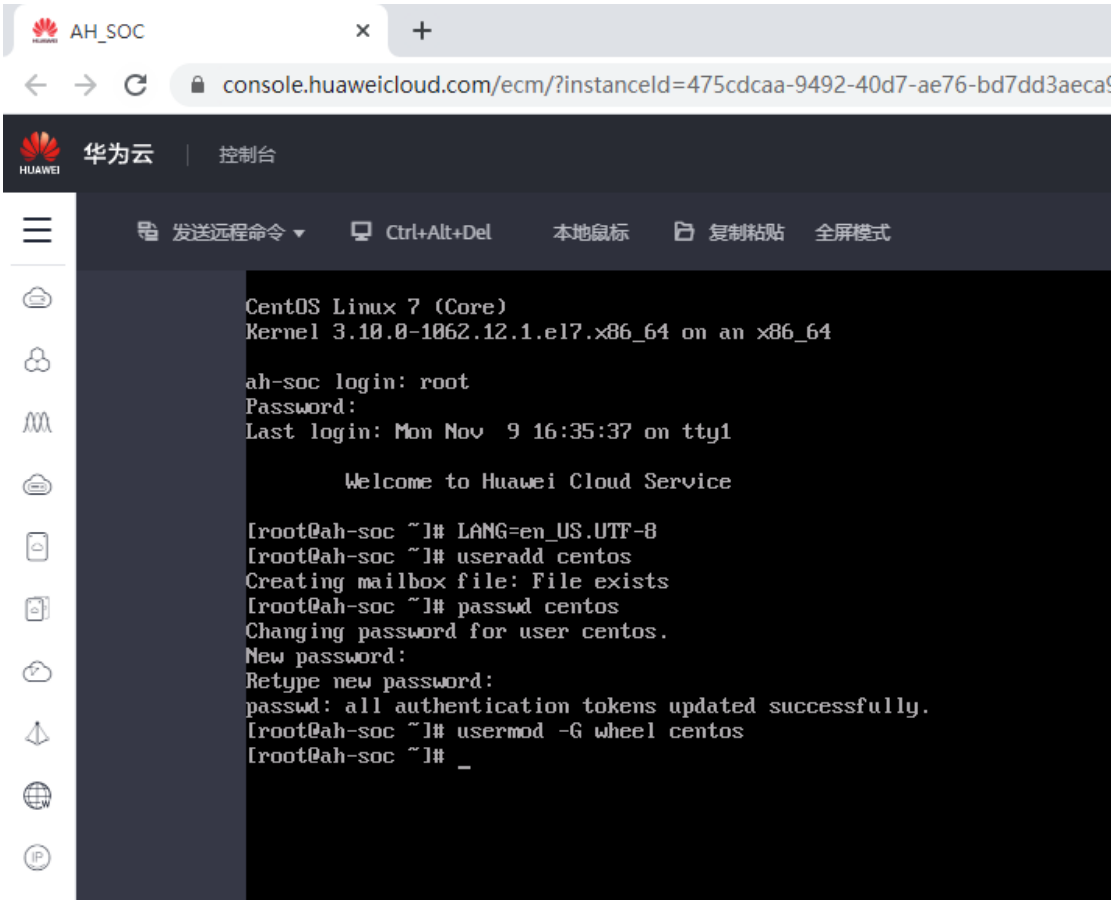
登录华为云服务器控制台，在弹性云服务器界面选择对应的云主机，点击远程登录



使用控制台提供的 VNC 方式登录



2、 输入云服务器的 root 账号和 root 密码登录



并输入如下命令

LANG=en_US.UTF-8

useradd centos

passwd centos

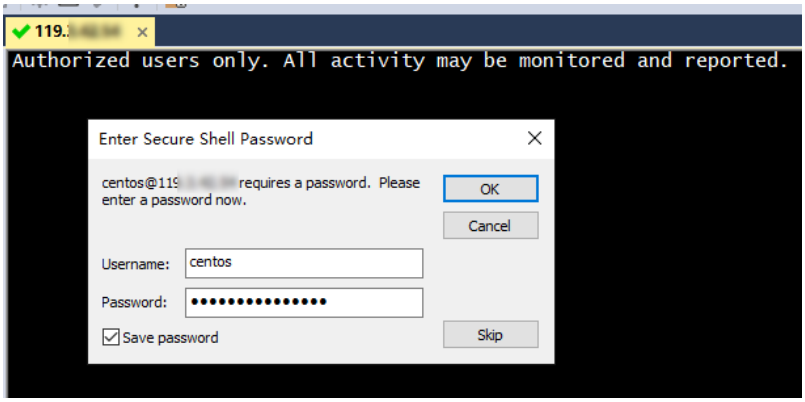
#给 centos 用户设置密码

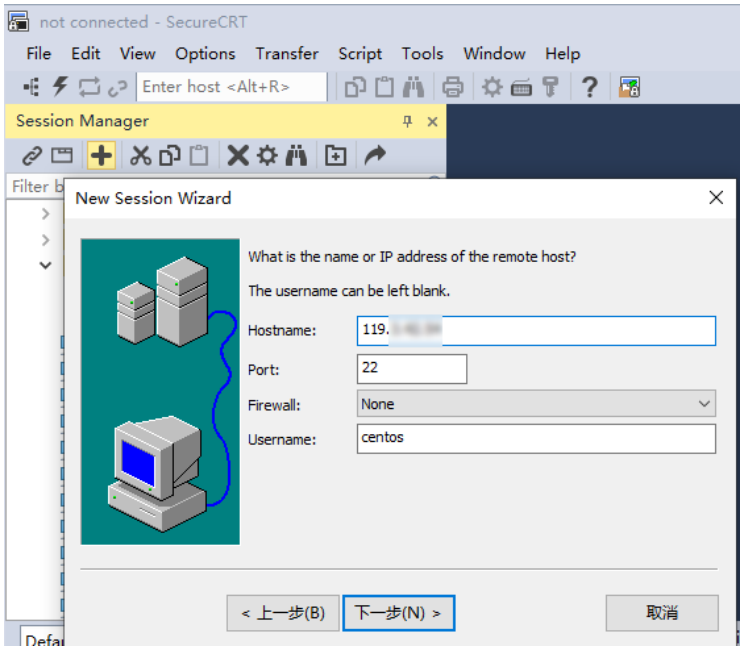
usermod -G wheel centos

并将 centos 用户加到 wheel 组

3、 使用 SSH 登录工具例如 SecureCRT

通过 centos 用户登录云主机的 SSH 后台





4、 登录成功后

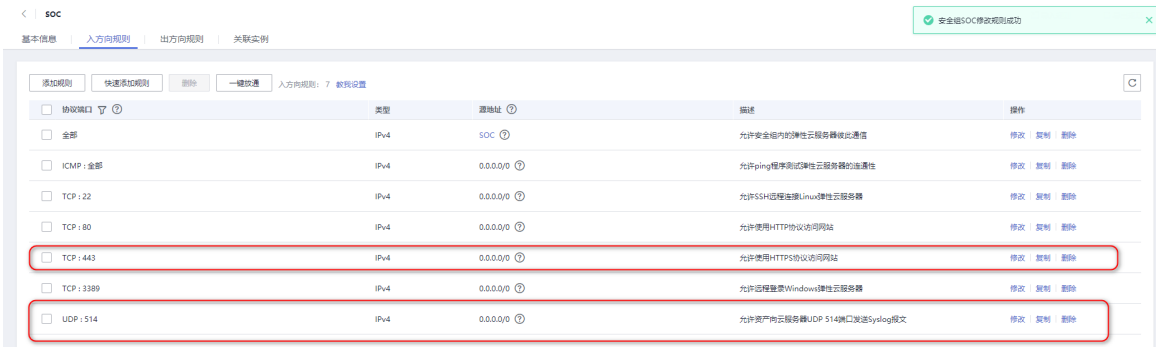
sudo su – root 切换成 root 用户

```
Authorized users only. All activity may be monitored and reported.
Last login: Mon Nov  9 16:42:26 2020 from 61.164.47.200

        Welcome to Huawei Cloud Service

[centos@ah-soc ~]$ LANG=en_US.UTF-8
[centos@ah-soc ~]$ sudo su - root
[sudo] password for centos:
Last login: Mon Nov  9 16:36:48 CST 2020 on tty2
[root@ah-soc ~]#
[root@ah-soc ~]#
```

1.4 Web 登录 SOC

云上版仅支持 Web 配置。云上版需保证配置资产 PC 与平台网络路由可达即可。

需要云主机安全组规则中开放 TCP443 与 UDP514 端口



用户可通过登录到设备的 Web 管理平台进行配置，操作方法如下：

步骤1. 在配置 PC 的 Web 浏览器（建议使用 Chrome 浏览器）地址栏中输入“”并回车，进入系统 Web 管理平台登录页面，如下图所示。

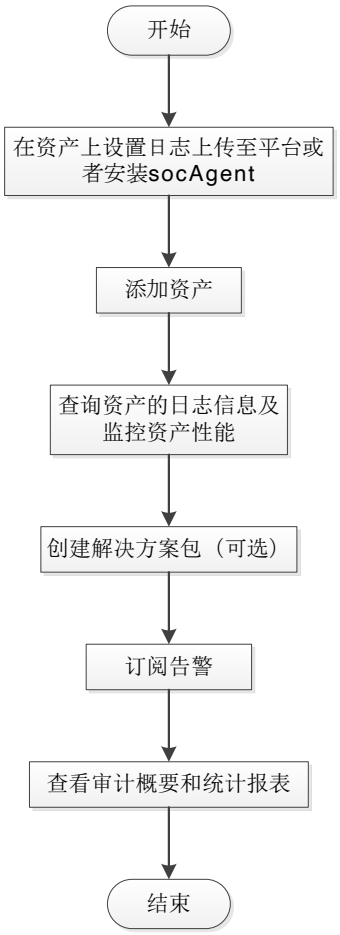
步骤2.　输入默认用户名和密码，点击<**登录**>进入系统 Web 管理平台首页。

如检测到当前用户在其它地方登录，可进行如下操作：

- 点击<**全部关闭**>，在其它地方使用当前用户名登录的会话将全部退出。
- 点击<**忽略**>，不影响任何会话。
- 在列表中点击<**关闭**>，可关闭对应 IP 地址登录用户的会话，但不影响其他会话。

1.5 主要业务流程

平台主要业务流程如下图所示。



步骤1. 在资产上设置日志上传至平台或者安装 socAgent 在资产上设置 Syslog 等协议将日志发送至平台，或者在资产上安装 socAgent，通过 socAgent 将日志发送至平台。

步骤2. 添加资产：平台可自动发现通过 Syslog 等协议向平台发送日志的资产以及通过 socAgent 向平台发送日志的资产，发现这些资产后，需要添加这些资产。详情请参见 3.2.2 发现资产。

步骤3. 查询资产的日志信息及监控资产性能：在事件管理模块中可查询资产的日志信息，在性能监控模块中监控资产的性能状态。详情请参见 4.1 自定义查询 和错误!未找到引用源。错误!未找到引用源。。

步骤4. 创建解决方案包：该操作为可选操作，平台已经内置了 2 个解决方案包。用户可根据需要创建解决方案包，解决方案包是一系列安全事件模板的集合，平台根据这些模板分析资产的风险趋势，对于威胁事件给予告警。

步骤5. 订阅告警：管理员可订阅自己关注的告警事件，可第一时间了解资产的威胁态势

步骤6. 查看审计概要和统计报表：平台会根据解决方案包对日志事件进行审计并对威胁趋势做出统计。

2. Web 配置页面简介

DAS-Logger 的 Web 配置页面包含三个部分：1.上边栏；2.菜单栏；3.操作区。

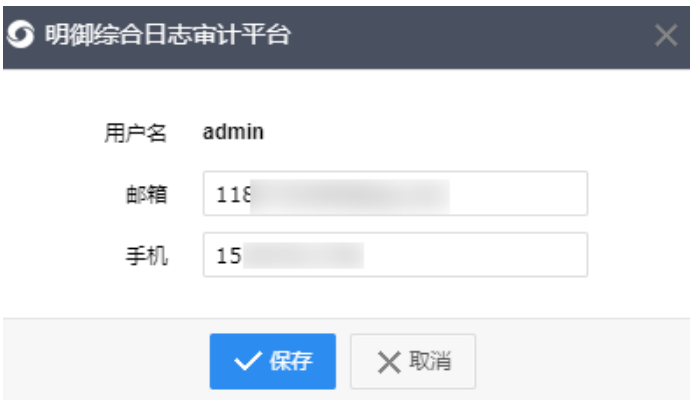
2.1 告警通知

在上边栏点击  图标可查看告警通知信息。点击告警通知后的数字跳转到告警消息页面查看详情，更多信息请参考 4.3.1 告警消息。

2.2 修改用户信息

步骤1. 在上边栏点击用户名，选择<**用户信息**>。

步骤2. 进入用户信息页面后，修改用户邮箱和手机号，点击<**保存**>。



2.3 修改用户密码

步骤1. 在上边栏点击用户名，选择<**密码修改**>。

步骤2. 在弹出的对话框中输入旧密码，再输入新密码并确认新密码，点击<**保存**>。

密码长度要求为 8~16 个字符，必须包含：大写字母、小写字母、数字和特殊字符。

2.4 查看系统时间

在上边栏点击用户名，选择<**系统时间**>，可查看系统时间。如需修改系统时间，请参见错误!未找到引用源。错误!未找到引用源。。

2.5 设置首选包

在上边栏点击用户名，选择<**首选包**>，在弹出的对话框中选择首选包，点击<**保存**>，即可设置在**审计概要**中默认显示的解决方案包。有关解决方案包的更多信息 ,请参考错误!未找到引用源。错误!未找到引用源。。

2.6 查看平台版本信息

在上边栏点击用户名，选择<**版本信息**>，即可查看平台的版本信息。

首页

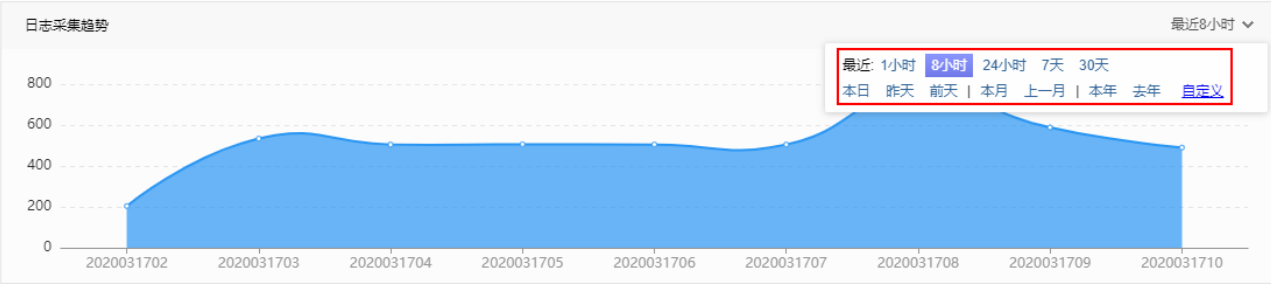
首页是用户登录平台后默认进入的界面。首页展示了系统的状态信息、资源使用信息以及安全事件等信息。包括数据概要和分析场景。

2.7 数据概要

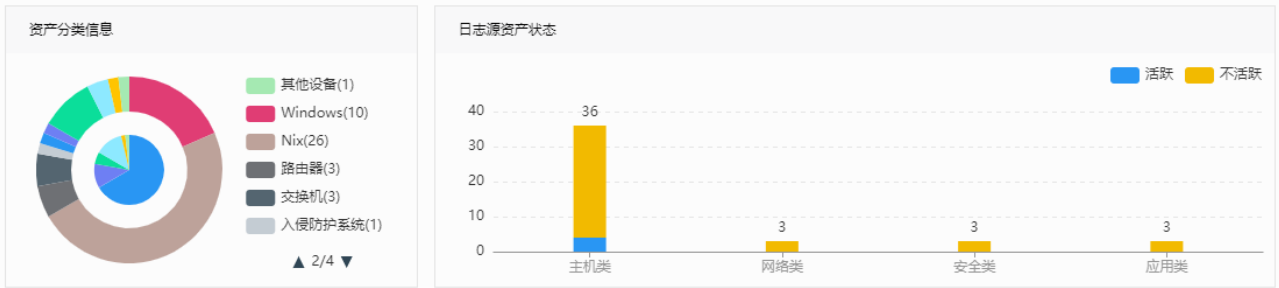
用户登录平台后默认进入首页的**数据概要**页面。

可查看日志源资产数、日志接收总数、日志存储占用空间和系统状况。

可查看相应时间段内的日志采集趋势图。



可查看资产分类信息和日志源资产状态信息。



可查看最近十分钟内最新的 10 条事件（点击<**配置**>，勾选过滤条件展示指定等级的事件）。

2.8 分析场景

在左侧菜单栏选择“**系统概况➢分析场景**”，可查看攻击场景、安全事件、设备状况信息，此外，可选择需要关注的场景。

3. 资产管理

资产管理是对向平台发送日志的设备或系统进行管理。

3.1 组织架构管理

资产隶属于某个组织，因此在添加资产前必须添加组织架构。

3.1.1 创建组织

可通过手动添加或者批量导入两种方法创建组织。

◆ 手动添加

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤组织架构**”进入**资产组织架构管理**页面。

步骤2. 在组织架构节点导航栏中选择某个组织，点击<**新增下级**>可新增下级机构，点击<**新增同级**>可新增同级机构。

步骤3. 在弹出的对话框中，输入名称，点击<**确定**>，即可增加下级机构或同级机构。

◆ 批量导入

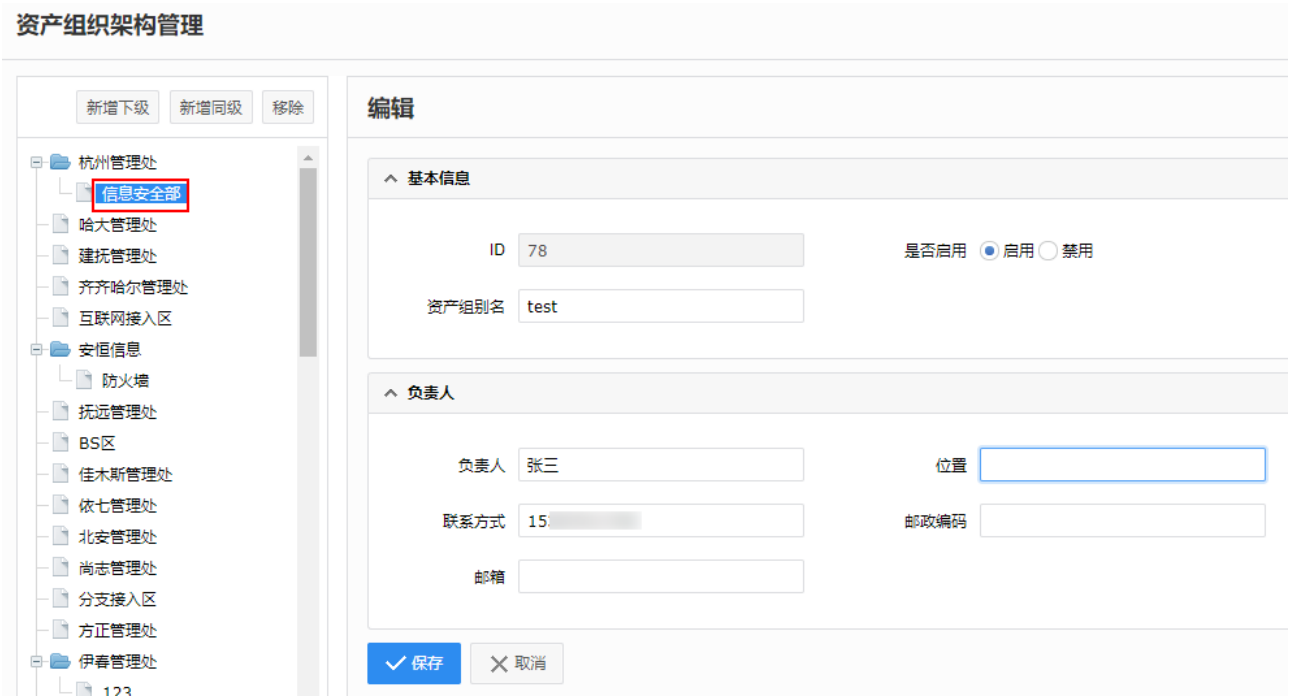
步骤1. 在**资产组织架构管理**页面，点击右上角的<**导入**>。

步骤2. 在弹出的对话框中点击<**选择文件**>，选择要导入的文件（文件格式为 xml），点击<**导入**>。

3.1.2 编辑组织信息

创建组织后，可编辑组织信息，操作方法如下：

选择组织（如“信息安全部”），选择是否启用资产，编辑资产组别名、负责人、联系方式、邮箱等信息，点击<**保存**>。



3.1.3 删除组织

选择要删除的组织，点击<**移除**>，在弹出的对话框中点击<**确定**>，即可删除该组织。

当组织下面有资产时，需要先删除组织下的资产后才能删除该组织。

3.2 资产管理

3.2.1 添加资产

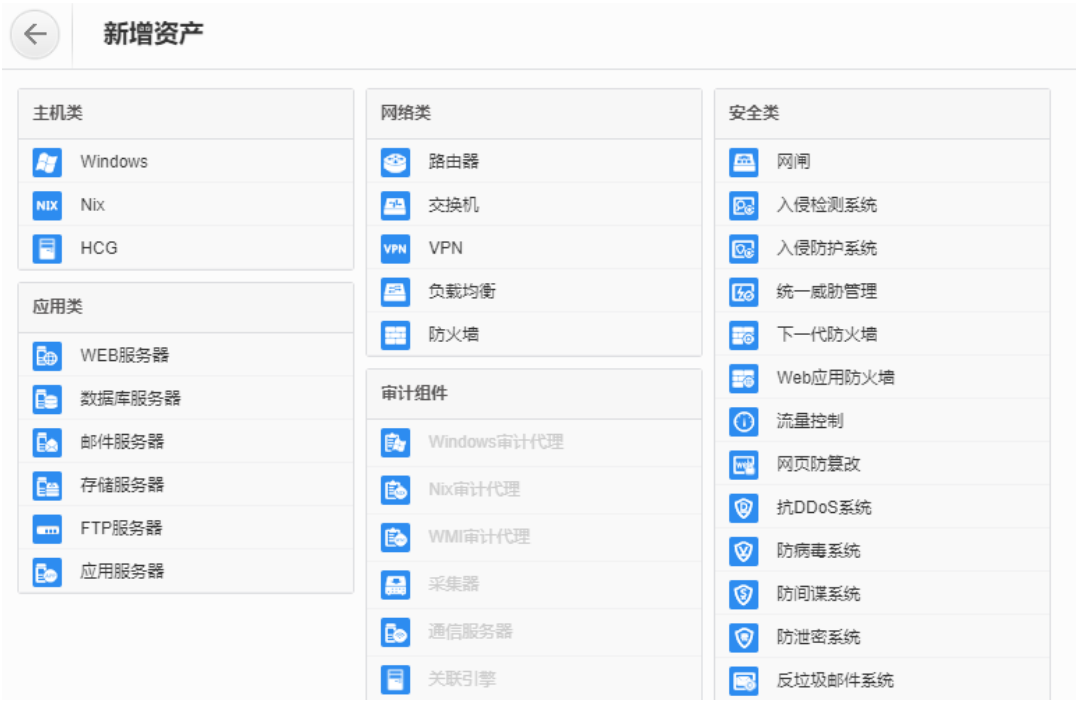
添加资产有两种方式：手动添加资产和对平台自动发现的资产进行确认。

手动添加资产包括单个添加和批量导入两种方式：

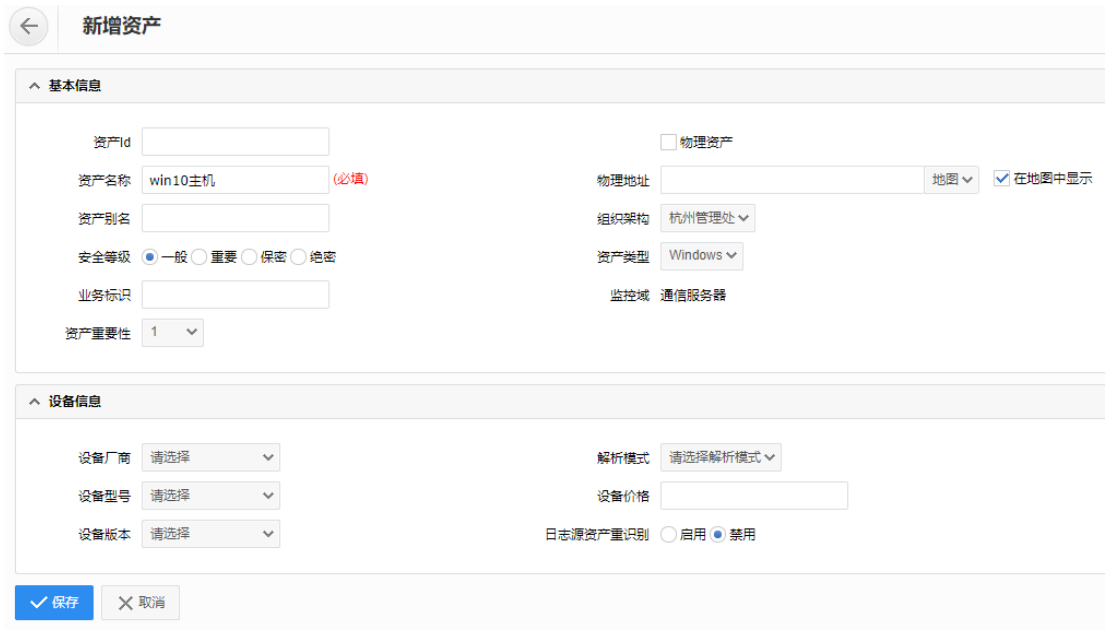
- 单个添加

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤全部资产**”进入**资产**页面。

步骤2. 点击<**新增**>进入**新增资产**页面，选择资产类型（如<**Windows**>）。



步骤3.　编辑相关信息，点击<**保存**>。

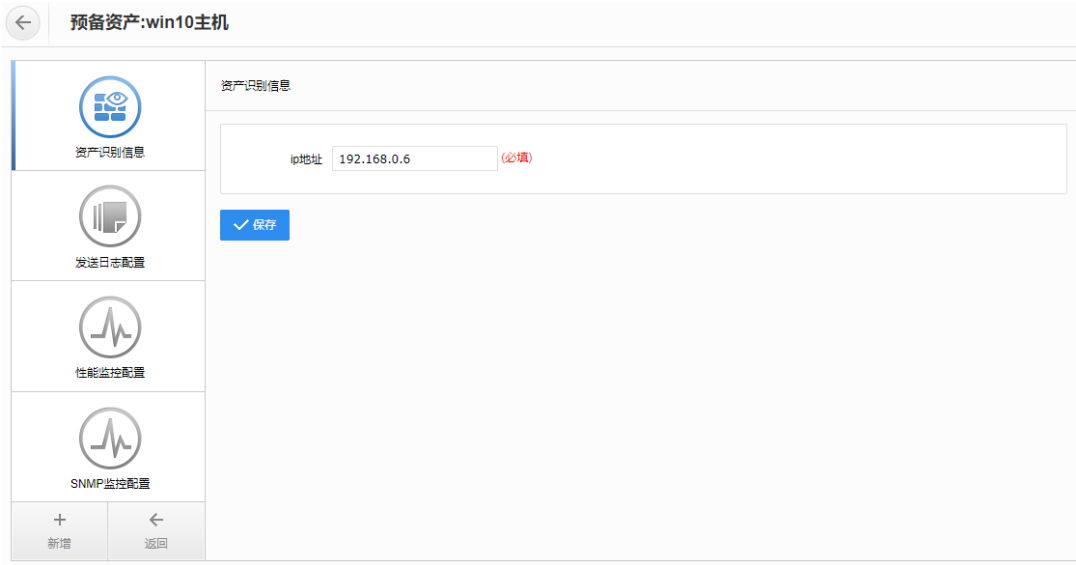


部分配置项说明请参见下表。

配置项	**说明**
基本信息	
资产名称	资产名称，用来标识资产。
组织架构	选择资产隶属的组织。
资产类型	资产类型设置后不可修改。
资产重要性	取值范围 1~10，取值越大越重要。
安全等级	资产的安全等级，包括一般、重要、保密和绝密。
设备信息	
解析模式	◆ 无限制：对资产发送过来的日志不限制指定厂商及设备型号的解析规则。建议使用该模式。

配置项	说明
	◆ 仅限厂商：对资产发送过来的日志只限制指定厂商的解析规则。 ◆ 仅限厂商与型号 :对资产发送过来的日志限制指定厂商及设备型号的解析规则。 ◆ 全部满足：对资产发送过来的日志限制指定厂商、设备型号、设备版本的解析规则，需要全部匹配。
日志源资产重识别	在以下场景下启用日志源资产重识别功能：平台既要监控服务器的系统日志，又要监控服务器上的应用日志，这两部分日志在平台中需要用多个日志资产源来区分开，也就是资产重识别。

步骤4. 设置资产 IP，点击<**保存**>。



步骤5. 配置发送日志配置，点击<**保存**>。

详细配置请参见下表。

配置项	说明
是否启用	◆ 启用：资产向平台发送日志。 ◆ 禁用：资产不向平台发送日志。
日志活跃超时	在指定的时间范围（例如 5 分钟）内没有收到日志，则认为超时。
日志协议	资产向平台发送日志事件所采用的协议类型。由资产本身支持的协议类型决定。
日志编码	资产向平台发送日志事件的编码格式。由资产本身支持的编码格式决定。
过滤等级	资产向平台发送日志事件的日志等级。例如选择过滤等级为“信息”，只发送含信息级别及信息级别以上的日志事件。

◆ 批量导入

步骤1. 在**资产**页面点击右上角的的<**导入**>。

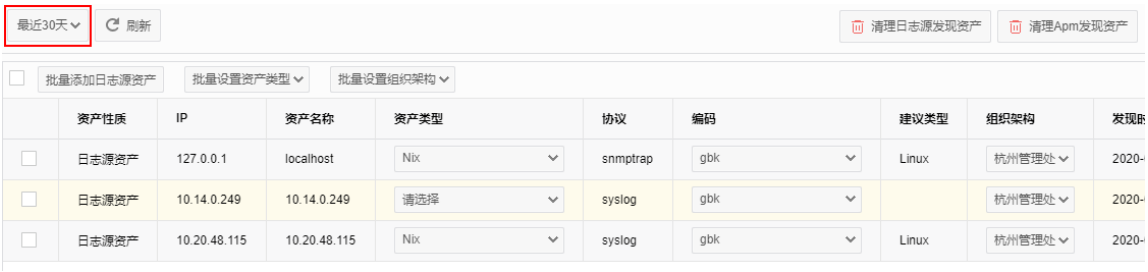
步骤2. 在弹出的对话框中点击<**模板下载**>下载模板文件至本地，编辑模板文件并保存。

步骤3. 点击<**选择文件**>，选择编辑好的模板文件，点击<**导入**>。

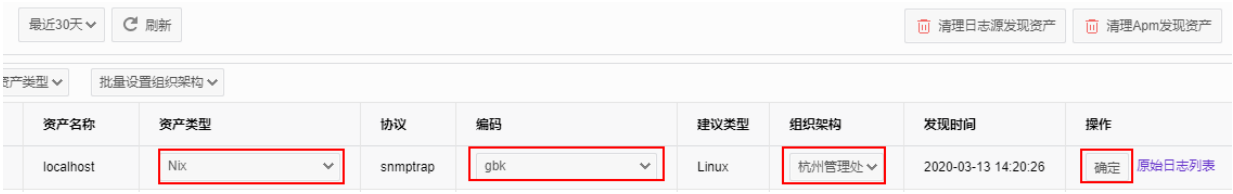
3.2.2 发现资产

平台会自动发现向平台发送日志的资产。对平台自动发现的资产进行确认添加的操作方法如下：

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤发现资产**”，选择时间段，查看平台发现的资产。



步骤2. 在发现资产列表中设置资产类型、编码、组织架构，点击<**确定**>。



- 当设备通过 Syslog、SNMPTrap 等协议以及 socAgent 向平台发送日志时，平台会在发现资产列表中发现一个资产性质为日志源资产的记录。
- 安装 socAgent 并启用了性能监控的设备向平台发送性能监控数据后，平台会在发现资产列表中发现一个资产性质为 Apm 性能监控资产的记录。

点击<**清理日志源发现资产**>，在弹出的对话框中点击<**确定**>，可以删除已发现的日志源资产；点击<**清理**

Apm 发现资产>，在弹出的对话框中点击<**确定**>，可以删除已发现的 Apm 资产。

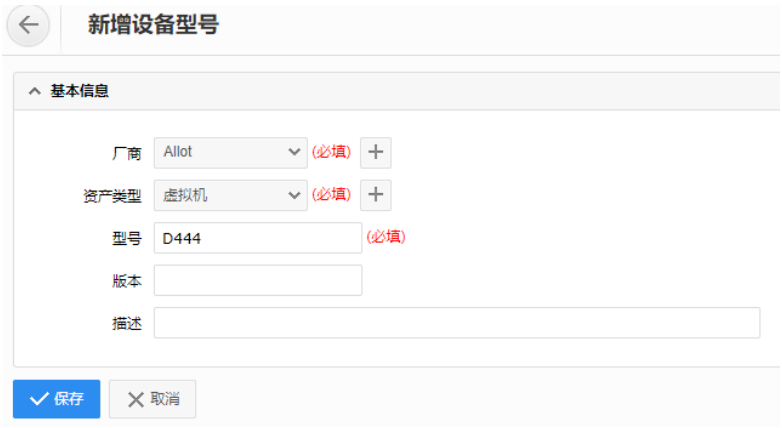
3.2.3 厂商设备型号管理

可对厂商设备型号进行添加、查询和删除操作。

新增厂商设备型号的操作方法如下：

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤厂商设备型号**”进入**厂商设备型号**页面。

步骤2. 点击<**新增**>进入**新增设备型号**页面，选择厂商、资产类型，编辑型号，点击<**保存**>。



3.2.4 查看日志源资产状态

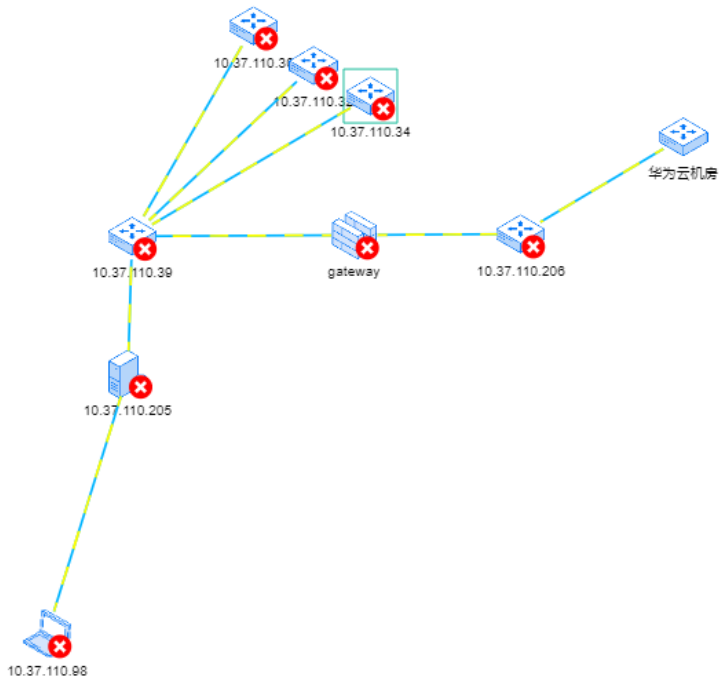
在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤日志源资产状态**”，可查看日志源资产的状态信息（包括发送事件数量及是否活跃等）。

3.2.5 拓扑视图

在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤全部资产**”，点击<**编辑拓扑**>，可编辑资产的网络拓扑图。

通过拓扑视图可查看资产的组网分布。操作方法如下：

在上边栏选择**资产管理**，在左侧菜单栏选择“**资产➤拓扑视图**”即可查看资产的拓扑图。



3.3 分类视图

分类视图是指从不同的维度查看资产，包括发送日志的资产、被监控的资产和审计组件三个维度。

3.3.1 发送日志的资产

在上边栏选择**资产管理**，在左侧菜单栏选择“**分类视图➤发送日志的资产**”，可以查看向平台发送日志的资产。点击列表中的资产条目对选中资产进行编辑。


发送日志的资产列表

资产名称	资产类型	ip地址
win10主机	Windows	192.168.0.6
测试用主机	Windows	192.168.0.3
10.14.0.85	交换机	10.14.0.85
ffff	Windows	ff:0:0:0:0:0:0:ff
192.168.1.17	Windows	192.168.1.17
10.14.0.84	Nix	10.14.0.84
zyyhips	入侵防护系统	192.168.199.199
192.168.33.75	Nix	192.168.33.75
测试mysql	Nix	12.12.12.31
10.20.48.115	Nix	10.20.48.115

共 46 条　　每页 10 / 1 / 5 页

3.3.2 被监控的资产

在上边栏选择**资产管理**，在左侧菜单栏选择“**分类视图➤被监控的资产**”，可查看被监控的资产。点击列表中的资产条目对选中资产进行编辑。


被监控的资产

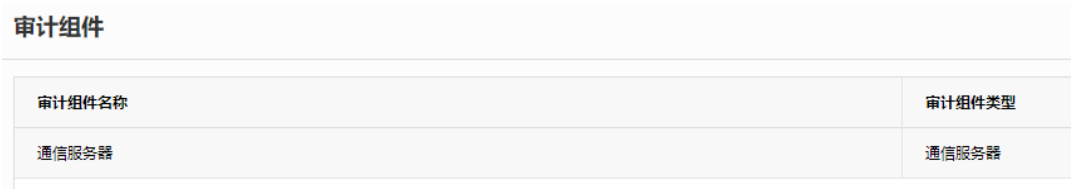
是否监控	资产名称	资产类型	ip地址	端口	操作
监控中 停止监控	10.14.0.28	Windows	10.14.0.28	-	
监控中 停止监控	10.20.176.13	Windows	10.20.176.13	-	

点击<**停止监控**>可停止对资产的监控。

3.3.3 审计组件

在上边栏选择**资产管理**，在左侧菜单栏选择“**分类视图➤审计组件**”，可查看审计组件。点击列表中的资产

条目对选中资产进行编辑。

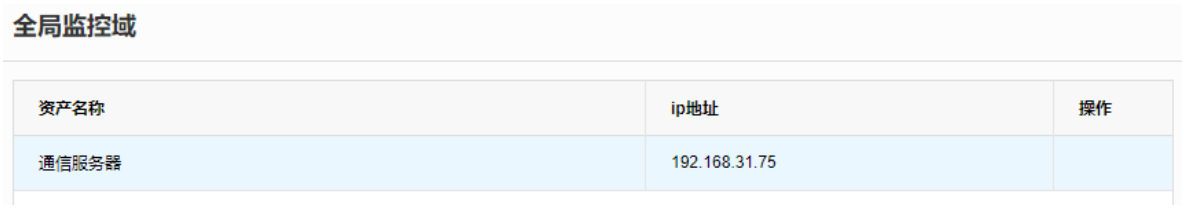


3.4 监控域视图

监控域是指针对类型为采集器、通信服务器、关联引擎的资产分类进行监控，不同类型归属于不同监控域。

3.4.1 全局监控域

在上边栏选择**资产管理**，在左侧菜单栏选择“**监控域视图➤全局监控**”，可查看全局监控域资产。点击列表中的资产条目对选中资产进行编辑。



3.4.2 通信服务器

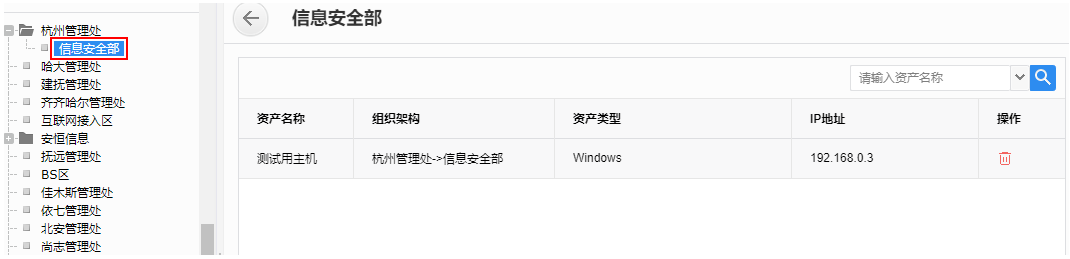
在上边栏选择**资产管理**，在左侧菜单栏选择“**监控域视图➤通信服务器**”，可查看通信服务器资产。点击列表中的资产条目对选中资产进行编辑。

3.5 组织架构视图

可查看各组织下的资产分布情况。操作方法如下：

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择**组织架构视图。**

步骤2. 在组织架构导航栏中选择某个组织，即可查看该组织下的资产。



3.6 网络视图

通过网络视图可查看某一网段下的资产。操作方法如下：

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择**网络视图。**

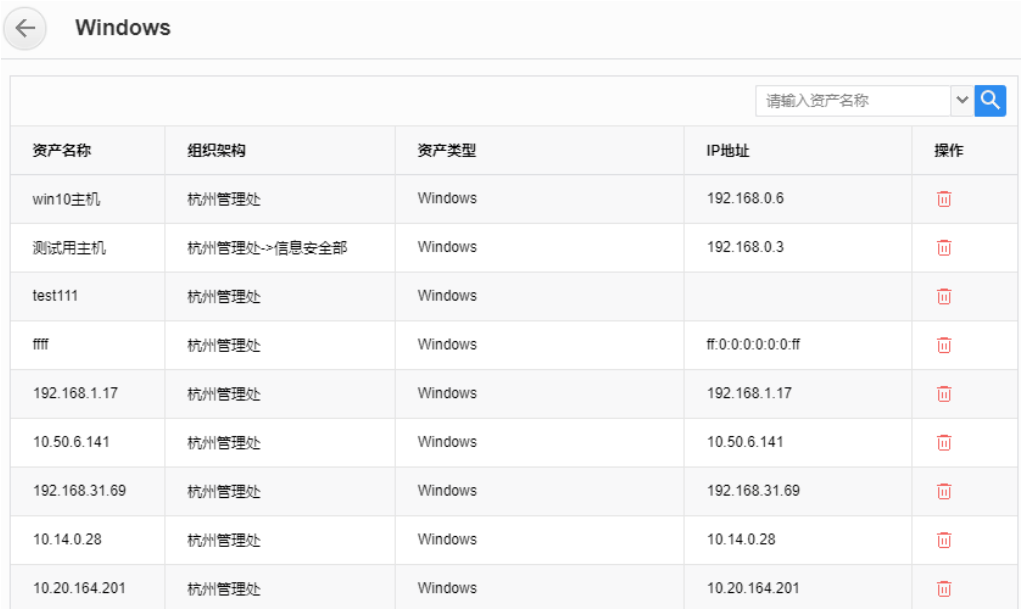
步骤2. 选择网段，即可查看该网段下的资产。点击列表中的资产条目对选中资产进行编辑。

3.7 资产类型视图

通过资产类型视图可查看不同资产类型下的资产分布情况。操作方法如下：

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择“**其他视图➤资产类型视图**”。

步骤2. 选择资产类型（如 Windows），即可查看该资产类型下的资产。点击列表中的资产条目对选中资产进行编辑。



资产名称	组织架构	资产类型	IP地址	操作
win10主机	杭州管理处	Windows	192.168.0.6	
测试用主机	杭州管理处->信息安全部	Windows	192.168.0.3	
test111	杭州管理处	Windows		
ffff	杭州管理处	Windows	ff:0:0:0:0:0:0:ff	
192.168.1.17	杭州管理处	Windows	192.168.1.17	
10.50.6.141	杭州管理处	Windows	10.50.6.141	
192.168.31.69	杭州管理处	Windows	192.168.31.69	
10.14.0.28	杭州管理处	Windows	10.14.0.28	
10.20.164.201	杭州管理处	Windows	10.20.164.201	

3.8 地图视图

通过地图的视角直观展示资产的分布情况。操作方法如下：

在上边栏选择**资产管理**，在左侧菜单栏选择**地图视图**，即可查看资产的地域分布情况。将光标悬停至位置

图标上，会显示资产名称。

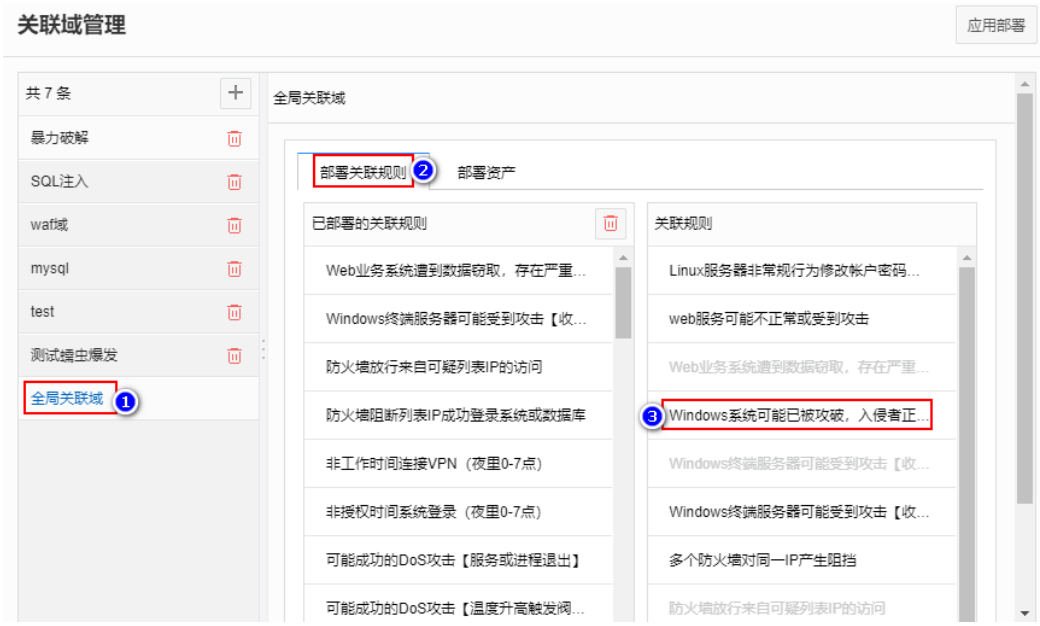
3.9 关联域管理

关联域管理是指将资产与规则进行关联的管理功能。

全局关联域设置的关联规则适用于所有的日志源资产。操作方法如下：

步骤1. 在上边栏选择**资产管理**，在左侧菜单栏选择“**资产域管理➤关联域管理**”进入**关联域管理**页面。

步骤2. 点击<**全局关联域>，**选择**部署关联规则**页签，在<**关联规则**>列表框中点击关联规则，将该关联规则添加至<**已部署的关联规则**>列表框中。在< **已部署的关联规则**>列表框中点击已部署的关联规则，解除选中的关联规则，或点击列表框右上角的图标解除全部已部署的关联规则。

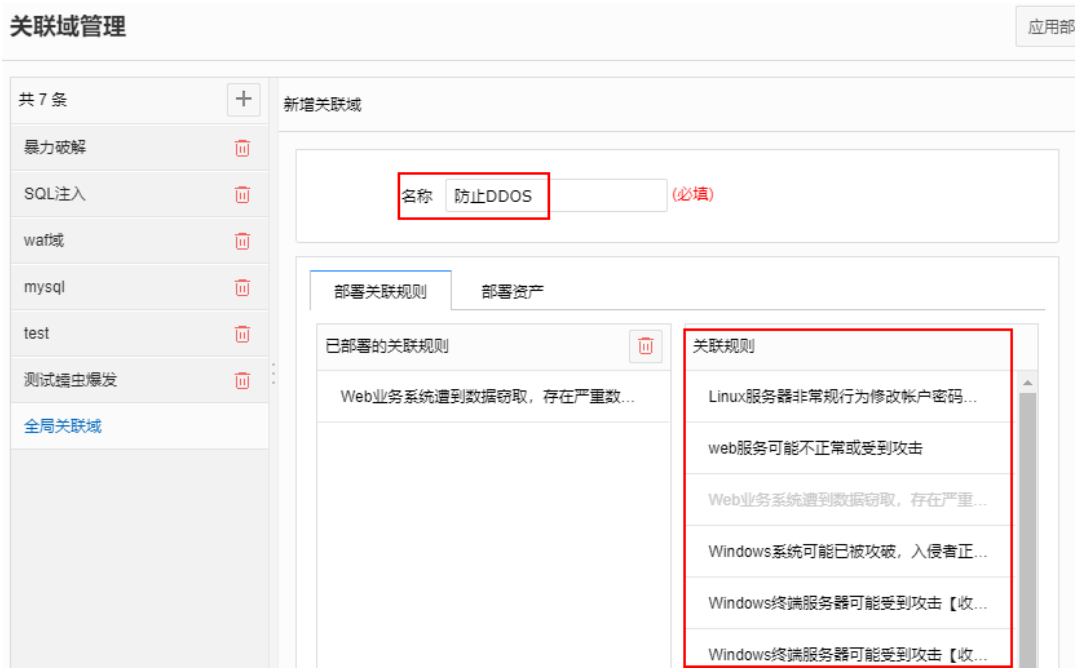


步骤3. 点击<**保存**>。

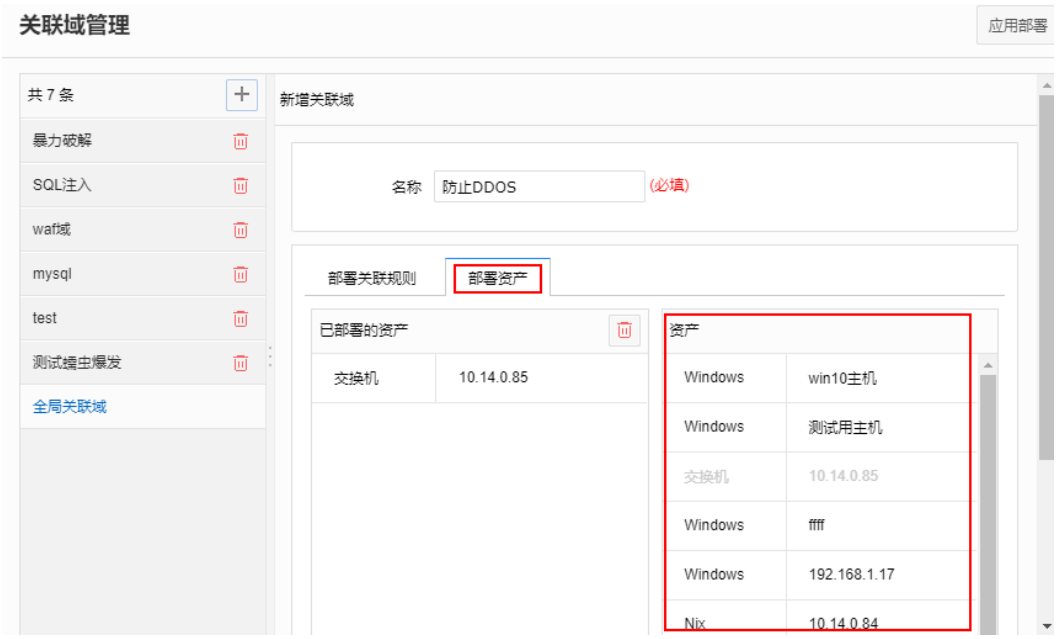
新增关联域的操作方法如下：

步骤1. 在**关联域管理**页面点击  图标。

步骤2. 进入**新增关联域**页面，编辑名称，在<**关联规则**>列表框中点击关联规则，将关联规添加至<**已部署的关联规则**>列表框。在<**已部署的关联规则**>列表框中点击已部署的关联规则，解除选中的关联规则，或点击列表框右上角的图标解除全部已部署的关联规则。



步骤3. 选择**部署资产**页签，在<**资产**>列表框中点击资产，将资产添加至<**已部署的资产**>列表框中。在 <**已部署的资产**>列表框中点击已部署的资产，解除选中的资产，或点击列表框右上角图标解除全部已部署的资产。



步骤4. 点击<**保存**>。

4. 事件管理

事件管理是针对日志审计事件，进行自定义查询和定义查询模板的功能模块。

4.1 自定义查询

4.1.1 查询条件

在上边栏选择**事件管理**，在左侧菜单栏选择“**事件➤自定义查询**”进入**自定义查询**页面。设置查询条件，点击<**查询**>即可查询事件，点击<**清空**>可以清空查询条件。

以下对查询条件进行详细说明。

4.1.1.1 关键字

关键字查询索引字段包含客户 ID、资产 ID、客户管理帐号 ID、事件级别、事件类型、事件名称、原始日志、效果信息描述、应用协议信息、源地址、源端口、目标地址。

关键字查询支持模糊查询。例如通过“Deny udp”关键字查询，只要事件中存在 Deny 及 udp 两个单词就可以将事件查询出来。

4.1.1.2 威胁等级

威胁等级的详细说明请参见下表。

威胁等级分类	威胁等级图标	说明
低等级	   	和安全有一定关系，需要管理员进行一定的关注，但是可以忽略的日志。
中等级	  	潜在的攻击（不确定有没有实际危害、攻击不成功、失效、不确定是否攻击）。
高等级	   	对系统已造成危害。

4.1.1.3 事件类型

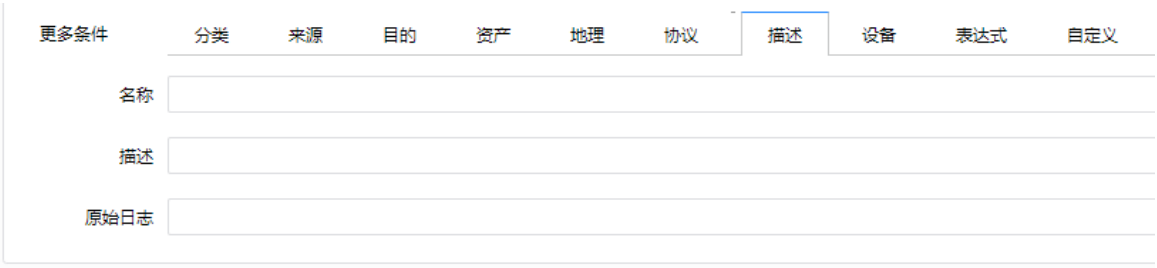
关于事件类型的详细说明请参见下表。

事件类型	说明
基本事件	设备发送过来经过分析后的事件。
聚合事件	通过算法把存在着重复和并发关系的事件合并为一条事件。
关联事件	通过综合分析各种网络告警信息产生新的安全告警事件。
三维关联事件	发送事件的资产存在弱点并且与知识库中的弱点相对应将产生一条三维关联事件。
原始事件	解析规则暂不支持的事件。

内部事件	平台自身内部的事件，即通信服务器的日志事件。

4.1.1.4 更多条件

点击<**更多条件**>，展示更多查询条件，如下图所示。



对于<**描述**>和<**设备**>参数说明请参见下表。

条件	**参数**	**说明**
描述	名称	即事件详情中的事件名称。
	描述	即事件详情中的事件描述。
	原始日志	即事件详情中的原始事件。
设备	处理动作	与事件相关联的一些设备的处理动作，如 accept、deny 等。
	危险级别	发送日志设备特定评估的事件严重程度。
	报文	发送设备获取到的报文内容。
	域名	与事件相关的设备的特定域。
	源端口	与事件相关联的流量入接口。
	目标端口	与事件相关联的流量出接口。
	分类	发送事件设备对事件的分类，如：管理事件、安全事件、系统事件等(现解析规则中大部分未使用此字段)。

条件	参数	说明
	分类 ID	发送事件设备对事件的分类 ID，如：管理事件为 01、安全事件为 02、系统事件为 03 等(现解析规则中大部分未使用此字段)。

界面查询条件涵盖事件解析的基本参数条件，如果仍不满足查询要求，用户也可以进行自定义条件查询。

- 点击+图标，可以新增自定义查询条件。
- 点击−图标，可以删除自定义查询条件。

自定义条件查询格式：例如查询行为结果为成功的事件，则前一个对话框输入字段名参数：catOutcome，后一个对话框输入字段查询值：OK。更多查询条件字段请参见下表。

字段名参数	字段名	参考查询值	说明
fileName	文件名称	system	指事件相关文件名称
restartTure	重启标记	true	系统重启则 restartTrue=true
loginOutTrue	登出标记	true	登出、注销操作
virusBaseVerion	病毒库版本	-	指事件相关病毒库版本号
sqlAction	数据库操作字段	-	指数据库 SQL 操作动作
accountLocked	用户锁定标记	true	用户被锁定则 accountLocked=true
originator	攻击源标记	true	如果 IP 为攻击源，则定义 originator=true

4.1.2 查询结果

设置查询条件后，点击<**查询**>，即可得到查询结果，如下图所示。

	事件级别	事件名称	组织架构	源地址	源端口	目标地址	目标端口	事件数量	资产名称	采集器接收时间
		{"eventCount":1,"eventId":535063	伊春管理处					1	192.168.27.40	11:14:21 2020-03-18
	1	cron 进程信息：执行cron任务	伊春管理处			192.168.31.101		1	192.168.31.101	11:13:36 2020-03-18
	1	cron 进程信息：执行cron任务	伊春管理处			192.168.31.101		1	192.168.31.101	11:13:36 2020-03-18
	1	cron 进程信息：执行cron任务	伊春管理处			192.168.31.101		1	192.168.31.101	11:13:36 2020-03-18
	1	会话已开始	伊春管理处			192.168.31.101		1	192.168.31.101	11:13:36 2020-03-18
	1	会话已开始	伊春管理处			192.168.31.101		1	192.168.31.101	11:13:36 2020-03-18
	1	会话已开始	伊春管理处			192.168.31.101		1	192.168.31.101	11:13:36 2020-03-18
		{"eventCount":1,"eventId":535063	伊春管理处					1	192.168.27.40	11:13:21 2020-03-18

在查询结果中点击事件名称即可进入事件详情页面。不同类型事件的展示页面有所区别。各类型的事件均包含以下信息：时间信息、基本信息、来源信息、目标信息、事件分类信息、设备信息。

4.1.2.1 基本事件详情

基本事件详情界面如下图所示。

4.1.2.2 关联事件详情

关联事件详情与基本事件相比，多了<**关联事件**>，所下图所示。

点击<**关联事件**>可以查看产生关联事件的原始事件列表。在列表中点击事件，即可查看原始事件详情。

4.1.2.3 三维关联事件

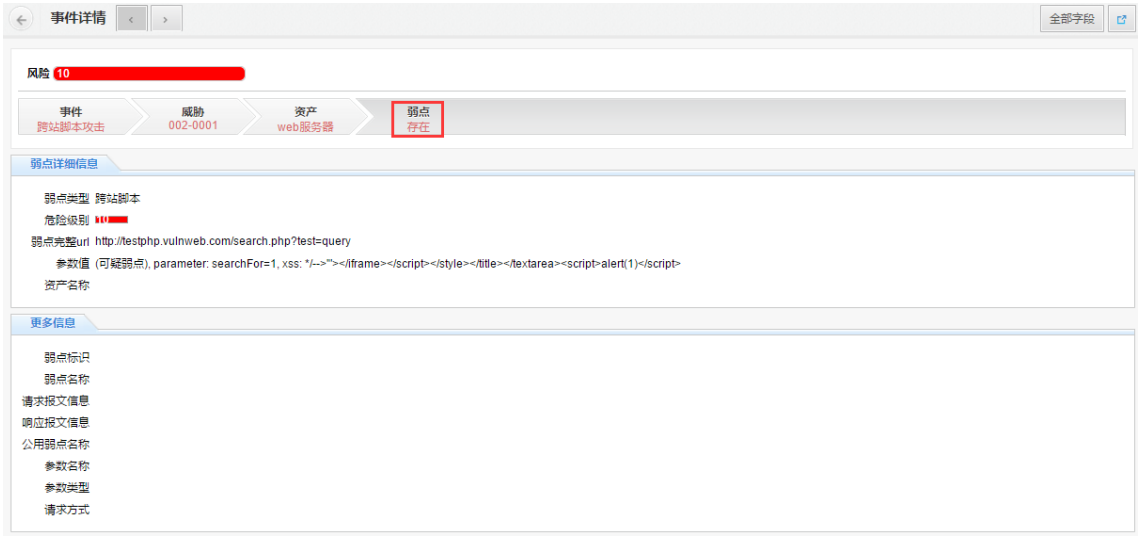
三维关联通过资产、安全知识库、弱点库三个维度进行分析事件是否存在威胁。在基本事件的信息的基础上，增加了三维关联指示图，如下图所示。

点击<**事件**>，查看事件的基本详细信息。

点击<**威胁**>，显示该事件收到的威胁的详细信息，包括漏洞编号、漏洞名称、漏洞的详细描述、漏洞的类型以及漏洞的解决方案，如下图。

点击<**资产**>，显示该事件对应资产的详细信息，如下图所示。

点击<**弱点**>，显示该资产对应的扫描结果中对应的弱点信息。内容包括弱点类型、危险级别、弱点类型URL、参数值、资产名称等信息，如下图。弱点主要通过将扫描器手动导入或者通过扫描器授权连接在线导入。弱点导入详请请参见[错误!未找到引用源。错误!未找到引用源。]。



4.1.2.4 事件回放

在自定义查询结果页面，点击右上角的<**回放**>，进入事件回放页面，页面会逐条显示当前查询结果中的事件，如下图所示。

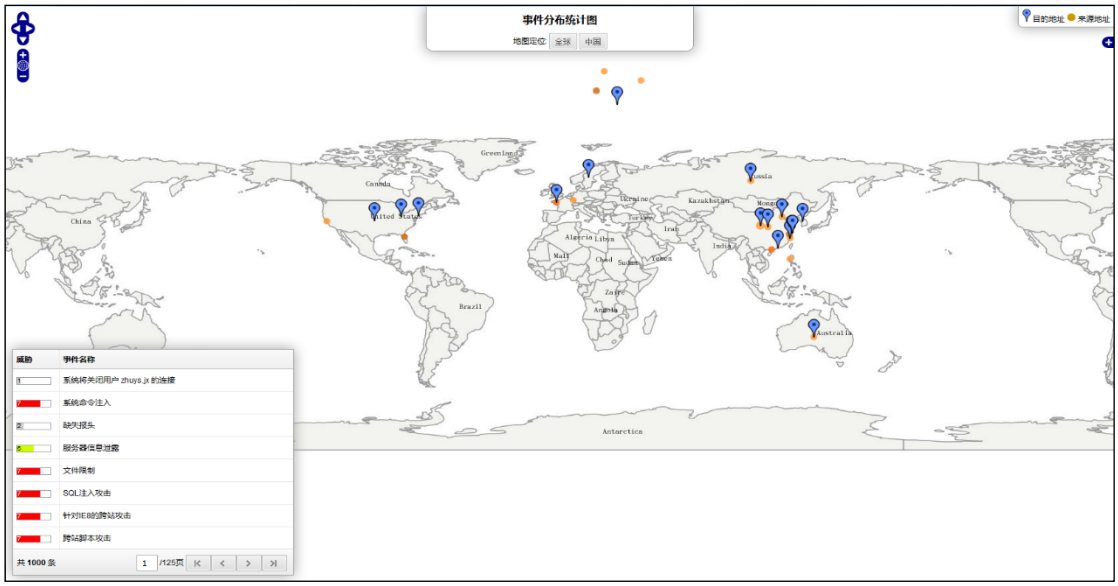
4.1.2.5 保存事件查询

在自定义查询结果页面，点击右上角的<**另存为**>，在弹出的对话框中选择解决方案包、上级目录名称，编辑已保存查询名称，点击<**保存**>。

保存成功后，该查询结果将会添加至<**已保存查询**>列表中。

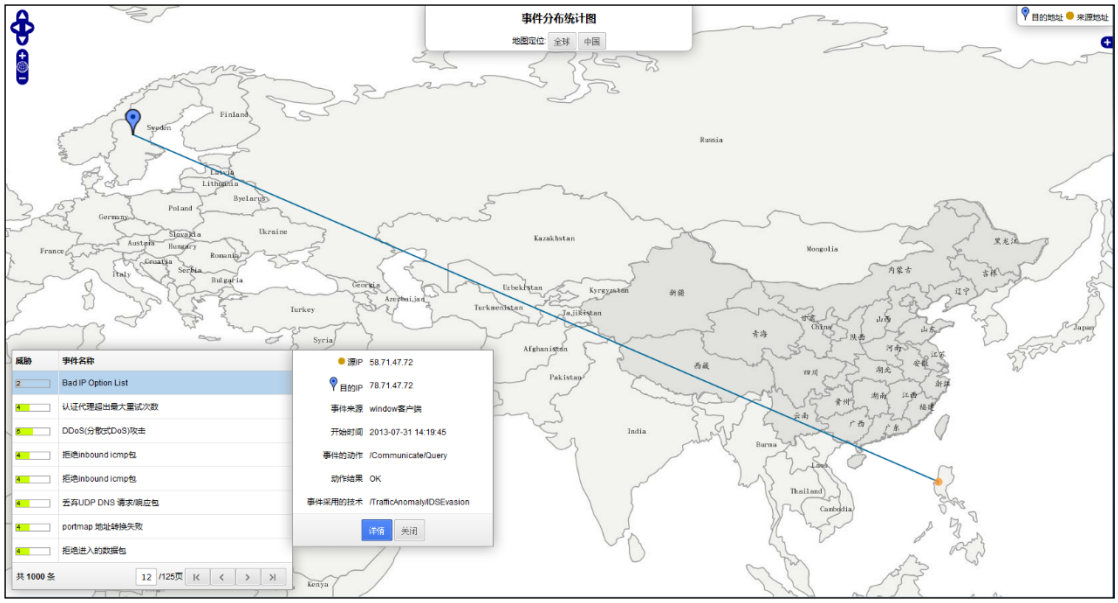
4.1.2.6 在地图中查看事件

在自定义查询结果页面，点击右上角的<**在地图中查看**>，进入如下页面。



事件分布统计图，在地图上显示世界各地近期事件的分布情况， 为目标地址， 为来源地址。点击<**中国**>，将地图定位到中国的区域，展示中国地区事件的情况。

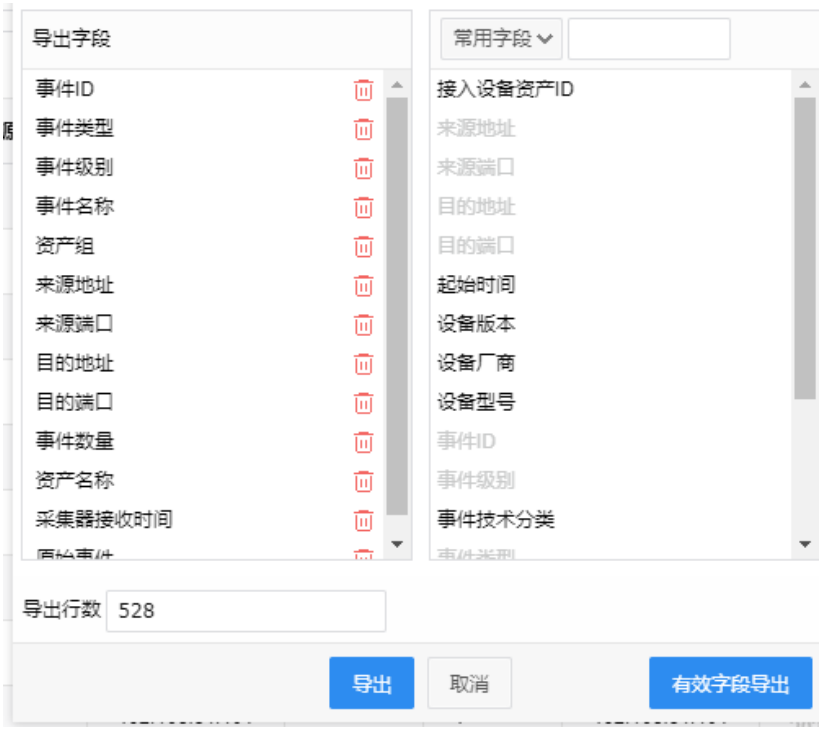
在页面左下角的事件列表中点击某条事件，在地图上显示对应的行为操作。



点击<**详细**>，可以查看该事件的详细内容。

4.1.2.7 **导出事件**

在自定义查询结果页面，点击右上角的<**导出**>，在弹出的对话框中点击<**常用字段**>列表框中的字段，将其设置为<**导出字段**>，点击<**导出**>将事件字段信息导出至本地。



4.2 已保存查询

已保存的查询保存了之前设置的查询条件及查询结果，作为查询模板，方便查询符合条件的事件。

操作方法如下：

在上边栏选择**事件管理**，在左侧菜单栏选择**已保存查询**，在已保存查询导航栏中选择已保存查询名称。可查询符合该已保存查询名称对应查询条件的事件。

4.3 告警

4.3.1 告警消息

平台的告警消息包括三类：自定义告警、订阅告警和系统告警（平台本身的告警，例如：磁盘空间告警、性能监控告警、日志源资产状态告警、FTP 远程仓库状态告警等）。

在上边栏选择**事件管理**，在左侧菜单栏选择“**告警➤告警消息**”可查看各类告警消息（本文以订阅告警举例说明）。

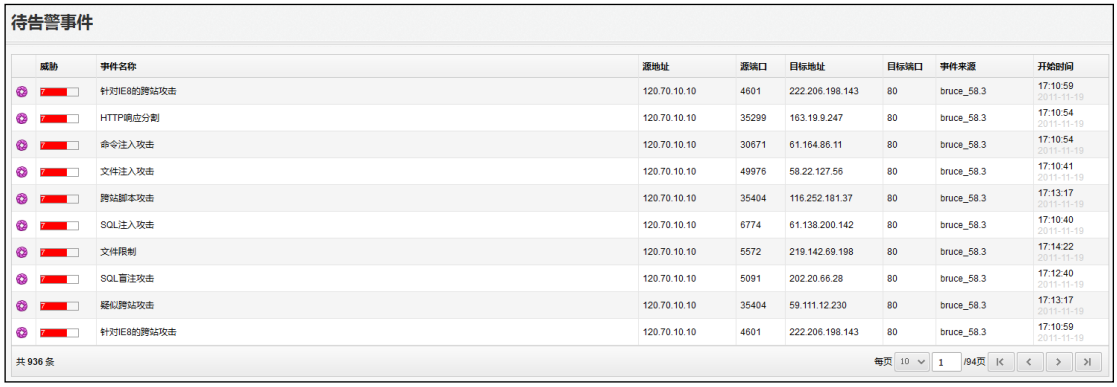
点击<**查询**>，在弹出的对话框中选择接收者、发送方式，点击<**过滤**>，则会显示符合过滤条件的告警消息。

在告警消息列表中点击<**告警消息详情**>，可查看告警消息详情。

4.3.2 待告警事件

待告警事件是指满足告警订阅条件，但是还没有发送出去的事件。查看待告警事件的操作方法如下：

在上边栏选择**事件管理**，在左侧菜单栏选择“**告警➤待告警事件**”，即可查看待告警事件。



4.3.3 外部告警用户

平台可以将告警信息以邮件、短信的方式通知外部用户。新增外部告警用户的操作方法如下：

步骤1. 在上边栏选择**事件管理**，在左侧菜单栏选择“**告警➤外部告警用户**”进入**外部告警用户**页面。

步骤2. 点击<**新增**>进入**新增外部告警用户**页面，编辑名称，邮件和手机号至少填写一个，设置邮件聚合周期、短信聚合周期和 TCP 聚合周期，点击<**保存**>。

详细配置请参见下表。

配置项	说明
邮件聚合周	建议的周期范围：1~120，默认 30 分钟。在一个邮件聚合周期中，平台如果检测到第一个威胁事件会进行邮件报警，后续再检测到威胁事件，如果事件威胁等级比第一个威胁事件等级高，则再次进行邮件报警；如果事件威胁等级比第一个事件威胁等级低，则不立即发送邮件告警。当聚合周期到期后，一次性发送后续的告警信息。

期	
短信聚合周期	取值范围：1~120，默认 10 分钟。短信聚合周期的含义与邮件聚合周期的含义类似。
TCP 聚合周期	取值范围：1~120，默认 10 分钟。TCP 聚合周期的含义与邮件聚合周期的含义类似。

4.3.4 告警订阅

系统管理员可以订阅日志事件告警和系统事件告警。

4.3.4.1 日志事件订阅

日志事件订阅是指订阅解决方案包中相应事件的告警通知。操作方法如下：

在上边栏选择**事件管理**，在左侧菜单栏选择“**告警➢告警订阅**”，选择**未订阅**页签，在左侧解决方案包导航栏中选择事件（如“防火墙阻断”），选择邮件订阅、短信订阅、FTP 订阅和 TCP 订阅的用户，点击<**保存**>。

详细配置请参见下表。

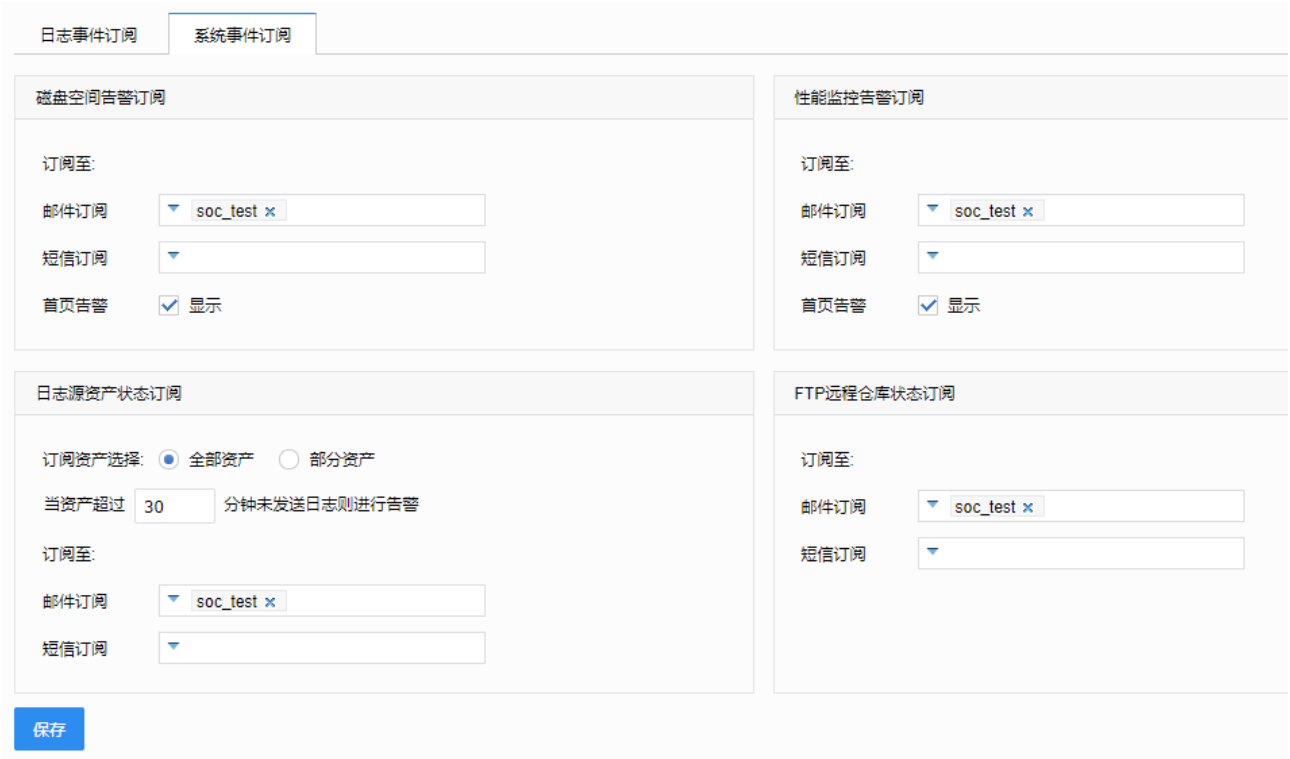
配置项	说明
邮件订阅	选择通过邮件接收日志事件告警信息的用户。
短信订阅	选择通过短信接收日志事件告警信息的用户。
FTP 订阅	选择通过 FTP 方式接收日志事件告警信息的用户。
TCP 订阅	选择通过 TCP 方式接收日志事件告警信息的用户。

上述订阅方式的更多信息，请参考 4.3.3 外部告警用户。

4.3.4.2 系统事件订阅

系统事件主要是指平台的状态不正常，例如磁盘空间不足、较长时间未收到资产的日志等。系统事件订阅的操作方法如下：

在告警订阅页面选择**系统事件订阅**页签，设置各类型系统事件告警通知的接收人，点击<**保存**>。



详细配置请参见下表。

配置项	**说明**
磁盘空间告警订阅	选择磁盘空间告警的接收人，包括邮件订阅和短信订阅。
性能监控告警订阅	选择性能监控告警的接收人，包括邮件订阅和短信订阅。
日志源资产状态订阅	资产在指定时间（取值范围：1~120，单位为分钟，默认值 30）内未发送日志则告警。可设置资产的范围，并选择告警接收人，包括邮件订阅和短信订阅。
FTP 远程仓库状态订阅	选择 FTP 远程仓库状态告警的接收人，包括邮件订阅和短信订阅。有关远程仓库配置的更多信息，请参考错误!未找到引用源。错误!未找到引用源。。

4.3.5 自定义告警

系统管理员可自定义告警。操作方法如下：

步骤1. 在上边栏选择**事件管理**，在左侧菜单栏选择“**告警➤自定义告警**”。

步骤2. 点击<**新增**>，在弹出的对话框中编辑相关信息，点击<**保存**>。

详细配置请参见下表。

配置项	**说明**
告警名称	用来标识告警。
告警描述	对告警进行描述。
数据来源	选择解决方案包中的事件。
触发条件	当选择为“单位条数”时，需设置指定时间以及指定时间内时间发生的次数，此外需设置聚合字段。 当选择为“事件范围”时，需要指定时间范围，并选择执行周期。
事件级别	设置事件的威胁等级，取值范围 1~9。等于或者比设置值高的事件都会触发告警。
聚合周期	取值范围：1~120，默认为 10 分钟。在一个聚合周期内当有一个事件触发了告警，后续再有事件触发告警时，若告警事件的级别比第一个事件高时则立即发送告警信息；若告警事件的级别比第一个事件低时，不立即发送告警信息，在聚合周期到期时发送告警信息。

配置项	说明
告警方式	选择“邮件”或“短信”告警方式，并在后面的文本框中输入邮箱地址或手机号码。