京东云
态势感知（专有云）
用户手册

产品版本 v6000

文档版本：20190701

版权声明

信息反馈

http://www.jdcloud.com

第一章　态势感知专有云

1.1 产品介绍

京东云态势感知（专有云）是京东面向政府、金融、制造业、医疗、教育等大型企事业单位推出的一款综合安全运营平台。通过集成网络层、主机层、应用层等安全产品数据源，经过威胁情报、AI 异常检测匹配，大数据关联分析，为企业提供多维度安全告警，可视化大屏呈现。

京东云态势感知（专有云）包含：

1、安全运营平台：捕捉和分析网络安全态势、主机安全态势，对安全事件进行关联还原黑客攻击链，通过安全大屏展示给用户，配合安全运营团队给用户提供托管的服务。

2、网络安全态势：包含应用交付系统、全流量检测系统，抗 DDoS 检测清洗系统， 应用交付系统包括：WAF、四层负载、GTC 智能流量监控与调度、域名解析等组件，方便用户构建自身的安全应用交付体系。全流量检测系统包含：网络入侵检测引擎、威胁情报匹配引擎、机器学习异常检测引擎。抗 DDoS 检测清洗系统包含：检测和清洗引擎。

备注：应用交付系统和抗 DDoS 检测清洗系统由京东云安全其他安全产品承载，需要单独购买。

3、主机安全态势：提供安全体检、风险发现（系统漏洞、账号风险、异常登录、暴力破解、合规基线）、入侵威胁检测（病毒木马、网页木马、系统后门、可疑操作、敏感文件篡改、异常网络连接）、以及调查分析功能，来保护专有云工作负载免受网络攻击。

备注：初始版本提供仅提供系统漏洞、账号风险、异常登录、暴力破解、网页木马等功能，其他功能需要单独购买京东云 EDR 主机安全产品。同时，本版本提供第三方杀毒软件的支持。

4、网络扫描系统：集资产自动关联发现、Web 漏洞扫描、端口漏洞扫描、弱密码检测四大核心功能，发现网站或服务器在网络中的安全风险，为专有云上业务提供多维度的安全检测服务，满足合规要求，让安全弱点无所遁形

5、安全审计：对第三方安全设备数据收集，日志归一化，提供全量日志可视化查询功能，帮助专有云用户安全运营

6、MSSP 托管服务包：提供 7*24 小时在线安全托管服务，服务内容包括：托管安全事件周报，合规报告、应急响应服务。

1.2 系统架构

态势感知私有化版本：通过集成 DDoS 防护引擎、Web 应用防火墙系统、网络入侵检测引擎，主机入侵检测引擎，网络威胁扫描系统，威胁情报&机器学习异常检测匹配引擎等安全探针产生的数据，使用 elastic search 大数据存储查询，使用 spark steaming 关联分析形成的一整套安全数据处理框架，最终通过实时安全大屏把结果呈现给用户，辅助其安全运营与决策。

1、DDoS 防护引擎提供四层、七层流量型攻击告警事件（包括：SYN Flood，ACK Flood，UDP 反射 Flood、UDP Flood、HTTP Flood 等）

2、Web 应用防火墙提供 7 层 web 攻击检测（包括：Web 注入攻击、XSS 攻击、代码/命令执行、文件包含攻击、恶意/后门文件攻击、越权访问等）、CC 攻击告警事件类型等

3、网络入侵检测引擎提供扫描行为监控（包括：主机扫描、应用扫描、应用漏洞攻击）、肉鸡行为行为监控（包括：对外 DDoS、对外暴力破解、对外可疑连接、恶意软件行为等）、异常下载监控（包括：敏感文件下载、备份文件下载、数据库文件下载等）。

4、主机入侵检测引擎提供暴力破解监控（支持 SSH、RDP、MYSQL、FTP 等协议）、网页木马监控（支持 PHP、JSP、ASP 等脚本语言各种类型）、异地登录、系统弱口令检测等告警事件类型。

5、网络威胁扫描系统提供网站、应急漏洞扫描事件告警（包括：弱口令检测（SSH、RDP、REDIS、mogodb、ElasticSearch、mysql、postgresql 等）、web 组件高危漏洞（WebLogic 反序列化漏洞、WordPress 拒绝服务攻击）、Web 通用漏洞（Web 注入攻击、XSS 攻击、代码/命令执行、文件包含攻击、恶意/后门文件攻击、越权访问等））。

6、威胁情报&机器学习异常检测匹配引擎提供失陷主机检测、DGA 域名检测、挖矿检测、HTTP 异常检测等未知威胁告警事件类型。

7、威胁关联分析提供资源滥用攻击、数据窃取攻击、web 定向攻击等 60 多种威胁模型匹配。以 ATT&CK Enterprise 形式展示

8、安全大屏包括：态势感知总览大屏、网络安全态势大屏和主机安全态势大屏

1.3 产品优势

- 日志源

  包括网络层：DDoS 防护产品、网络入侵检测系统、网络威胁扫描系统，主机层面主机入侵检测系统，应用层包括：Web 应用防火墙，同时支持多种第三方安全产品日志接入。

- 大数据架构：

  支持对 PB 级海量数据接入、存储、关联分析、查询，支持分布式部署。

- 威胁情报：

  数据来源：公有云、城市云、手机客户端、商业威胁情报，经过专业团队分析处理，形成准确度高，覆盖面广，实时性强的威胁情报。

- AI 异常检测：

  内置京东企业安全多年积累的数据模型、安全模型和机器学习算法模型，有效识别高级威胁入侵。

第二章　系统登录

用户管理是态势感知系统的基础部件，它为威胁概览、安全大屏、攻击详情、弱点详情等部件提供了身份认证和授权控制。态势感知系统是基于角色的管理模式，使得管理员的权限控制更加细化，使得整个系统处于非常安全的管理环境。

2.1 系统登录

用户在登录系统前应首先部署安全管理系统服务器，安装成功后启动相应的程序，才能通过管理主机登录并对系统进行集中管理。关于安全管理系统的安装请参见十一章系统安装手册。

账户管理员的登录操作为：

1）管理员可以通过 http 或 https 协议以 WEB 访问的方式对京东城市云进行远程管理。在访问时，管理员需要在管理主机的浏览器上输入服务器的管理 URL 加上端口号，例如：https://192.168.0.1 弹出如下的登录页面。

2）输入账户管理员的用户名、密码（默认为 admin/ ZM3lgZf2nfddrhOyqFw2t9jE7c4BwDH5）和验证码。

3）点击“登录”按钮。

登录后，如果本设备已经导入 license，系统会默认展示“威胁概览”，具体的说明请参见。如果是第一次登陆，系统会自动跳转到【系统设置】->【授权管理】页面，拷贝激活码，给授权管理人员发送邮件。例如：

eyJ1dWlkIjoiIiwibm9kZUlkIjoiNEM0QzQ1NDQtMDAzNC00NzEwLTgwNDctQ0FDMDRGMzg1MDMyySjRHRzhQMkRFTEwgSU5DLiIsImVuYWJsZUxiIjpmYWxzZSwiZW5hYmxlV2FmIjpmYWxzZSwiY3VzdG9tZXIiOiIiLCJlbWFpbCI6IiIsImJlZ2luVGltZSI6MCwiZW5kVGltZSI6MH0=

授权管理员，会给你发送一个 license 文件，导入即可。

第三章　威胁概览

提供专有云用户业务安全状态量化指标，以攻击者视角的告警事件、威胁事件，以防御者视角的引擎覆盖率、主机漏洞事件、网站漏洞事件指标与变化。同时提供安全事件 7/30 天发展趋势，以告警、威胁事件聚合统计的 Top10 风险资产，以告警分类、威胁模型聚合统计的 Top10 威胁形态 。

名词解释

- 告警事件

包含网络入侵检测、DDoS 基础防护检测和主机安全检测发现的告警事件，新增威胁情报、动态行为分析、机器学习发现的高价值告警事件。

- 关联分析

通过京东云提供的基于安全威胁模型大数据关联的新型攻击事件，包含实时分析事件、离线分析事件。

功能说明

提供租户业务安全状态量化指标，以攻击者视角的告警事件、威胁事件，以防御者视角的引擎覆盖率、主机漏洞事件、网站漏洞事件指标与变化。同时提供安全事件 7/30 天发展趋势，以告警、威胁事件聚合统计的 Top10 风险资产，以告警分类、威胁模型聚合统计的 Top10 威胁形态 。

同时提供升级企业版入口。

操作步骤

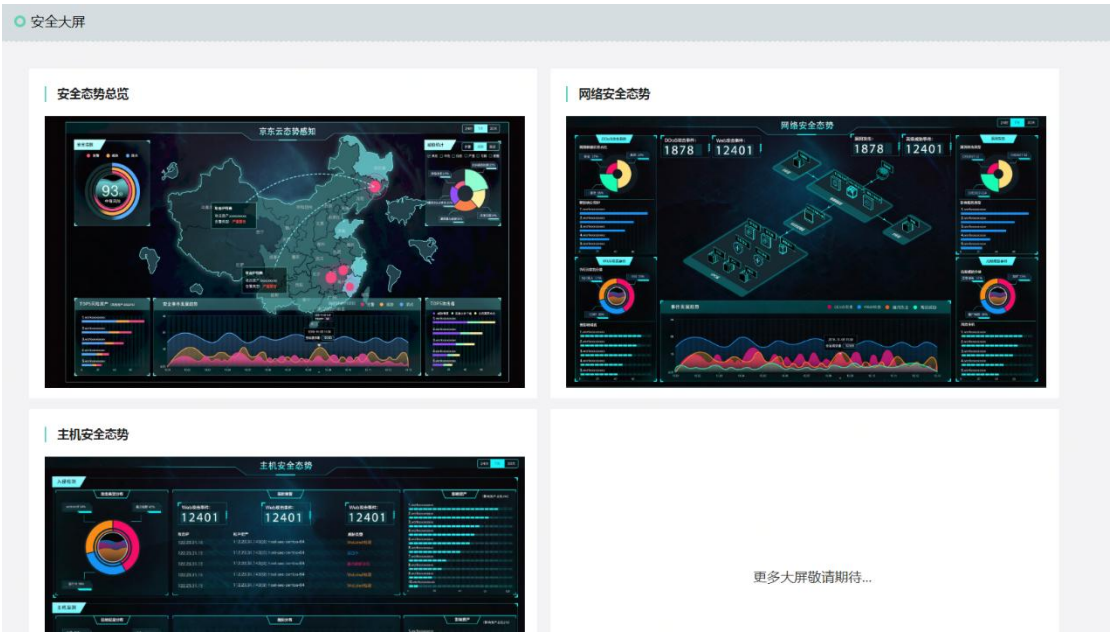
默认进入威胁概览页面，单击攻击者视角的告警事件的数字跳转到【告警事件详情】页面。单击攻击者视角的威胁事件的数字跳转到【威胁事件详情】页面，单击防御者视角引擎覆盖率跳转到【配置变更】->【资产管理】，单击防御者视角主机跳转到【弱点事件】->【主机漏洞】，单击防御者视角主机跳转到【弱点事件】->【网络漏洞】。 *【攻击事件发展趋势】点击 7 天或者 30 天提供，7 天或者 30 天内的告警事件、威胁事件、引擎覆盖率、主机事件、网站漏洞数量趋势，右侧坐标显示百分比，针对安全引擎启动覆盖率显示。鼠标移动到每天后会显示告警事件、威胁事件、引擎覆盖率、主机事件、网站漏洞数量。

*点击 Top10 某个被攻击资产，系统会携带对应的资产 IP 过滤条件跳转到【告警事件详情】页面。统计时长为 7 天或者 30 天根据其实选定的时间状态。

*点击 Top10 某个威胁分类，系统会携带对应的威胁分类过滤条件跳转到【告警事件详情】页面。统计时长为 7 天或者 30 天根据其实选定的时间状态。

第四章　安全大屏

安全大屏，主要是帮助安全运营人员做安全运营决策，本企业领导或者行业用户参观视察以及给用户展示全局安全态势等需求因运而生。现阶段安全大屏包含：态势感知总览、网络安全态势 、主机安全态势



4.1　态势感知总览

态势感知总览大屏主要是从全局的角度告诉安全团队发生了什么安全问题，安全团队需要做什么以及做的怎么样。

态势感知总览大屏包含：安全指标、攻击炮图、Top5 风险资产、Top5 攻击者、安全事件发展趋势、事件统计（告警/威胁/弱点类别分布）、统计状态配置（状态时间|告警级别设置）

安全指标：通过对本账号名下所有云主机的告警、威胁、弱点数量统计，计算出风险值，从而得出安全评级（高/中等/低风险），低风险<=40，中等风险 40<x<=70，高风险 70<x<=100

攻击炮图：可视化显示攻击源、攻击目的、攻击类型，让安全运营人员对攻击有感性的认识。攻击显示【攻击 IP|风险资产|告警类别】

Top5 风险资产：让用户了解最容易遭受攻击的资产，知道运营人员重点关注这些资产和发生的攻击，尽快按照安全建议整改。同时提供影响资产占比。

Top5 攻击者：让用户关注 Top 攻击者，可以通过 ACL、安全组、云 WAF 等阻断这些 IP 高危的访问，完成安全响应。攻击者计算方式：首先以 IP 维度统计。分别从 4 个方面统计：

- 入侵探测（主机扫描、应用扫描、应用漏洞攻击、 遭受暴力破解）
- Web 攻击（Web 注入攻击、XSS 攻击、代码/命令执行、 文件包含攻击、恶意/后门文件攻击、越权访问、敏感文件探测）
- 肉鸡行为（对外 DDoS、对外暴力破解、对外可疑连接、 恶意软件行为、暴力破解成功、Webshell 检测）
- 高级威胁（失陷主机检测、DGA 域名检测、恶意文件下载、隐藏信道检测、挖矿检测、HTTP 异常检测）

安全事件发展趋势：让用户了解告警、威胁、弱点的发展趋势，从宏观的角度上对云上业务做出安全策略规划。

事件统计：根据不同安全等级给出告警、威胁、弱点的安全事件分布

4.2 网络安全态势

网络安全态势大屏主要是从网络层面告诉安全团队发生了什么安全问题，安全团队需要做什么以及做的怎么样。

网络安全态势大屏包含：DDoS 告警事件、Web 攻击事件、漏洞攻击事件以及高级威胁事件 4 个方面统计。同时配合网络安全检测引擎图，以及网络安全事件发展趋势。

- DDoS 告警事件包含：网络连通状态占比（正常、黑洞和清洗的时长占比）、Top5 受影响公网 IP。
- Web 攻击事件包含：Web 攻击类别分布、Top5 受影响域名。
- 漏洞攻击事件：漏洞攻击类型、Top5 受影响服务类型。
- 高级威胁事件：高级威胁分类、Top5 风险主机。

4.3 主机安全态势

主机安全态势大屏主要是从主机层面告诉安全团队发生了什么安全问题，安全团队需要做什么以及做的怎么样。

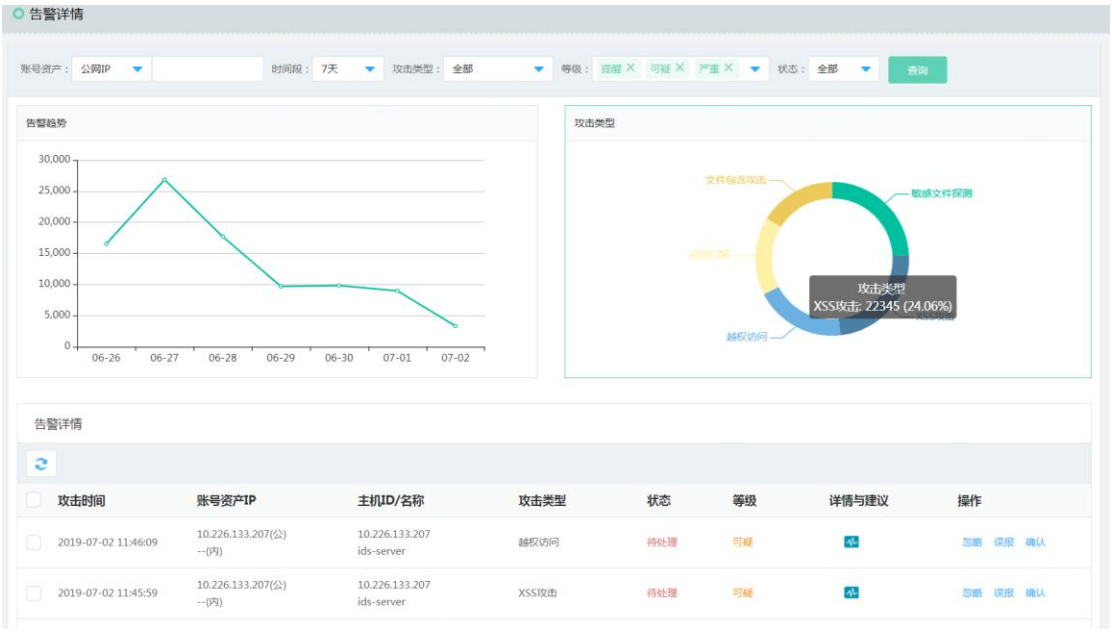
主机安全态势大屏包含：主机入侵检测事件和主机漏洞两个方面描述主机上的安全。

- 主机入侵检测事件包含：攻击类型分布、实时告警、影响资产和影响资产占比。
- 主机漏洞：危险程度分布、漏洞分布、影响资产和影响资产占比。


主机安全态势
今天
7天
30天
入侵检测
攻击类型分布
webshell检测
暴力破解成功
遭受暴力破解
系统弱口令
实时告警
WebShell:
33370
弱口令:
153K
暴力破解:
87190
攻击时间
攻击IP
账户资产
威胁类型
13:23:29
59.47.72.235
JD一号
遭受暴力破解
13:23:37
影响资产
(影响资产占比100%)
i-ak6zcyca30
vpc-waf-test
vpcwaf-wangxiaomei-test
Jason_JdogOpAgent-test
i-hxo3qza4xy
i-6m72pryrvu
i-t8x5rw9ibr
i-qb1469u4on
i-uqnluspvfj
i-zgkalji65f
0
20,000
40,000
60,000
80,000
100,000
120,00
主机漏洞
危险程度分布
高危
漏洞分布
CVE-2016-1979
CVE-2016-4794
CVE-2017-1000368
CVE-2016-10088
CVE-2016-1839
CVE-2017-7541
CVE-2016-7167
CVE-2016-9536
CVE-2017-7679
CVE-2017-9074
影响资产
(影响资产占比33%)
i-ecfd7ecome
0
20
40
60
80
100

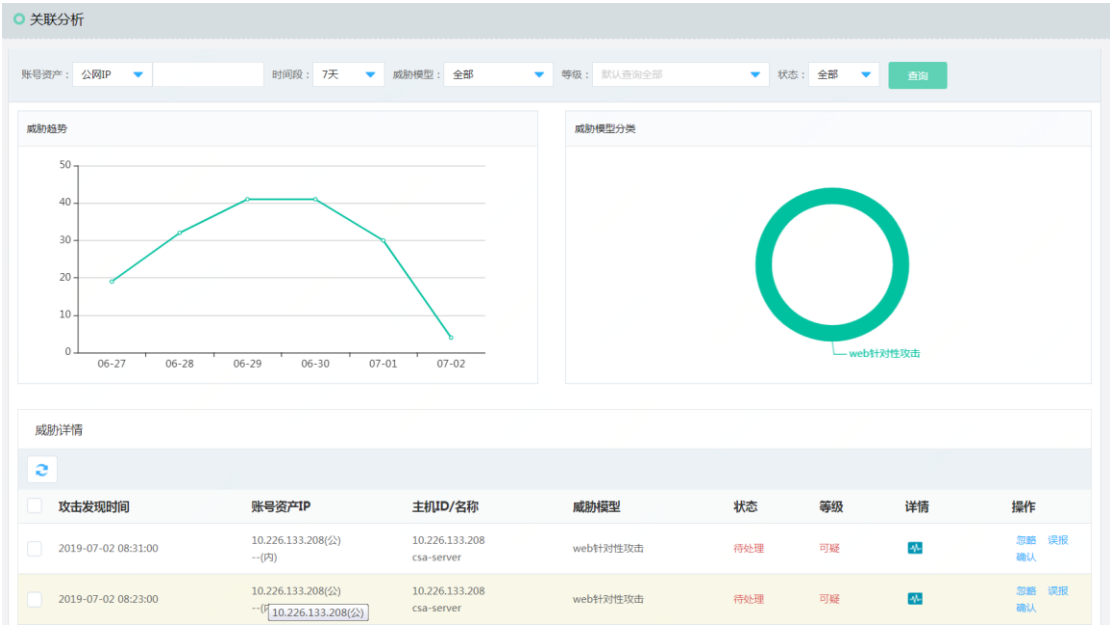
第五章　攻击详情

提供基于账号资产、详情时间段、攻击类型、等级和处理状态的查询，事件详情列表，以及事件处理状态。同时提供具体事件详情和修复建议。



关联分析

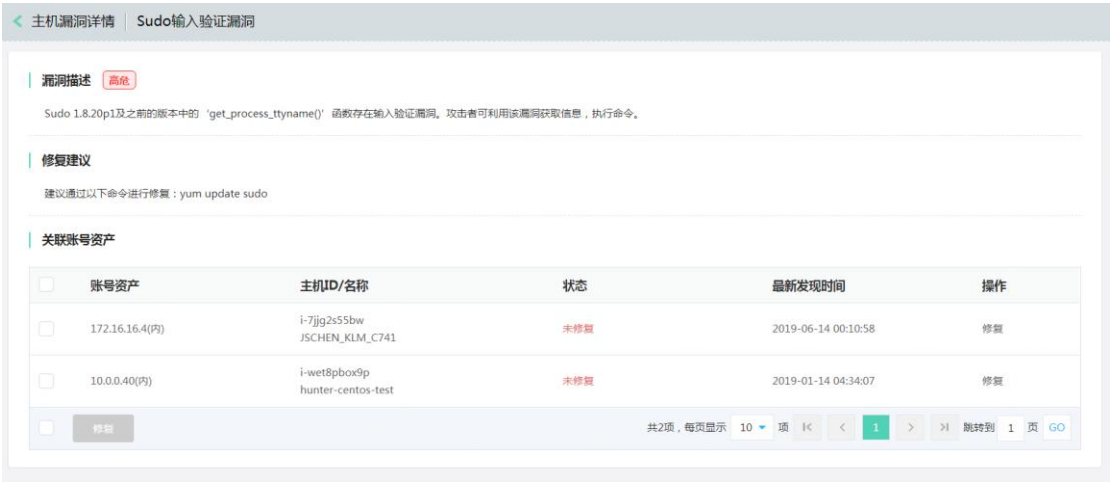
提供基于账号资产、详情时间段、威胁模型、等级和处理状态的查询，事件详情列表，以及事件处理状态更细。同时提供具体事件详情。根据关联挖掘时长区分实时挖掘、离线挖掘。



第六章　弱点详情

6.1 主机漏洞

提供基于主机漏洞详情，以漏洞为统计维度想用户展示主机弱点。督促用户修复相关漏洞。



6.2 网站漏洞

结合白帽渗透测试实战经验，通过先进的爬虫，分布式技术对京东云提供全面网站威胁检测服务。帮助用户缩短云资产漏洞发现时间，及时修复漏洞，一定程度上缓解黑客入侵行动的进一步发生，同时避免遭受品牌形象和经济损失。

6.3 应急漏洞

当有紧急漏洞发生时，京东云安全运营团队会提供应急漏洞验证 POC，帮助用户快速检查服务器的健康状态，缩短云资产漏洞发现时间，及时修复漏洞。

功能说明

当有紧急漏洞发生时，京东云安全运营团队会提供应急漏洞验证 POC，帮助用户快速检查服务器的健康状态，缩短云资产漏洞发现时间，及时修复漏洞。

操作步骤

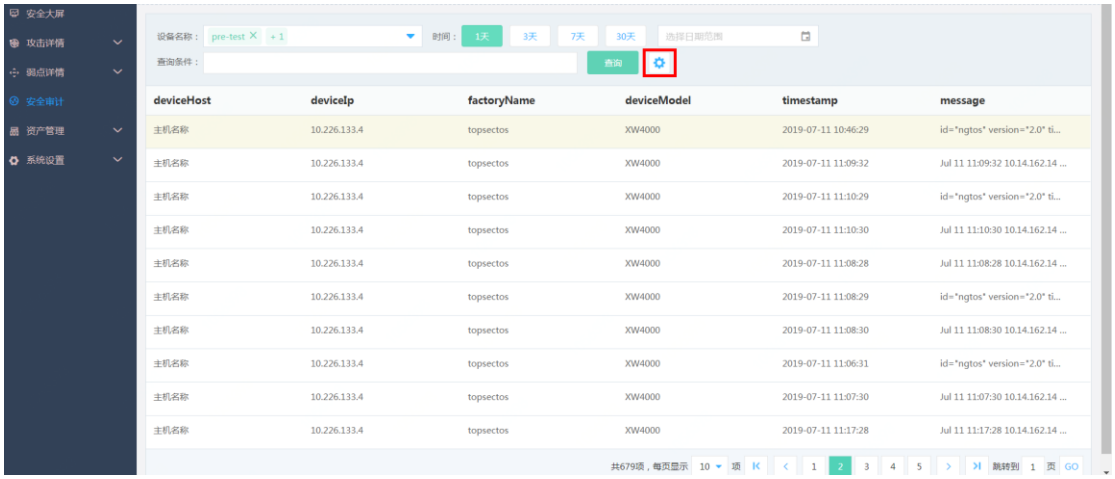
在应急漏洞列表页，点击具体的漏洞名称，进入到单漏洞详情页。通过搜索功能，找到需要检测的资产，点击【检测】或者【再次检测】，会启动手工检测流程。观察检测结果。

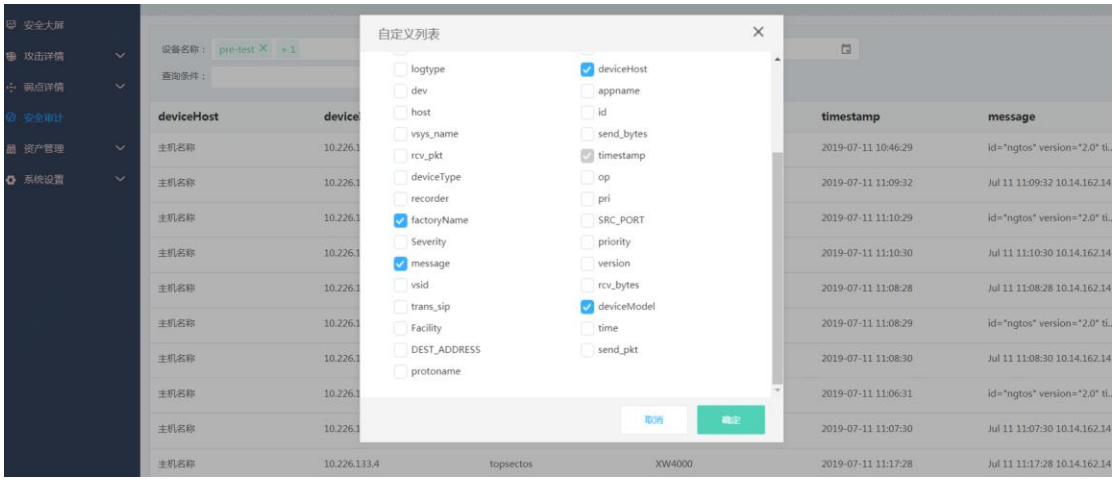
第七章　安全审计

安全审计功能支持采集归一化后的日志和保留原始日志，方便用户对关键日志快速定位，和事后取证；

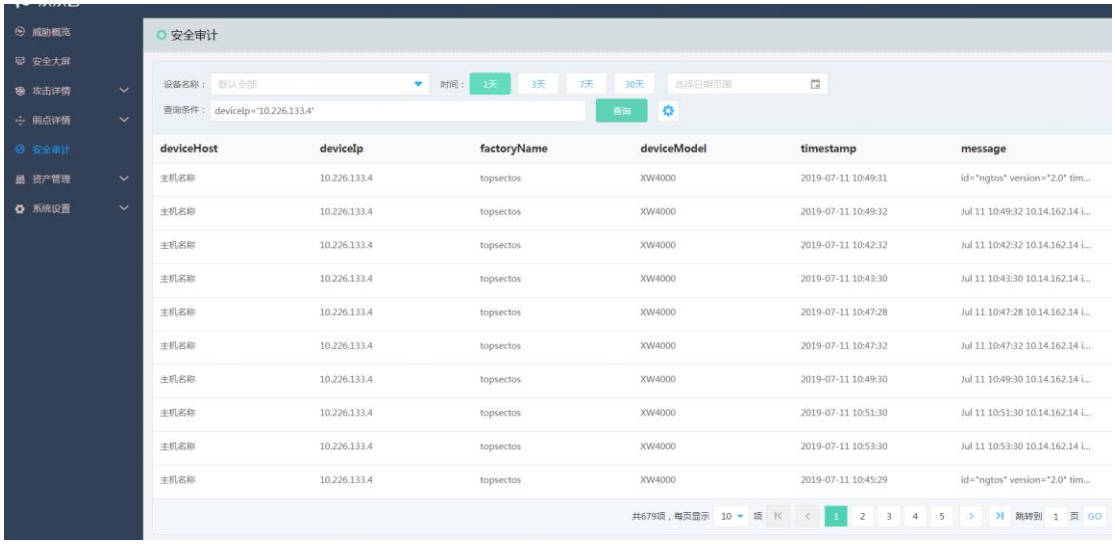
支持原始消息中的关键字查询，可进行全文检索；

1、首先选择显示列





2、输入查询条件


威胁概览
安全大屏
攻击详情
弱点详情
安全审计
资产管理
系统设置
安全审计
设备名称：
默认全部
时间：
1天
3天
7天
30天
选择日期范围
查询条件：
deviceIp="10.226.133.4"
查询
deviceHost
deviceIp
factoryName
deviceModel
timestamp
message
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:49:31 id="ngtos" version="2.0" tim...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:49:32 Jul 11 10:49:32 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:42:32 Jul 11 10:42:32 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:43:30 Jul 11 10:43:30 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:47:28 Jul 11 10:47:28 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:47:32 Jul 11 10:47:32 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:49:30 Jul 11 10:49:30 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:51:30 Jul 11 10:51:30 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:53:30 Jul 11 10:53:30 10.14.162.14 i...
主机名称 10.226.133.4 topsectos XW4000 2019-07-11 10:45:29 id="ngtos" version="2.0" tim...
共679项，每页显示 10 项
1 2 3 4 5
跳转到 1 页 GO

第八章　资产管理

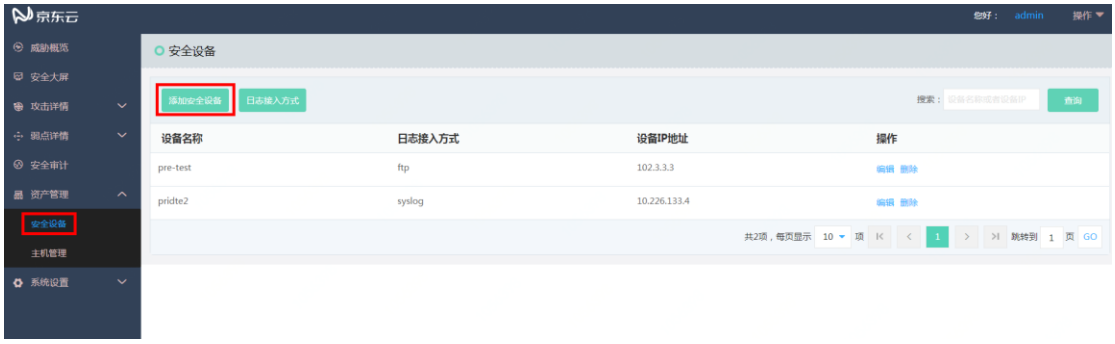
8.1 安全设备

安全审计对象包括支持审计各种网络设备（路由器、交换机、等）配置日志、运行日志、告警日志等；支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防 DDOS 攻击，Web 应用防火墙、等）配置日志、运行日志、告警日志等；支持审计各种主机操作系统（包括 Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）配置日志、运行日志、告警日志等；支持审计各种中间件（tomcat、apache、webshpere、 weblogic 等）配置日志、运行日志、告警日志等；

【安全设备】提供了第三方接入设备管理：

◇ 提供安全设备增删改查功能

◇ 日志接入方式设定，目前支持 syslog、snmp、ftp 等方式



添加设备：

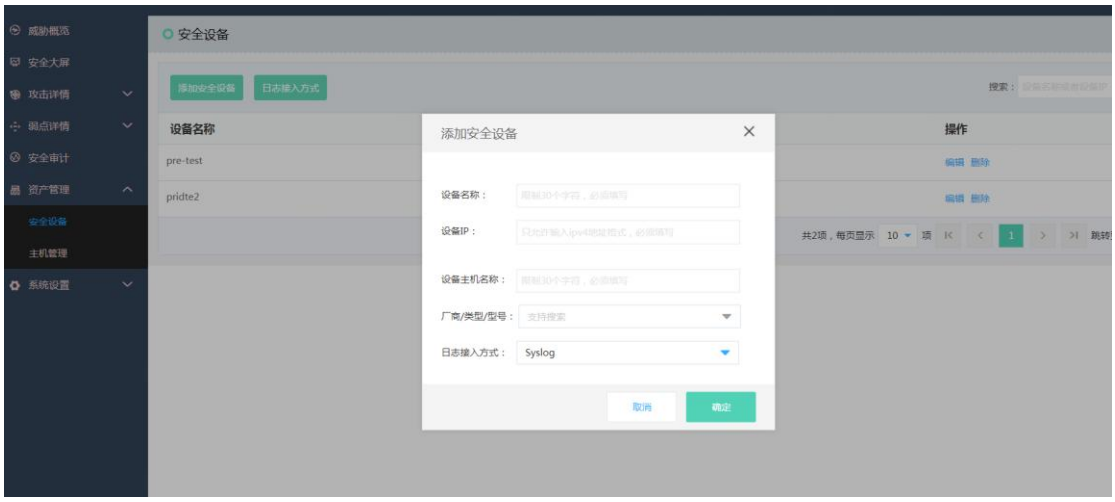
◇ 设备名称

◇ 设备 IP

◇ 设备主机名

◇ 厂商/类型/型号：系统默认支持山石防火墙、天融信防火墙等日志的接入，如果有用户其他设备接入，可联系运维人员另行增加。

◇ 日志接入方式：Syslog、FTP、snmp



【安全设备】->【syslog】接入方式

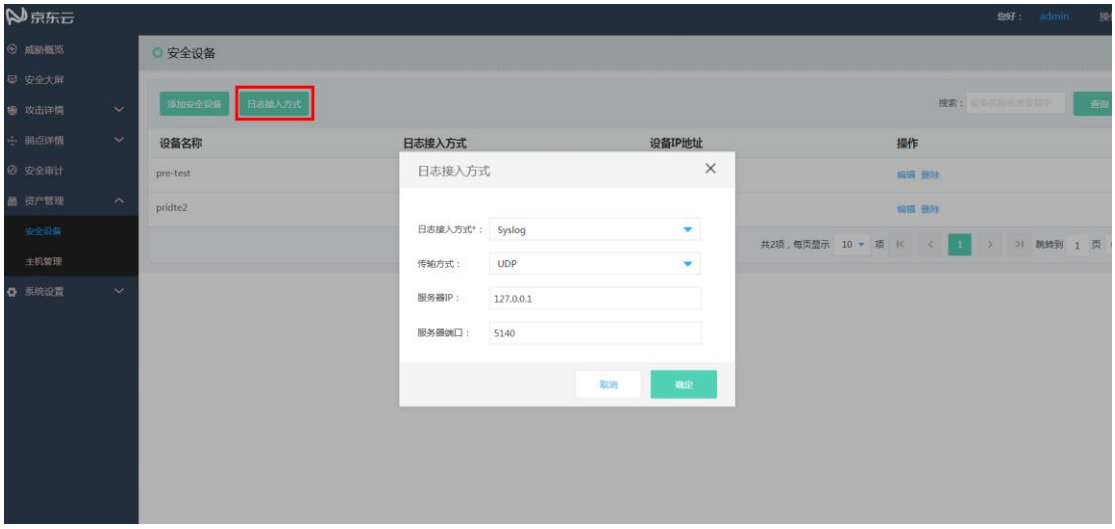
具体功能选项如下：

◇ Syslog 传输方式：支持 TCP 和 UDP 两种方式，默认是 UDP 方式

◇ 服务器 IP：syslog 日志接受服务器的 IP

◇ 服务器端口：syslog 日志接受服务器的端口，默认 514

◇ 添加地址：点击按钮，添加服务的 IP 和端口

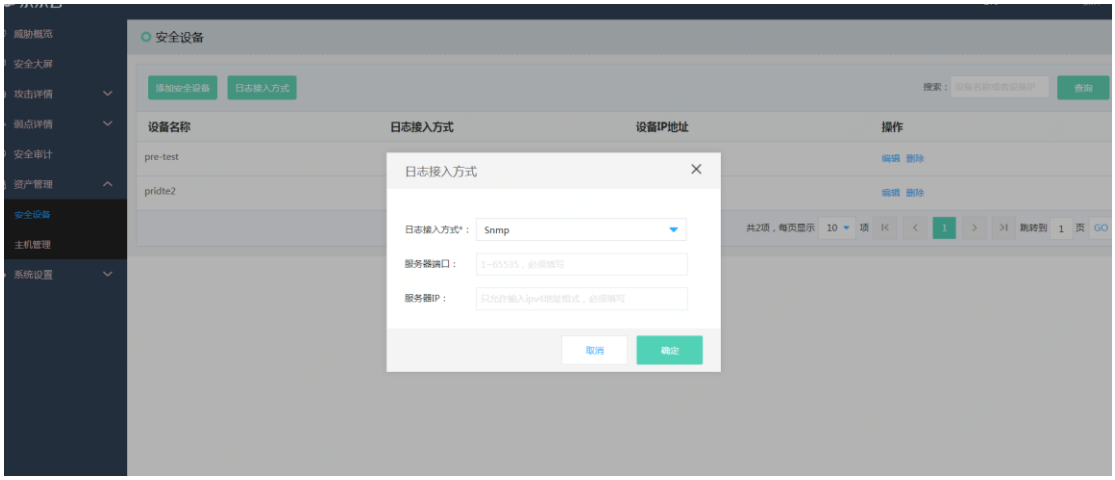


【安全设备】->【snmp】接入方式

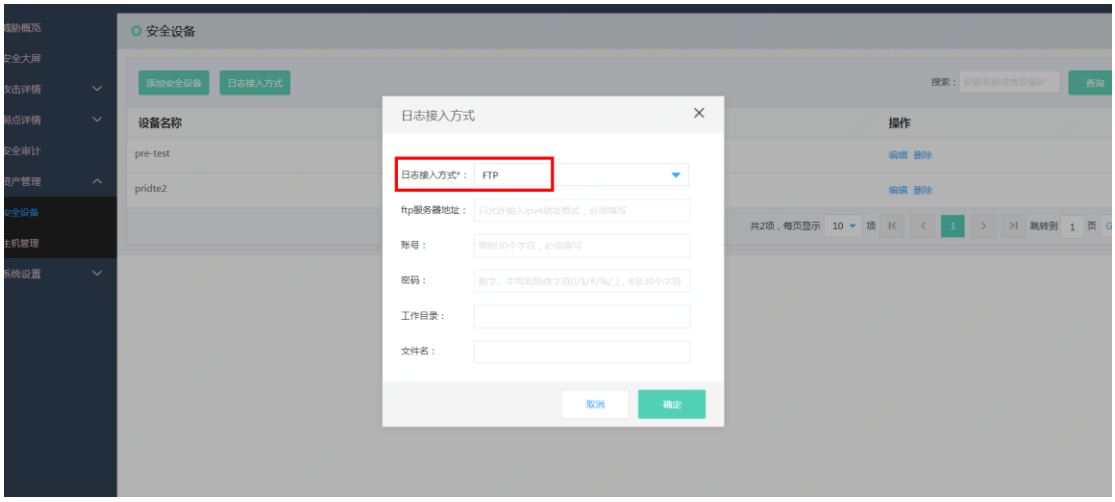
Snmp trap 收集日志方式，snmp 服务器端配置，

◇ Snmp 服务器地址：默认 127.0.0.1

◇ 服务器 IP：syslog 日志接受服务器的 IP



【安全设备】->【ftp】接入方式



◇ Ftp 服务器地址：用户提供的 FTP Server 地址

◇ 账号：FTP 登录账号

◇ 密码：FTP 登录账号密码

◇ 工作目录：FTP 文件存储的目录

◇ 文件名：FTP 工作目录存储，我们要采集的文件，支持多个文件，支持正则表达式的文件名

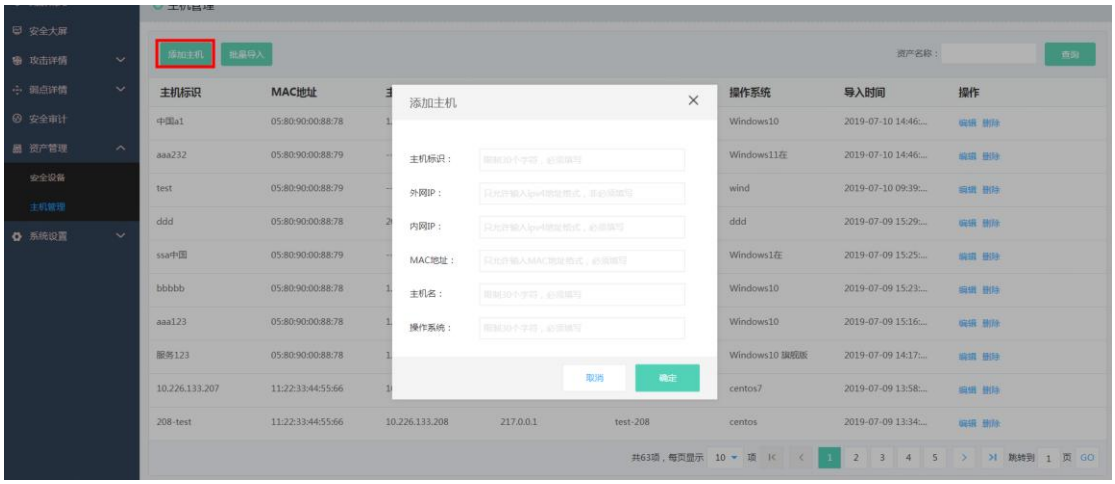
8.2 主机管理

主机管理模块提供了主机自动识别和主机手动登记功能。用户可以进行主机的新增、批量删除、批量导入、批量导出以及搜索操作。

> 注：主机识别需要京东态势感知全流量引擎接入后才可以体现出来。

8.2.1 添加主机

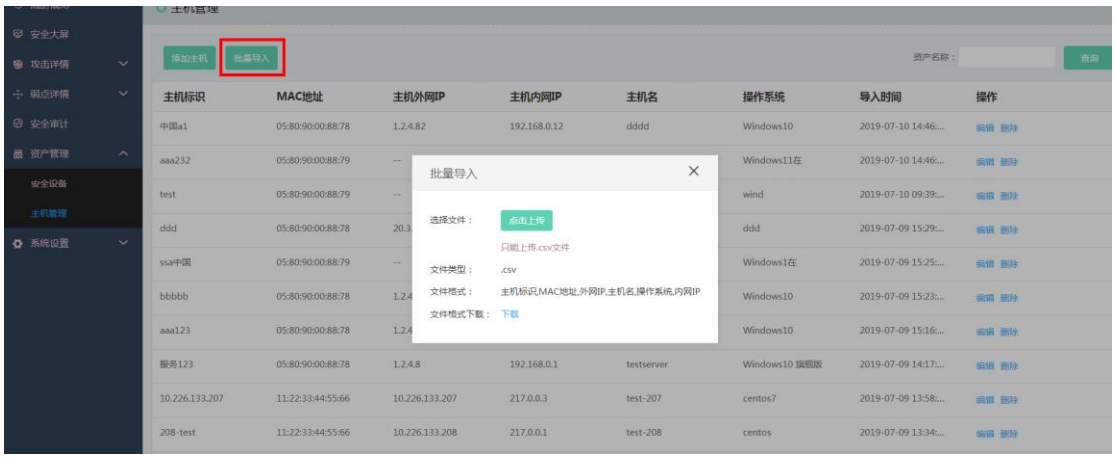
【资产管理】->【主机管理】页面，点击【添加主机】，在弹出的新增主机页面填写主机信息，点击【保存】 即可完成主机新增操作，如下图所示。



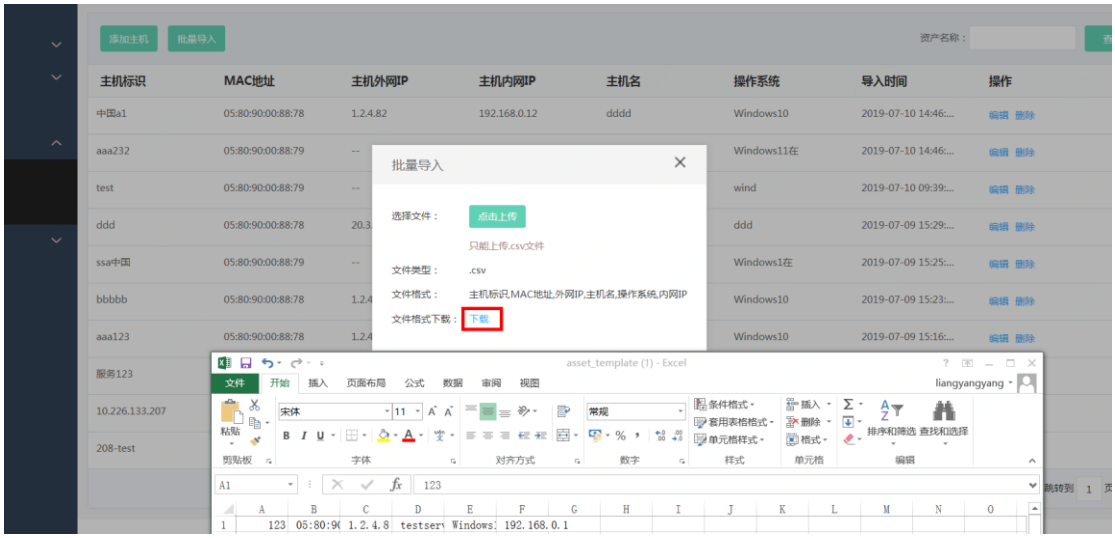
- ◇ 主机标识：主机的唯一标识符。
- ◇ 外网 IP：主机的外网 IP 地址。
- ◇ 内网 IP：主机内网 IP 地址
- ◇ MAC 地址：主机的 MAC 地址。
- ◇ 主机名：可选项，主机的计算机名称。
- ◇ 操作系统：主机的操作系统名称。

8.2.2 批量导入

【资产管理】->【主机管理】页面，点击【添加】，，用户可以通过批量导入来一次性录入多个主机信息，模板文件可以在导入页面下载，如下图所示。



批量导入模板文件格式为 excel，用户不得随意更改后缀或者另存为其他格式文件，只能编辑文档中要求的字段信息，如下图所示：



导入时候系统会对模板文件做格式校验，文件格式或者字段内容格式不正确的会给出提示。

第九章　系统设置

9.1 用户管理

【用户管理】提供了登录用户管理：

◇ 提供用户增删改功能

◇ 包含简单的角色管理，管理员，可以对系统进行设置，普通用户，只能查看数据。

操作步骤：

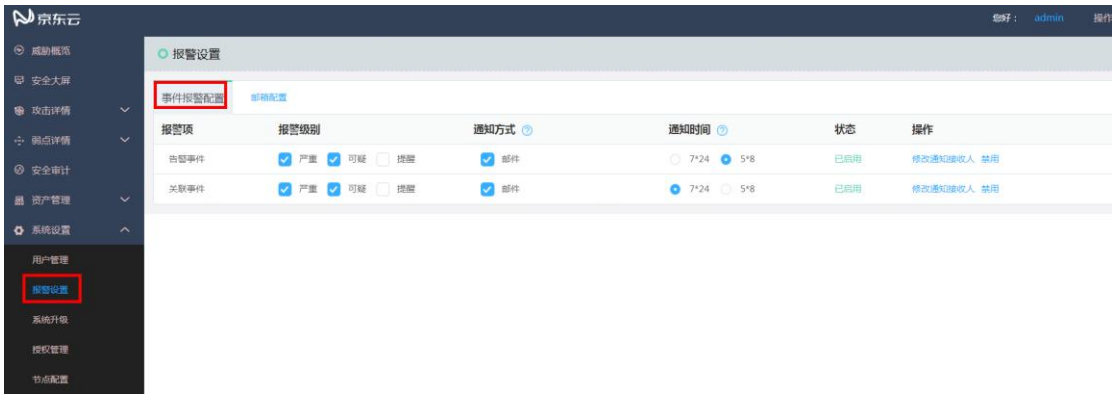
1、 点击【新增】， 填写账号名称，密码，确认密码，用户角色。然后点击确认

2、 在查询窗口输入账号名称，可以查询到建立的用户。可编辑，权限降级等。

9.2 报警设置

【事件报警配置】提供了告警相关选项：

- ◇ 告警级别设置，包括：严重、可疑、提醒
- ◇ 通知方式：目前支持邮件
- ◇ 通知时间：支持 5*8 和 7*24 小时
- ◇ 是否启动
- ◇ 通知接收人：可以设置多个邮件接收人，以，号分割。



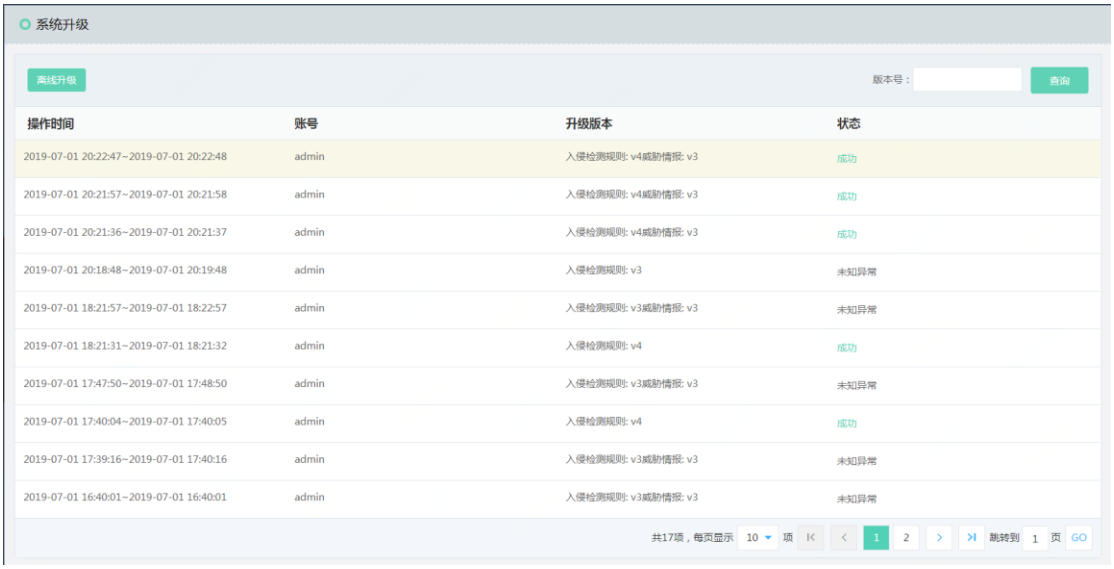
【邮箱配置】提供了邮箱相关选项：

- ◇ 服务器地址，例如：smtp.126.com
- ◇ 服务器端口，例如：25
- ◇ 邮件协议：默认 SMTP
- ◇ 服务器认证，默认为关
- ◇ 发信人：邮箱的账户名
- ◇ 密码：邮箱服务器的密码
- ◇ SSL：默认关闭
- ◇ SSL 协议端口:服务器自带的邮箱端口， 例如：465

9.3 系统升级

【系统升级】提供了离线升级系统软件版本和规则库版本，如下图所示：

◇ 离线升级：为用户提供离线升级方式，从云端服务器下载系统软件版本升级包，后缀为.zip 文件，手动导入升级包。



操作步骤：

3、 点击【离线升级】，把从对象存储下载来的 zip 包上传。

4、 观察等级状态，如果显示未知异常，请重新升级。或联系售后工程师。如果限制成功，表示升级成功。

5、 可以通过版本号查询，升级历史记录，方便故障排查。

9.4 授权管理

【授权管理】模块提供系统证书管理功能，包括系统证书信息的显示、证书导入等功能。

注：设备出厂默认无证书，请联系相关人员制作证书然后按下文说明导入证书。

证书导入后：

操作步骤：

1、 根据用户系统默认登录账号，进入到系统中，首先要导入 licence，才能使用该设备。

2、 复制激活码：

eyJ1dWlkIjoiIiwibm9kZUlkIjoiNEM0QzQ1NDQtMDA1Ny00RTEwLTgwMzEtQjZDMDRGNTMzNjMyNldOMVM2MkRFTEwiLCJlbmFibGVMYiI6ZmFsc2UsImVuYWJsZVdhZiI6ZmFsc2UsImN1c3RvbWVyIjoiIiwiZW1haWwiOiIiLCJiZWdpblRpbWUiOjAsImVuZFRpbWUiOjB9

发送给授权管理员。

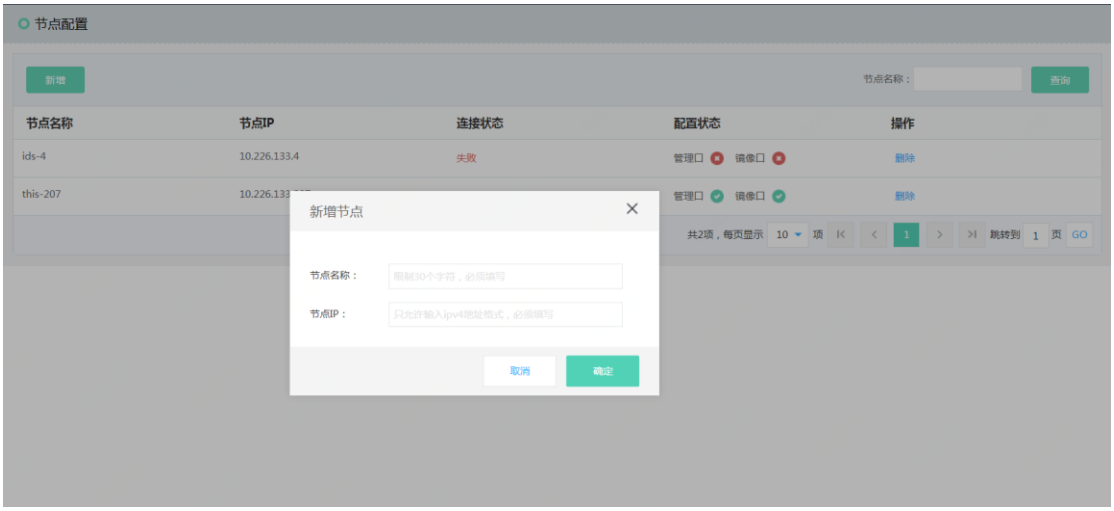
3、 授权管理员会生成一个 txt 的授权文件，用户点击导入授权。

4、 如果导入成功， 会显示授权有效期，

例如：2019-05-03 06:04:05 ~ 2020-06-03 14:04:05

9.5 节点管理

【节点管理】当分布式部署多个 IDS 探针。



第十章　产品规格指标

硬件形态	
态势感知私有云型号	JDSAV6000-企业版
CPU	英特尔® 至强® E5-2620 v4 2.1GHz* 2
内存	64G
硬盘	600GB 10K RPM SAS 12Gbps 2.5 英寸热插拔硬盘
操作系统	CentOS7.6
高度	2U
电源	双冗余电源
固定接口	4*GE 电口（1 个千兆管理接口、3 个千兆监听接口），可选 2*10GE 光口
工作环境温度	工作温度：5°C ～ 45°C（41°F ～ 113°F） 存储温度：-40°C ～ +65°C（-40°F ～ 149°F） 温度变化每小时小于 20°C（36°F）
环境湿度	工作湿度：8% RH～90% RH 非凝结 存储湿度：5% RH～95% RH 非凝结 湿度变化每小时小于 20% RH
EPS	10000

硬件形态	
态势感知私有云型号	JDSAV6000-旗舰版
CPU	英特尔® 至强® E5-2640 v4 2.4GHz* 2
内存	128G
硬盘	1.92TB SSD SAS 读取密集型 12Gbps 512 2.5 英寸热插拔 AG 硬盘
操作系统	CentOS7.6
高度	2U
电源	双冗余电源
固定接口	4*GE 电口（1 个千兆管理接口、3 个千兆监听接口），可选 2*10GE 光口
工作环境温度	工作温度：5°C ～ 45°C（41°F ～ 113°F） 存储温度：-40°C ～ +65°C（-40°F ～ 149°F） 温度变化每小时小于 20°C（36°F）
环境湿度	工作湿度：8% RH～90% RH 非凝结 存储湿度：5% RH～95% RH 非凝结 湿度变化每小时小于 20% RH
EPS	100000

第十一章　系统安装说明

11.1 部署系统要求

操作系统版本要求大于 CentOS7.4

独立的磁盘分区存储 docker 数据 如/export/docker

将压缩包上传到系统目录/opt/csa-dvd

11.2 安装流程

执行如下命令：
#本地源安装 docker，
#install-csa.sh -h 帮助信息
./install-csa.sh
-o 离线安装
-O 在线安装，默认
-f 指定安装包文件名，默认 csa_all_in_one.tgz
-r 安装包主目录，默认/usr/local/csa
-I 管理主机的网卡名，默认是系统 default 网卡
-u IDS 的数据网卡，默认是系统 default 网卡
-z docker 服务数据主目录，默认/export/docker
执行镜像导入时，时间会比较长请耐心等待

```
[admin@A04-R08-I193-79-J4GG8P2 csa-dvd-2019-07-10]$ sudo ./install-csa.sh -r /home/csa-test
```

```
 1. Check System:
    Pre-Checking: ... PASS
    Check System:vm.max_map_count = 262144
 ... PASS
    Update Package Repository: ... PASS

 2. Get CSA:
    Download CSA package: ... PASS
    Unpack CSA package: ... PASS
    Install CSA Docker:检查Docker......
 ... -Docker version 18.09.6, build 481bc77156
检查到Docker已安装!
PASS
ln: failed to create symbolic link '/usr/bin/docker-compose': File exists
    docker load images,pls wait for minutes...:Loaded image: spark-submit-jobs:2.3.3
Loaded image: nginx:1.0.0
Loaded image: redis:5.0.4-alpine
Loaded image: amazon/opendistro-for-elasticsearch-kibana:latest
Loaded image: portainer/portainer:latest
Loaded image: hadoop-datanode:latest
Loaded image: spark-worker:2.3.3
Loaded image: spark-submit-jobs:2.3.3.1
Loaded image: zookeeper:3.4.14
Loaded image: wurstmeister/kafka:2.12-2.2.0
Loaded image: rabbitmq:v1
Loaded image: hadoop-namenode:latest
Loaded image: spark-master:2.3.3
Loaded image: mariadb:10.3.14
Loaded image: portainer/portainer:1.20.2
Loaded image: hub.ark.jd.com/jcloud-sec/ids-agent:develop-priv-67d76535-0626103019
Loaded image: hub.ark.jd.com/jcloud-sec/ids-suricata:develop-priv-6399874f-0703101153

 3. Install CSA Tools:
```

```
 3. Install CSA Tools:
    Change Owner in CSA: ... PASS
    Install all-compose.yml docker-compose in CSA: ... |WARNING: Some networks were defined but are not used by any service: hostnet
Creating network "runningcontainer_csa-network" with the default driver
Creating csa-hub      ... done
Creating flume-es     ... done
Creating flume-kafka  ... done
Creating aws-es       ... done
Creating nginx        ... done
Creating flume-yun    ... done
Creating namenode     ... done
Creating portainer    ... done
Creating ids          ... done
Creating redis        ... done
Creating flume-snmp   ... done
Creating flume-ftp    ... done
Creating zookeeper    ... done
Creating etcd         ... done
Creating flume-syslog ... done
Creating mariadb      ... done
Creating kafka        ... done
Creating ids-agent    ... done
Creating data-api     ... done
Creating csa-kibana   ... done
Creating datanode1    ... done
Creating data-app     ... done
Creating sas-biz      ... done
Creating spark-master ... done
Creating console        ... done
Creating spark-worker-1 ... done
Creating spark-jobs-agg    ... done
Creating spark-jobs-ddos   ... done
Creating spark-jobs-attack ... done
Creating spark-jobs-risk   ... done
PASS
elasticsearch-curator-5.7.6-1.x86_64
installed lasticsearch-curator!

CSA All In One  Installation Completed:
 - Installation path: /home/csa-test
 - all service started ,client https:10.226.193.79/
 - manage container client http:10.226.193.79/

 - you can change to Installation path use docker-compose -f all-compose.yml down to stop all services
```

异常查看日志文件 tail -f /tmp/csa_installation.log