全流量平台使用分析培训

2019护网专项培训

NSFOCUS

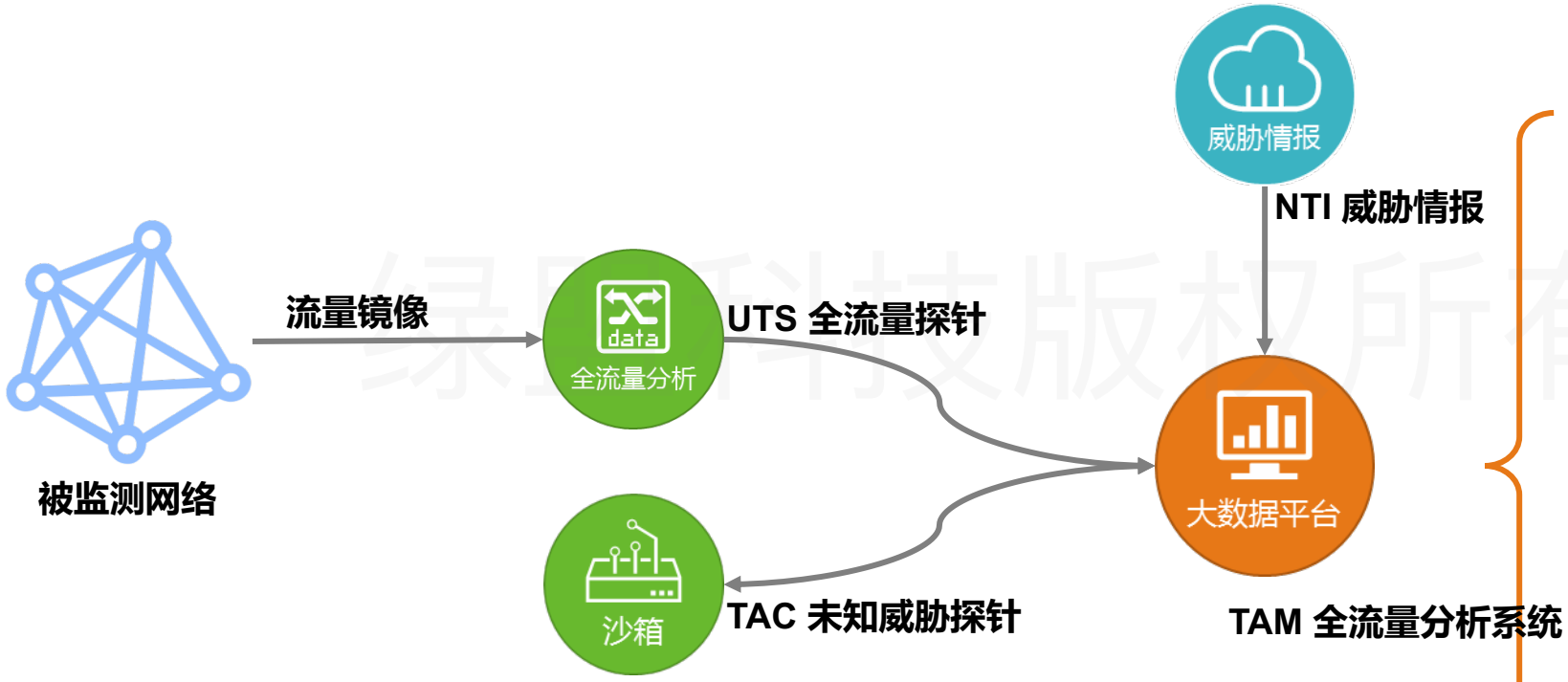
目录
CONTENTS

NSFOCUS

01

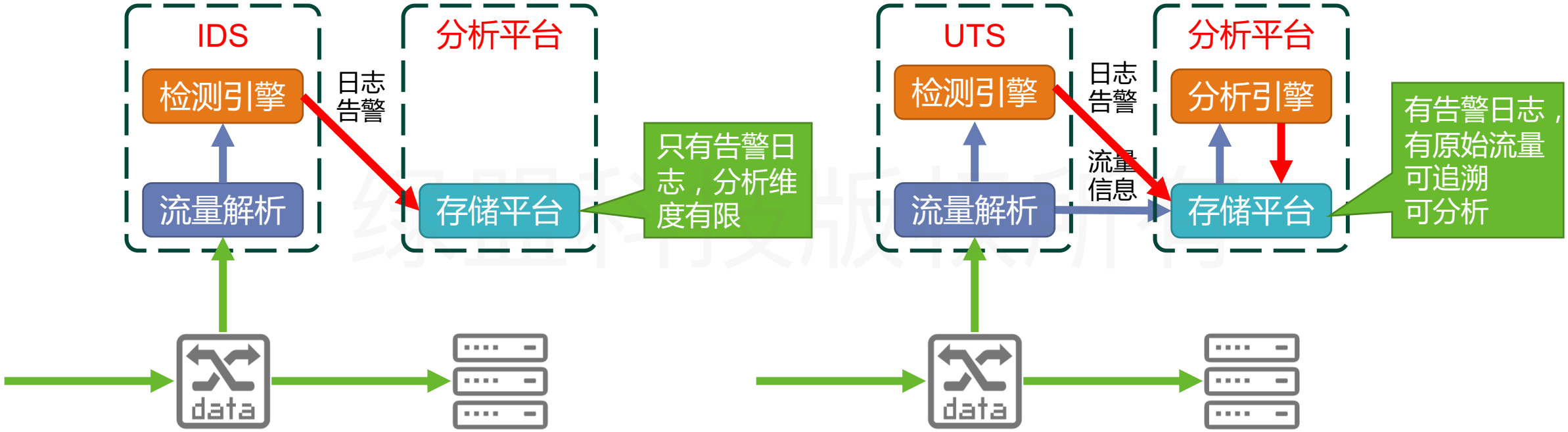
工作原理

全流量方案架构



- 高危事件监控
- 失陷资产监控
- 攻击者画像
- 流量监控
- 资产监控
- 情报分析
- 攻击链分析
- 流量黑名单监控
- 应急事件分析
- 自定义场景分析

传统方案 vs. 全流量方案



大数据平台上只有IDS告警，只能做告警分析，但对于漏报等问题无法解决。

由于大数据平台上有原始流量，所以可以利用机器学习技术针对流量做额外的分析。

全流量组成

高级威胁检测TAC

样本文件虚拟执行，恶意文件检测、文件动态执行、信息还原

威胁情报系统NTI

威胁情报数据推送，威胁情报分析，为威胁事件的判定及回溯提供有力支撑

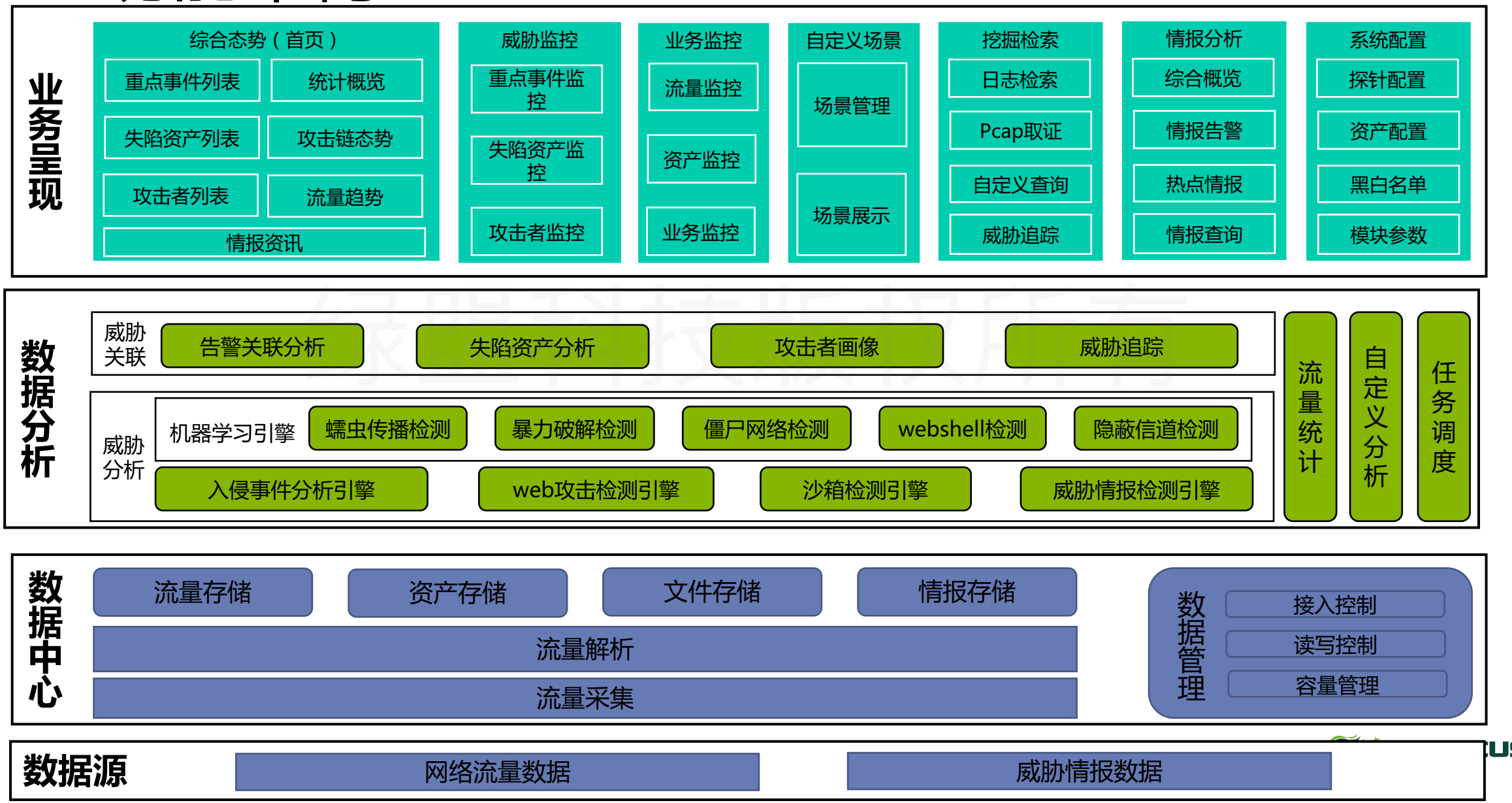
全流量分析探针UTS

原始流量协议解析、流量留存、样本文件提取，智能引擎检测

全流量存储分析平台TAM

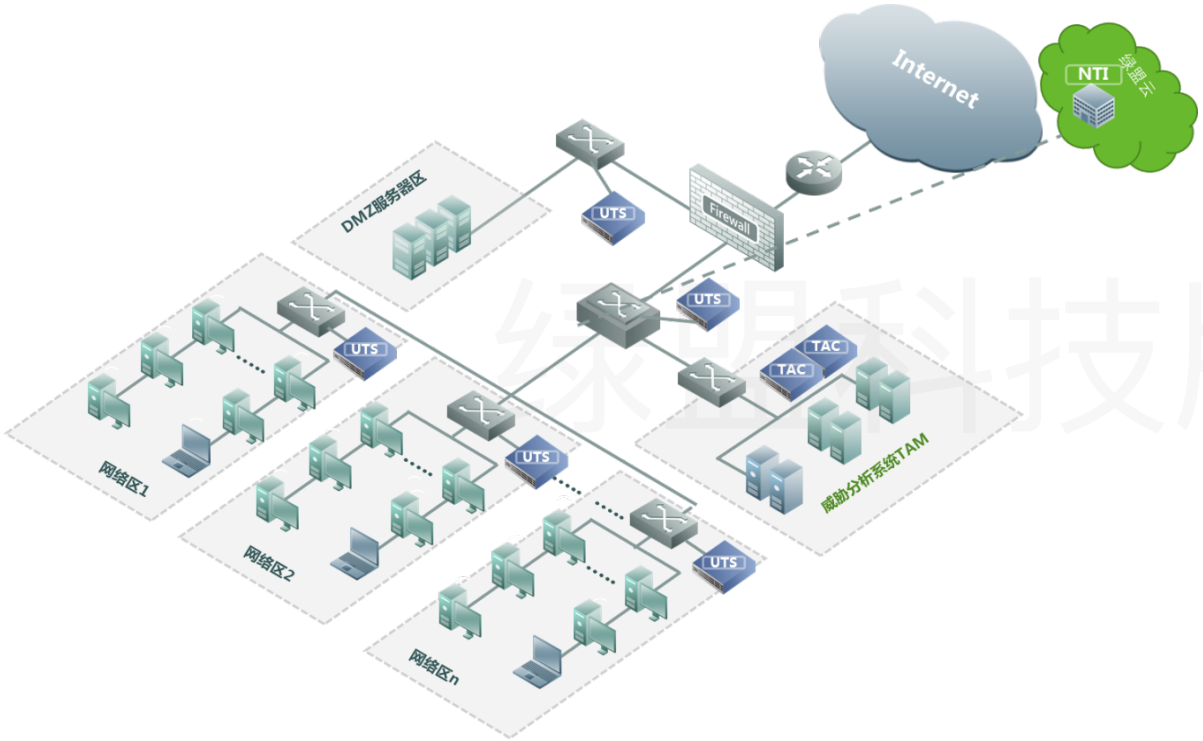
利用大数据技术对解析还原的流量数据进行存储、挖掘；结合探针智能检测告警进行关联分析，发现APT事件，同时可进行溯源分析。

功能架构


业务呈现
综合态势（首页）
重点事件列表
统计概览
失陷资产列表
攻击链态势
攻击者列表
流量趋势
情报资讯
威胁监控
重点事件监控
失陷资产监控
攻击者监控
业务监控
流量监控
资产监控
业务监控
自定义场景
场景管理
场景展示
挖掘检索
日志检索
Pcap取证
自定义查询
威胁追踪
情报分析
综合概览
情报告警
热点情报
情报查询
系统配置
探针配置
资产配置
黑白名单
模块参数
数据分析
威胁关联
告警关联分析
失陷资产分析
攻击者画像
威胁追踪
威胁分析
机器学习引擎
蠕虫传播检测
暴力破解检测
僵尸网络检测
webshell检测
隐蔽信道检测
入侵事件分析引擎
web攻击检测引擎
沙箱检测引擎
威胁情报检测引擎
流量统计
自定义分析
任务调度
数据中心
流量存储
资产存储
文件存储
情报存储
流量解析
流量采集
数据管理
接入控制
读写控制
容量管理
数据源
网络流量数据
威胁情报数据

全流量部署

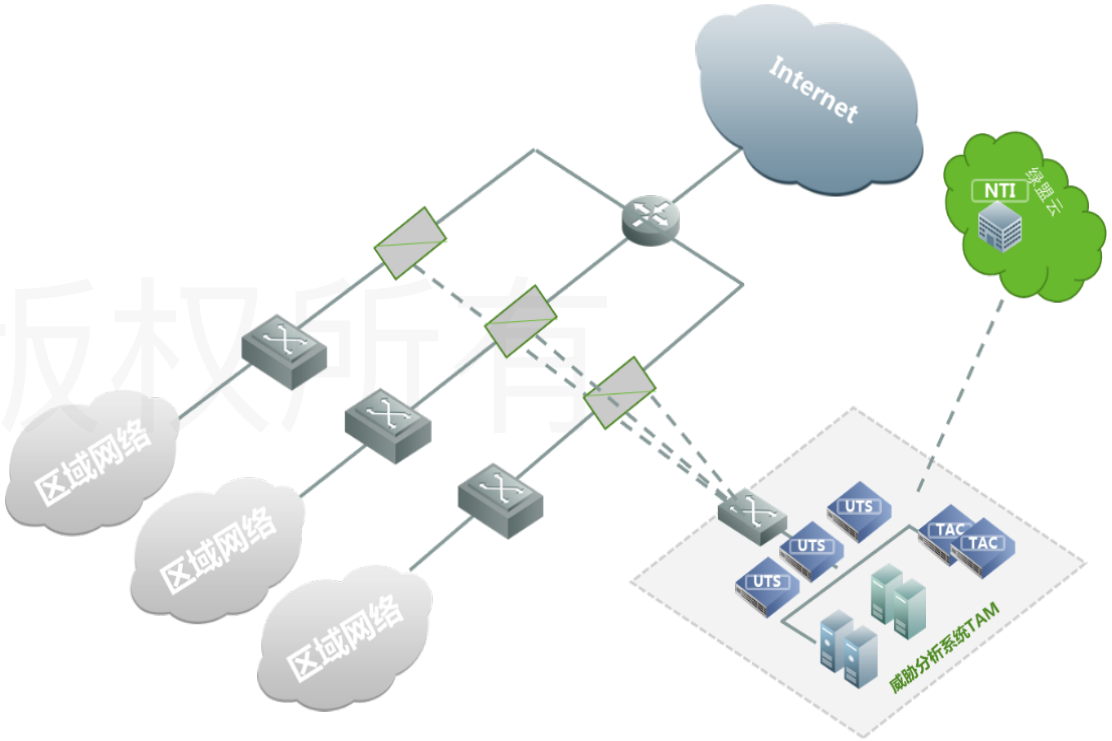
企业网络部署



企业出口和内部关键节点部署流量探针UTS，集中部署分析系统TAM。

监测外部威胁和内部横向威胁。

网络出口部署



运营商或大型网络出口，分光/镜像干路流量，集中/分布式部署UTS，集中部署分析系统TAM。

监测内外部威胁，掌握安全态势。

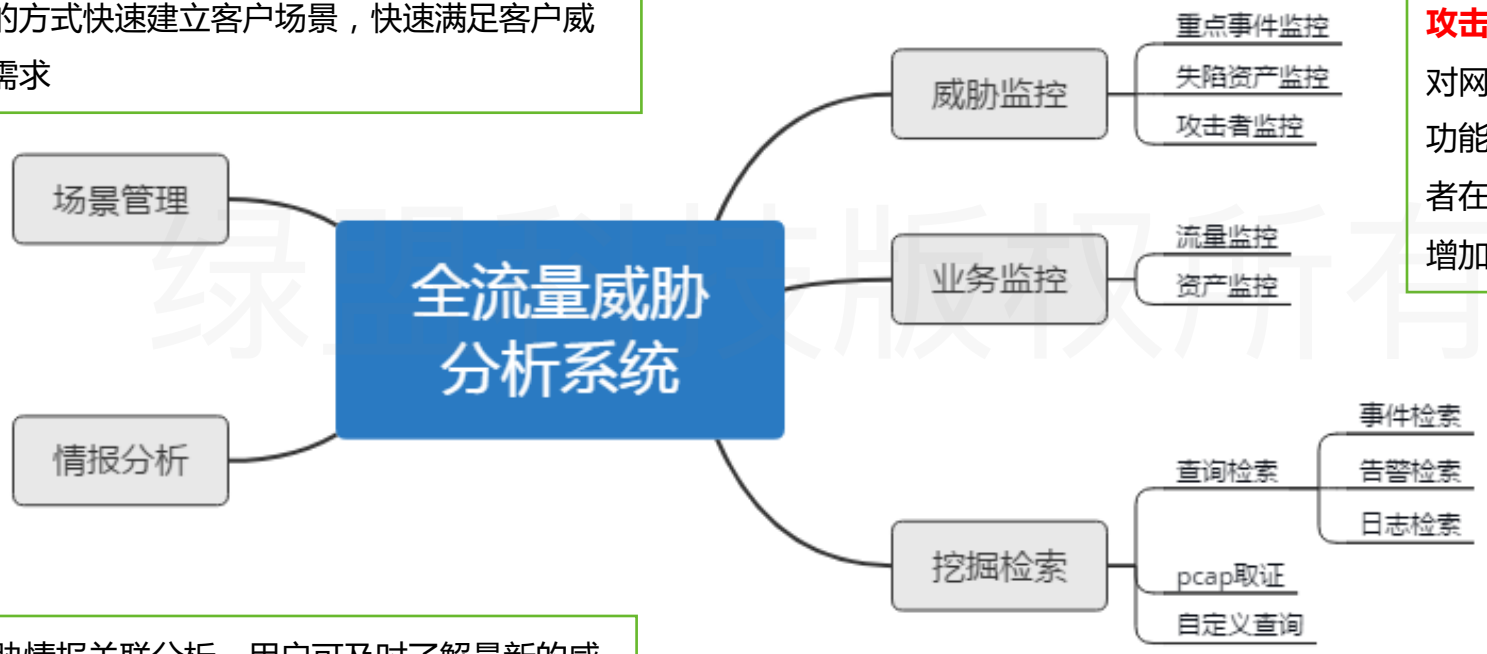
NSFOCUS

重点功能介绍

重点事件监控：对事件告警进行关联分析并输出用户关注的重点事件，如热点事件、apt攻击事件、Botnet事件、恶意样本传播事件或是单次高危攻击事件等（webshell、隐蔽信道）。

失陷资产监控：从资产角度结合攻击链向用户展示失陷资产的情况，帮助客户从海量告警事件中，快速定位需要关注和处理的资产

场景管理：支持自定义黑名单、自定义规则、自定义检测插件的方式快速建立客户场景，快速满足客户威胁检测的需求



攻击者监控：从攻击者角度出发，梳理出对网络最具威胁的攻击者，通过情报关联功能，追溯攻击者的相关信息，聚合攻击者在客户网络中的攻击行为和通信行为，增加攻击事件可信度

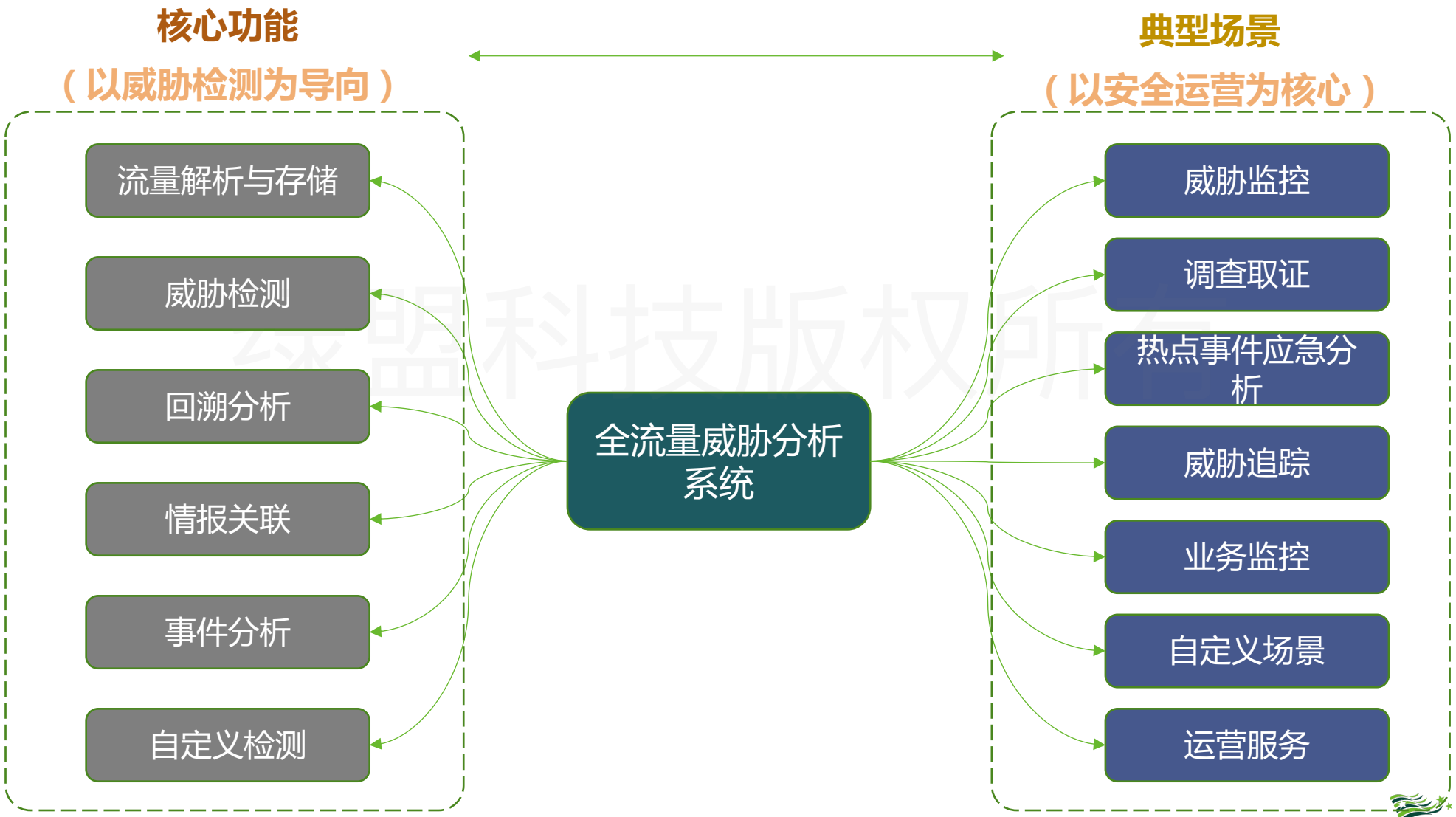
流量监控：监控流量日志，分析流量成分及趋势，对流量异常的情况形成告警，及时反馈给用户。

资产监控：监控资产活跃情况，对资产外联情况进行分析及预警。

情报分析：通过威胁情报关联分析，用户可及时了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，通过情报验证功能增加安全事件的可信度，并准确地进行威胁追踪和攻击溯源

Pcap取证：基于数据回溯功能，用户可以通过查看流量日志进行pcap包取证；支持以事件下钻方式自动关联出攻击告警相关的pcap包信息；用户还可以手动设置条件，查询自己关心的流量，对历史流量进行精确下载。

核心功能和应用场景



02

部署方式

BSA安装部署流程

一.和商务申请证书
1.1申请加密狗，只能识别无驱，如何判断有驱无驱参考WIKI
所有材料请必须从工程ftp获取
二. 安装及部署
2.1操作系统centos7.3，参考操作系统安装手册和BSA安装部署手册中的要求
2.2获取BSA和APP安装包，推荐BSA F05，TSA F02，TAM F00SP03
2.3后台配置及安装BSA，参考BSA安装部署手册
2.4前台倒入证书，初始化BSA，分盘及部署组件等，参考BSA安装部署手册
2.5安装TSA,TAM APP
三.数据接入
3.1设备端安装部署及配置联动，数据接入，详情咨询设备端技术支持
3.2老A接口接入需部署BSA转发器，通过设备—转发器—BSA方式接入
3.3三方数据接入，需要配置Grok解析规则及自定义事件规则
四.数据查看
4.1查看TAM首页面及挖掘检索下的重点事件、告警，原始日志是否正常；
查看TSA首页面及风险态势下的子态势事件，数据分析下的原始日志是否正常;
4.2查看集群管理的状态，Hadoop的资源及Job状态等

和商务申请证书

BSA证书

- 集群可以给单机用，单机不可以给集群用
- 更换加密狗会有问题，因为安装时识别的hash是来自于加密狗内的产生的hash

加密狗有驱无驱问题

- http://192.168.255.65/iaes/search/viewsolution/5676
- http://192.168.255.65/iaes/search/viewsolution/7990

BSA 加密狗使用、证书制作 [BSA的证书是使用加密狗hash制作的]

分类: BSA

BSA使用的是"深思洛克-精锐4型USB Key，支持U盘版和普通版：

1）U盘版都是无驱的，可以直接插在安装有BSA的服务器上使用。

2）普通版分为：有驱动和无驱动两种，BSA只支持无驱型的。

注：如果从生产中心拿到的usb key是有驱动型的，需要通过工具转换为无驱动型的。详见知识点：11448

另外：

RSAS和BSA的加密狗，硬件相同，软件不同，不能混用。

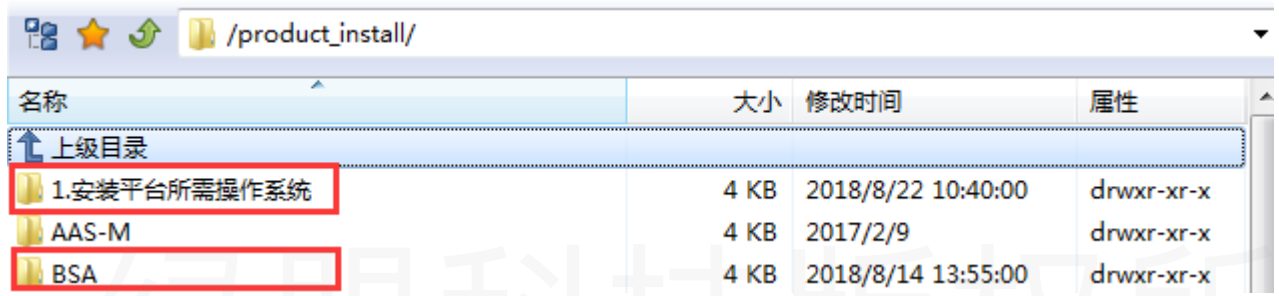
- 1. 如何判断BSA使用的【普通版】加密狗是"有驱"还是"无驱"型的？ [加密狗有驱和无驱型识别和转换方法]
- 2. 如何获取BSA加密狗的hash，供做证书使用？ [获取加密狗hash的方法]
- 3. 如何查看BSA的证书信息？ [BSA证书查看方法]

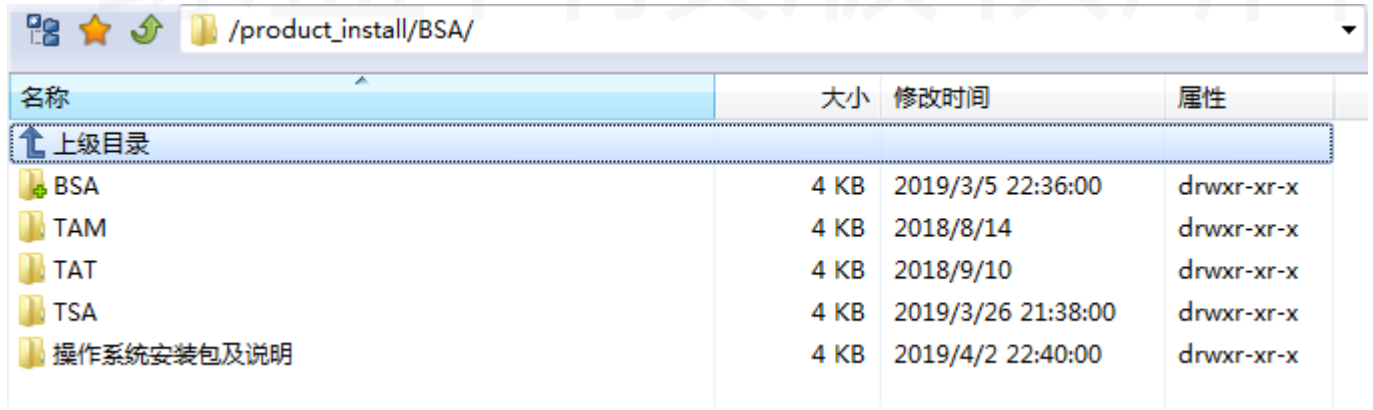
NSFOCUS

请前往工程FTP获取材料

材料获取

BSA系列产品安装包路径在install中，SP包及部分手册及漏洞修复方案均在upgrade中





材料获取

/upgrade/BSA/

名称	大小	修改时间	属性
上级目录			
A.工程武道会	4 KB	2018/10/15 13:25:00	drwxr-xr-x
BSA	4 KB	2018/6/8	drwxr-xr-x
TAM	4 KB	2018/9/10 11:37:00	drwxr-xr-x
TAT	4 KB	2018/6/7	drwxr-xr-x
TSA	4 KB	2018/6/7	drwxr-xr-x
安装部署快速指南（一本通）	4 KB	2018/6/8	drwxr-xr-x
系统漏洞修复方案	4 KB	2018/8/21 11:01:00	drwxr-xr-x

/upgrade/BSA/BSA/4.技术文档/培训手册/

名称	大小	修改时间	属
上级目录			
2.BSA进阶培训.pptx	4.33 MB	2017/11/10	-r
4.第三方日志数据源接入BSA培训.pptx	1.32 MB	2017/5/3	-r
2018-12-27-《BSA运维介绍》.avi	252.08 MB	2018/12/28 13:55:00	-r
2019-03-12-《BSA F05产品培训》.mp4	53.03 MB	2019/3/20 10:00:00	-r
BSA F04培训.pptx	3.98 MB	2018/6/29	-r
BSA F05培训.pptx	2.55 MB	2019/3/11 17:52:00	-r
BSA运维介绍.pptx	6.46 MB	2018/12/27 16:06:00	-r
SOP-BSA售后培训.pptx	6.69 MB	2018/7/19	-r
北京培训-BSA.pptx	9.66 MB	2018/8/16	-r
西安培训-BSA.pptx	3.83 MB	2018/5/26	-r
重庆培训-BSA.pptx	10.77 MB	2018/8/17	-r

/upgrade/BSA/TAM/3.技术文档/常用配置手册/

名称	大小	修改时间	属性
上级目录			
全流量的安装部署checklist(2019.4.2)	4 KB	2019/4/4 21:25:00	drwxr-xr-x
PVD-TAM-V2.0R00F00-ReleaseNotes版本更新说明.doc	231 KB	2018/7/23	-rw-r--r--
PVD-TAM-V2.0R00F00SP01-ReleaseNotes版本更新说明.doc	249 KB	2018/9/5	-rw-r--r--
PVD-TAM-V2.0R00F00SP02-ReleaseNotes版本更新说明.doc	211 KB	2018/12/11 15:33:00	-rw-r--r--
PVD-TAM-V2.0R00F00SP03-ReleaseNotes版本更新说明.doc	165 KB	2019/3/7 10:32:00	-rw-r--r--
绿盟全流量威胁分析系统安装配置手册-V2.0R00F00.pdf	1.33 MB	2018/7/23	-rw-r--r--
绿盟全流量威胁分析系统安装配置手册-V2.0R00F00SP01.pdf	1.11 MB	2018/9/4	-rw-r--r--
绿盟全流量威胁分析系统安装配置手册-V2.0R00F00SP02.pdf	1.06 MB	2018/11/23 15:17:00	-rw-r--r--
绿盟全流量威胁分析系统用户手册-V2.0R00F00.pdf	5.82 MB	2018/7/23	-rw-r--r--
绿盟全流量威胁分析系统用户手册-V2.0R00F00SP01.pdf	6.07 MB	2018/9/4	-rw-r--r--
绿盟全流量威胁分析系统用户手册-V2.0R00F00SP02.pdf	6.26 MB	2018/11/23 15:28:00	-rw-r--r--
绿盟全流量威胁分析系统证书制作说明-V2.0R00F00SP02.pdf	965 KB	2018/11/23 15:20:00	-rw-r--r--
全流量安装部署checklist（公司白牌服务器版本).xlsx	15 KB	2019/4/2 16:32:00	-rw-r--r--
全流量部署 - 服务器数量评估文档.xlsx	20 KB	2018/7/24	-rw-r--r--

部署操作系统

配置要求

需求类型		推荐配置
硬件	CPU	2 个 E5-2640 v3 2.60GHz 8 Core 及以上
	内存	128GB ECC DDR3
	硬盘	• 2 块 1T 的 ssd 盘：建议配置 raid1，用来部署操作系统和 BSA 管理节点服务。集群部署时只需要管理节点部署两块 ssd 盘，工作节点不需要。 • 8~24 块 1.2T 的硬盘：建议每一块均配置成 raid0 盘或 no-raid 盘，用来部署 BSA 的组件，例如 hadoop 或 kafka 等。 说明 服务器磁盘不能配置为 raid5 格式或者 LVM 方式。
	光驱	内置光驱
	网卡	1 块 Broadcom 5720 QP 1Gb 网络子卡、1 块 Broadcom 5719 PCIE Gb 网卡
	Raid 卡	推荐使用带有读写缓存的 raid 卡：例如 PERC H710p
	电源	热插拔冗余电源（1+1）1100 瓦

软件	操作系统	仅支持 64 位操作系统： • Red Hat Enterprise Linux 6.5（注册过的） • CentOS 6.5/7.x 推荐使用操作系统： • CentOS 7.3 说明 ✓ 在安装前，请确认主机中只有新的操作系统、未安装多余软件，否则会导致 BSA 安装失败。 ✓ 安装操作系统时，需要选择安装 software development workstation 版本，否则会由于缺少依赖库，导致 BSA 安装失败。
	依赖库	已经安装如下库： • cyrus-sasl
		• cyrus-sasl-plain • libxml2 • libxslt • fontconfig • python2.6 或者 python2.7 • java1.7 及其以上版本 说明 • 若未安装依赖库，BSA 在安装管理节点时，会给出提示。在操作系统中可以执行 yum install cyrus-sasl，安装 cyrus-sasl 库。其他依赖库的安装与 cyrus-sasl 库类似，这里不重复介绍了。

配置要求

【基础功能模块】

1.数据接入和存储。包括流量日志，uts告警日志以及uts还原出来的文件。对应后台的高性能解析器，普通解析器，session日志入库，http日志入库，dns日志入库，普通入库job。

2.流量统计分析。对应后台的实时统计引擎。

3.内置场景检测。对应后台的恶意样本检测，uts告警日志检测，告警增强，告警入库，事件归并引擎。

4.重点事件、失陷资产、攻击者画像检测、查询和展示。对应后台的失陷资产、攻击者画像检测进程。

5.挖掘检索。包括事件、告警、流量日志的查询和展示。对应后台的thrift server进程。

【全部功能模块】

1、增加威胁情报联动功能。包括情报实时关联分析和回溯检测分析。

2、增加机器学习检测功能。包括蠕虫传播、dns隐蔽信道、僵尸网络、webshell访问检测模型。

3、自定义检测场景。包括自定义的实时和离线检测场景。

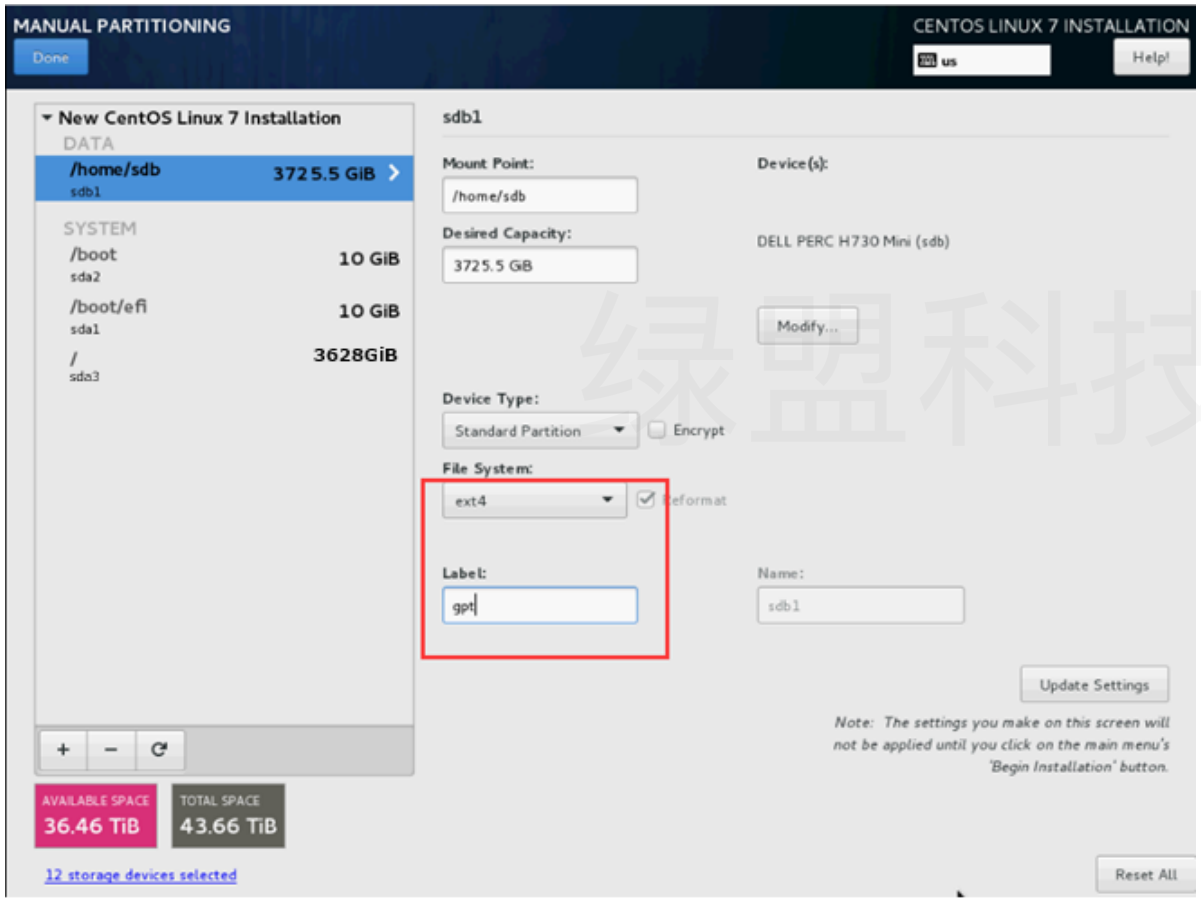
【单机场景】

单机场景只支持40核，128G内存，12*4TB的服务器，只支持跑基础功能模块，只能保留30天的数据。

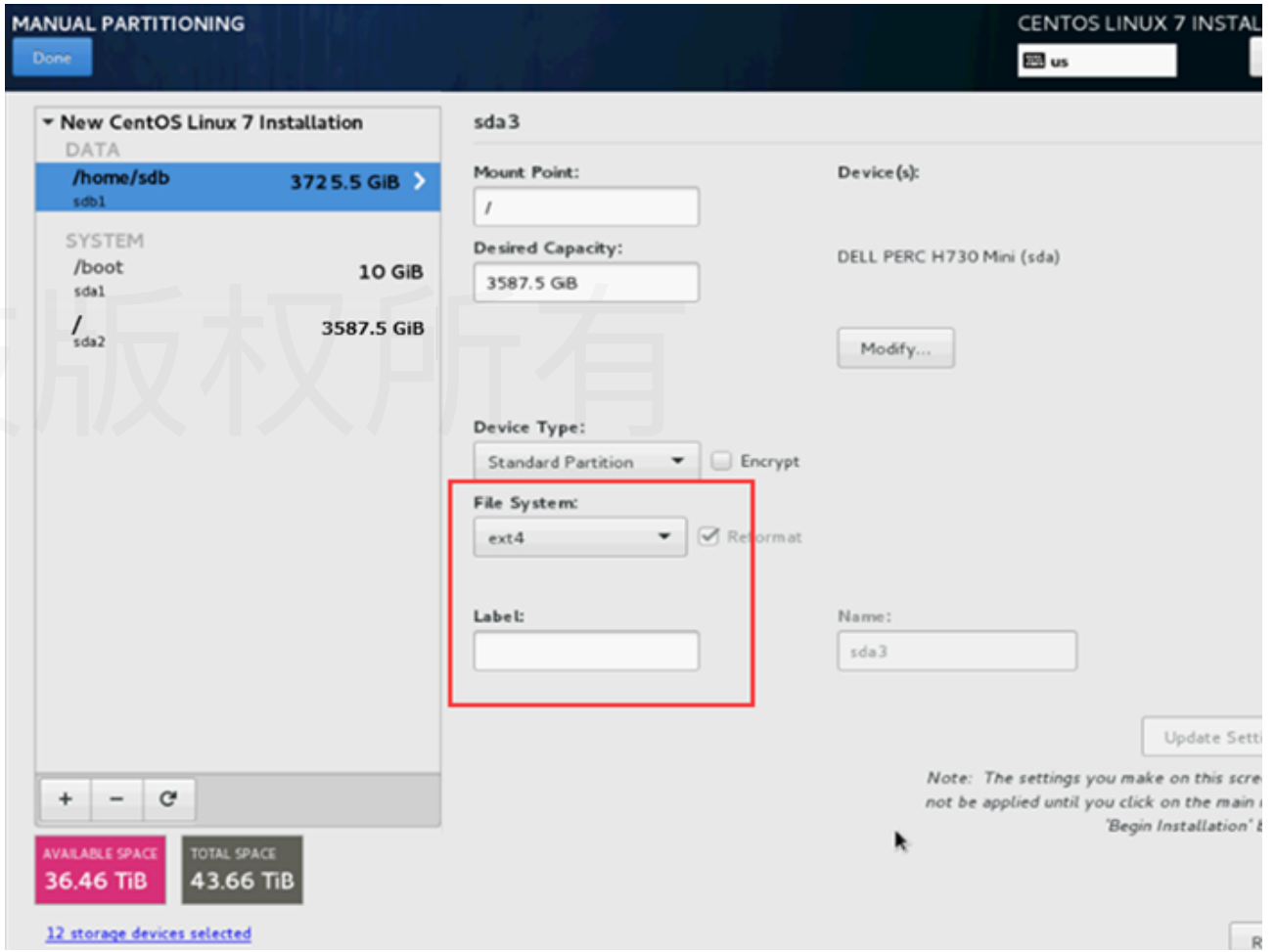
用户输入区(黄色区域)		
功能场景	基础功能模块	
带宽大小(Gbps)	5	
数据保留时间（天）	30	
服务器配置		
CPU(线程数)	40	
内存（GB）	128	最低128GB，大于>=5Gbps的流量，建议使用256G内存的服务器。
磁盘（TB，可用空间）：	4	
数据盘数量（块）：	12	
计算结果		
需要的服务器的数量(台)	4	集群规模》=7台时，单独拿一台机器作为集群管理节点。

操作系统分区

UEFI模式分区



BIOS模式分区



具体详情请参考手册

NSFOCUS

操作系统分区

错误的

```
[root@bsa204 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda5        46G  8.0G   36G  19% /
devtmpfs        126G     0  126G   0% /dev
tmpfs           126G  104K  126G   1% /dev/shm
tmpfs           126G  4.1G  122G   4% /run
tmpfs           126G     0  126G   0% /sys/fs/cgroup
/dev/sda1       9.2G  160M  8.6G   2% /boot
/dev/sda2        82G   71G  7.3G  91% /home
/dev/sdd1       1.5T  1.9G  1.4T   1% /home/sdd
/dev/sdc1        15T  1.7G   14T   1% /home/sdc
/dev/sda6        46G   65M   44G   1% /tmp
/dev/sdb1        15T  6.0G   14T   1% /home/sdb
/dev/sde        7.2G   62M  6.8G   1% /run/media/nsfocus/1678bbd1-c429-462e-af45-c
tmpfs            26G   16K   26G   1% /run/user/42
tmpfs            26G     0   26G   0% /run/user/0
tmpfs            26G     0   26G   0% /run/user/987
tmpfs            26G     0   26G   0% /run/user/986
```

正确的

```
[root@bsa211 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda4       3.4T  3.9G  3.2T   1% /
devtmpfs         63G     0   63G   0% /dev
tmpfs            63G   80K   63G   1% /dev/shm
tmpfs            63G   11M   63G   1% /run
tmpfs            63G     0   63G   0% /sys/fs/cgroup
/dev/sda2       9.8G  154M  9.1G   2% /boot
/dev/sda1        10G  9.6M   10G   1% /boot/efi
/dev/sde1       3.6T   89M  3.4T   1% /home/sde
/dev/sdl1       3.6T   89M  3.4T   1% /home/sdl
/dev/sdf1       3.6T   89M  3.4T   1% /home/sdf
/dev/sdh1       3.6T   89M  3.4T   1% /home/sdh
/dev/sdk1       3.6T   89M  3.4T   1% /home/sdk
/dev/sdg1       3.6T   89M  3.4T   1% /home/sdg
/dev/sdb1       3.6T   89M  3.4T   1% /home/sdb
/dev/sdd1       3.6T   89M  3.4T   1% /home/sdd
/dev/sdi1       3.6T   89M  3.4T   1% /home/sdi
/dev/sdc1       3.6T   89M  3.4T   1% /home/sdc
/dev/sdj1       3.6T   89M  3.4T   1% /home/sdj
tmpfs            13G   16K   13G   1% /run/user/988
tmpfs            13G     0   13G   0% /run/user/0
[root@bsa211 ~]#
```

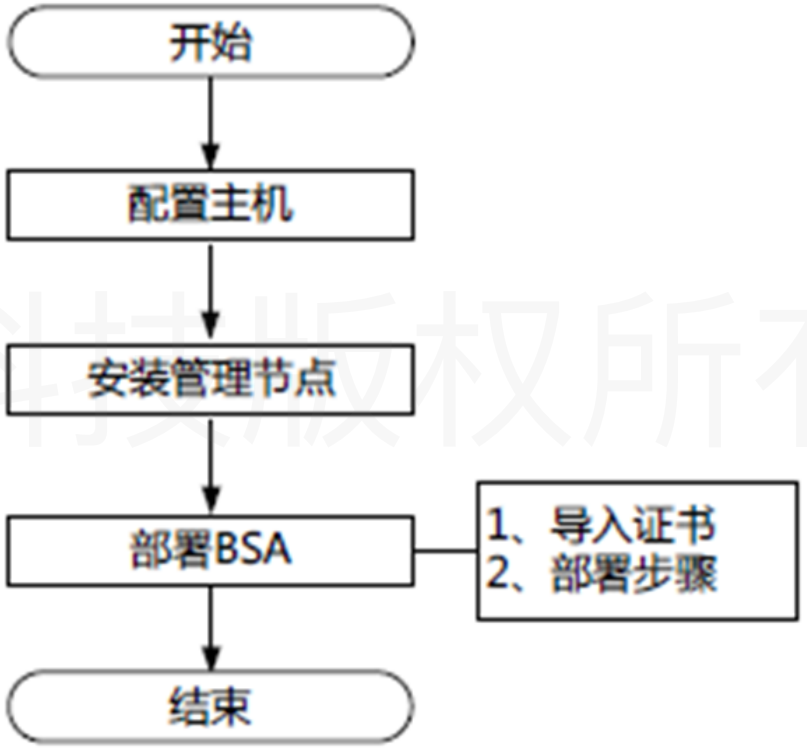
安装前注意事项

- 防火墙要保持开启，不要使用iptables –F
- /home；时间，时区；Ip，主机名唯一
- BSA F04主机名唯一，可通过界面更改ip
- 磁盘挂载尽量按照/home/sdb、/home/sdc目录挂载，方便进行分盘部署。
- /etc/hosts文件和prepareTools/hosts文件前两行不要删
- prepareTools/hosts末尾不要有空行
- 由于centos7.0本身内核存在缺陷会影响平台稳定性，不再使用centos7.0

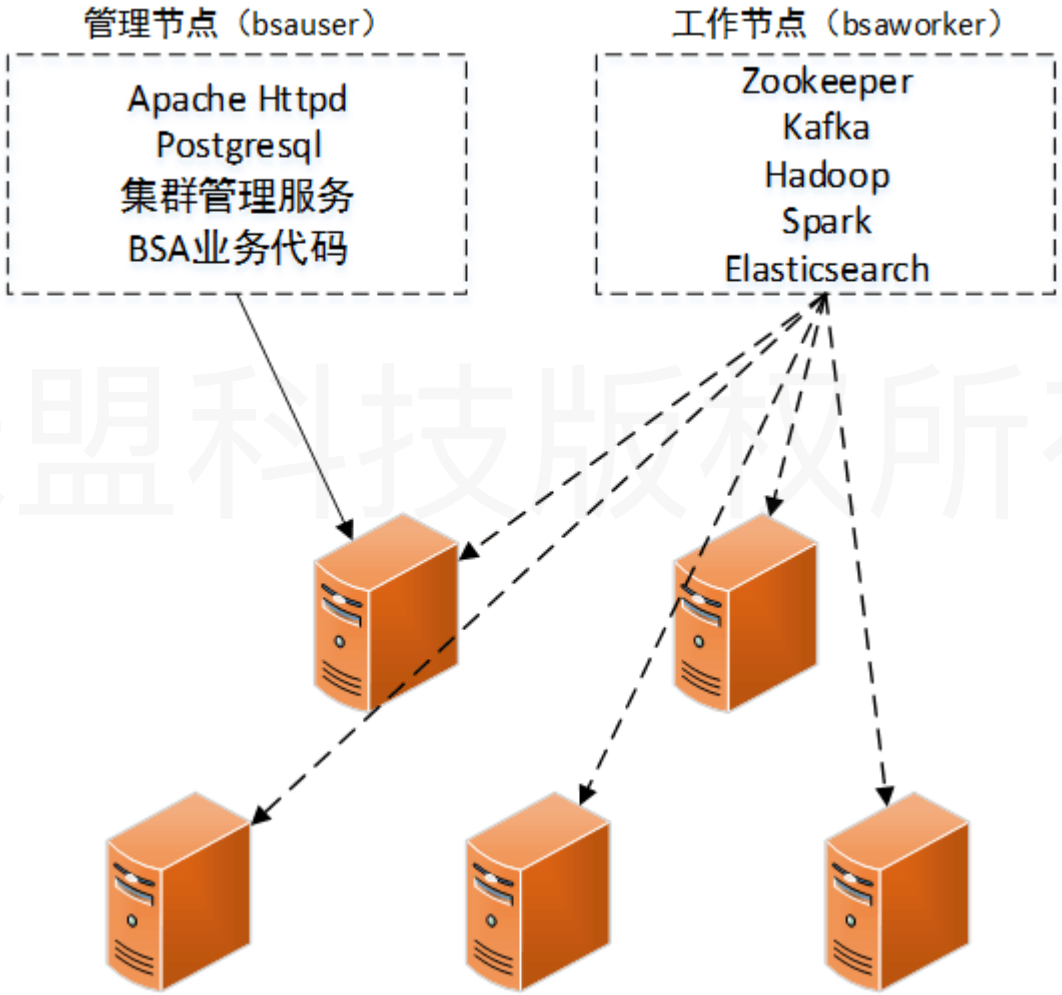
准备项		描述
节点所在主机	IP 地址	确保网络连接正常。各节点所在主机处于同一个网段。
	操作系统登录帐号	必须具有 root 帐号权限。
	防火墙	处于开启状态。
	时间	所有节点的系统时间要保持同步。
	主机名	所有节点需要统一规范命名。
	hosts 文件	每个节点需要添加管理节点和所有工作节点的 IP、主机名。
	bsauser 帐号（管理节点）	安装前不允许存在 bsauser 帐号及/home/bsauser 目录，在安装管理节点时，会自动创建 bsauser 帐号。
	其他	已经开启 Yum、RPM、SSH。
	组件状态	• 停止已经运行的 Hadoop、Kafka、Zookeeper、Elasticsearch、Postgres SQL、Spark、Apache、Tomcat 组件。 • 确保 BSA 所需端口未被占用。
BSA	证书	• 与加密狗配套使用。 • 证书中包含授权节点数。
	加密狗	• 与证书配套使用。 • 安装在管理节点所在主机上。
	光盘	包含 BSA 管理节点的安装文件。
访问 BSA 的主机	浏览器	• IE 11 • 最新版本的 Firefox 或 Chrome

NSFOCUS

安装部署流程



管理节点和工作节点



组件部署

表3-2 Hadoop 组件路径参数

配置项	描述
NameNode Path	NameNode 数据的存放路径，支持分盘部署，即除了操作系统磁盘以外，其他所有磁盘都可以存放 NameNode 数据，建议将 NameNode 部署在 2~3 块磁盘上。此时，NameNode Path 可以配置多个，中间用英文“,”分隔。 例如，服务器有/home/sdd 和/home/sdc 两个可用磁盘，则 Namenode Path 输入框输入“/home/sdd/hes/hadoopDirs/name,/home/sdc/hes/hadoopDirs/name”。
DataNode Path	DataNode 数据的存放路径，支持分盘部署，即除了操作系统磁盘以外，其他所有磁盘都可以存放 DataNode 数据。此时，DataNode Path 可以配置多个，中间用英文“,”分隔。 例如，服务器有/home/sdd 和/home/sdc 两个可用磁盘，则 Datanode Path 输入框输入“/home/sdd/hes/hadoopDirs/data,/home/sdc/hes/hadoopDirs /data”。
Hadoop Temp Path	Hadoop 临时文件存放路径。
Yarn Local Path	Yarn 中间结果的存放路径，支持分盘部署，即除了操作系统磁盘以外，其他所有磁盘都可以存放 Yarn 中间结果数据。此时，该参数可以配置多个，中间用英文“,”分隔。 例如，服务器有/home/sdd 和/home/sdc 两个可用磁盘，则该参数的输入框输入“/home/sdd/hes/hadoopDirs/nm-local-dir,/home/sdc/hes/hadoopDirs/nm-local-dir”。

组件部署

组件设置

全选	组件	配置	主机
☑	Hadoop	保存 取消	选择主机
NameNode Path	/home/sdb/hes/hadoopDirs/name,/hoı	多路径请用逗号分隔	
DataNode Path	/home/sdf/hes/hadoopDirs/data,/hom	多路径请用逗号分隔	
Hadoop Temp Path	/home/bsaworker/hes/hadoopDirs/hac		
Yarn Local Path	/home/sdf/hes/hadoopDirs/nm-local-di	多路径请用逗号分隔	
☑	Zookeeper	编辑	选择主机
☑	Kafka	编辑	选择主机
☑	Spark	编辑	选择主机
☑	Elasticsearch	编辑	选择主机

部署

TAM APP

全流量场景

- 5个APP安装完整，F00SP03安装完内置数据源后需要选择单机场景或集群场景部署

序号	APP名称	APP详细描述	APP MD5
TAM APP			
1	威胁情报APP	bsa_ti.3.0.0.25443	772f82319005527061254f535ad61344
2	资产管理APP	bsa_am.2.1.3.25582	2d23de11b8d3c285e56621da4ff75d17
3	数据源APP	bsa_tds.2.0.2.30231	96845998740c1741f05341a7877421b3
4	诺亚引擎APP	bsa_mlengine.2.0.1.27818	9336BE36A12EC2A451B5A8549273CF27
5	全流量APP	bsa_tam2.2.0.3.29845	72f86d6829bc1ed0b23661d626409dbe
TSA APP			
1	网络入侵APP	bsa_ckc.2.1.0.29270	5AE7194623995BCB61A38BD06FAB2214
2	规则引擎APP	bsa_rule_engine.2.2.0.30018	F5E4C4EEAF0AB2E7F6F479A8812BB144
3	态势感知APP	bsa_tsa.2.2.0.29986	A921B9EFA4DCB582C30D979B5EE0A22E
4	网站安全APP	bsa_wss.2.1.0.29776	C88E6CC1EDBC0137498CD581ED9D78DA
5	僵木蠕APP	bsa_zsa.2.1.0.29667	235E5607AFAB140DC81F4E0A38ED5785
6	威胁情报APP	bsa_ti.3.0.0.25443	772F82319005527061254F535AD61344
7	资产管理APP	bsa_am.2.1.4.29961	E0776C65744E9F4311913A8F84E4E0D3
8	异常流量APP	bsa_ata.2.2.0.29271	84369D169C9CF7068CFA4EA00999171C
9	内置数据源APP	bsa_cds.2.1.0.29578	113D76B836D0AF93A937DCE1039BDD0C
10	一键封堵APP	bsa_okp.2.0.1.29913	96AAAC8575D659CDB4379A2F14055D42

数据接入

支持的设备版本

TAM F00SP03

支持设备	设备引擎版本
UTS	V2.0R00F00
TAC	V2.0R02F00 及以上版本
NTI	V4.0R00F00

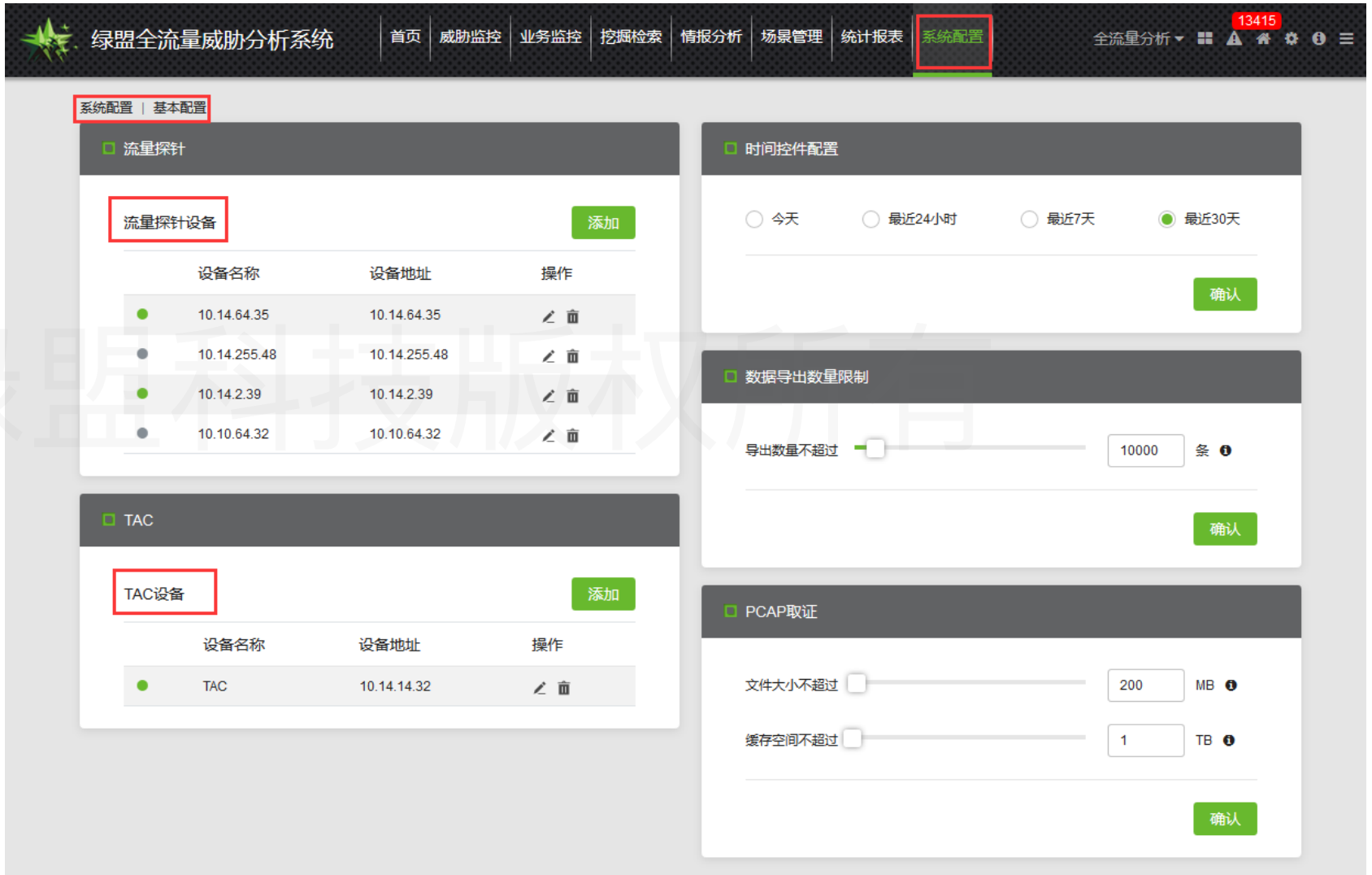
需要开放的端口

方向：入BSA方向

	端口	端口用途
BSA平台	443	BSAweb服务
	自定义数据源端口	数据源接收数据端口
A接口	5050	SFTP服务默认端口
	5051	FTP服务默认端口
	60000-60200	FTP服务数据端口
转发器	12306	转发器web访问端口
	12307	转发器服务端口
	5002	TCP端口
	5003	SSL端口
	50071	FTP服务端口
	60000-60200	FTP服务数据端口
态势感知	1111	异常流量数据源端口
	5005	网络入侵数据源端口
	5666	waf数据源端口
攻击溯源	异常流量数据源端口	异常流量数据源端口
	flow采集器端口	flow采集器端口
全流量	5008	会话日志数据源端口
	5009	DNS日志数据源端口
	5010	web日志数据源端口
	5011	其他流量日志数据源端口
	5012	UTS告警数据源端口
UTS	22	ssh端口
	443	web服务
	8081	restapi http

TAM联动UTS，TAC

- PCAP包取证，TAM需要配置UTS，TAM去UTS调取数据，UTS实时存储数据包至本地，磁盘越大存储越多；如果UTS磁盘空间已满，会自动覆盖最老的数据
- 针对文件，TAM先检测本地缓存，再匹配情报，未命中发给TAC



03

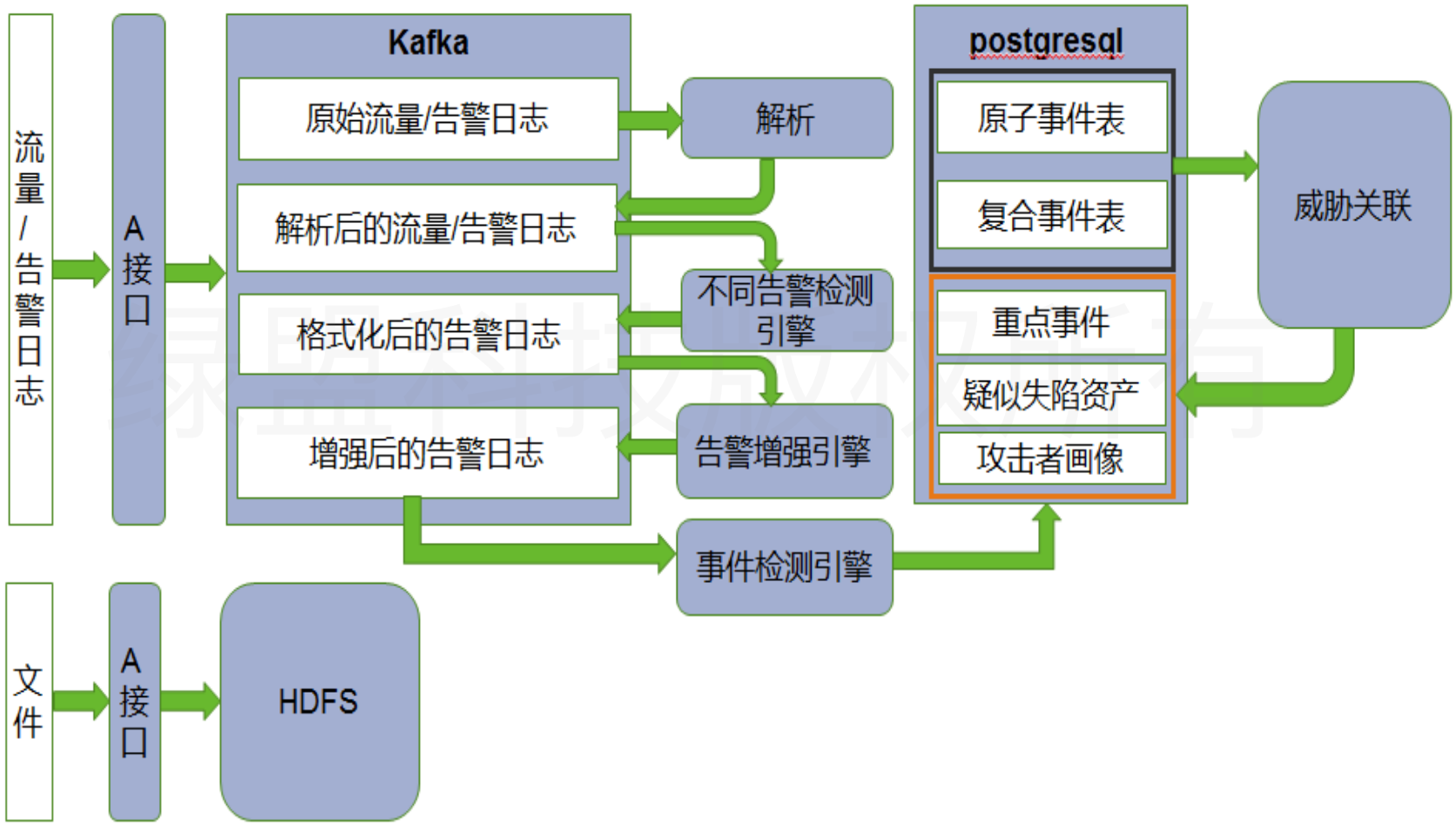
查询分析

全流量TAM

TAM

TAM的首页以列表、概览以及分布图的方式展示基础流量数据、威胁检测结果和威胁关联结果，而且，通过首页的相应链接，用户可以快速跳转至相应的菜单栏，查看更为详细的监控数据，或者对事件进行处理。

TAM数据展示流程


流量/告警日志
A接口
Kafka
原始流量/告警日志
解析后的流量/告警日志
格式化后的告警日志
增强后的告警日志
解析
不同告警检测引擎
告警增强引擎
事件检测引擎
postgresql
原子事件表
复合事件表
重点事件
疑似失陷资产
攻击者画像
威胁关联
文件
A接口
HDFS

TAM重点事件

TAM 展示及产生重点事件：

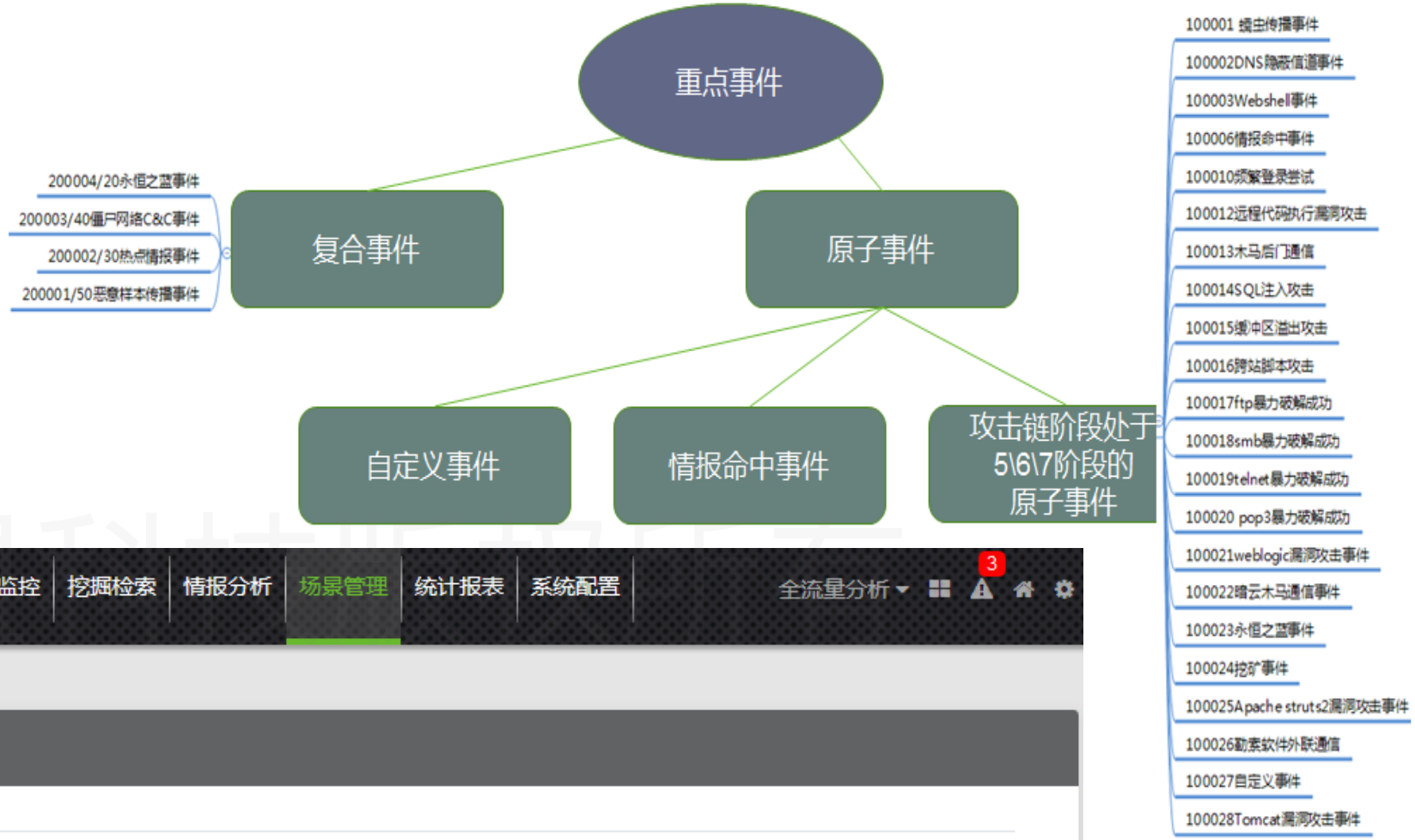
1. UTS 端要配置与 TAM 联动（接收原始日志和告警日志外，如果还需下钻存储在 UTS 上的原始数据包，需要在 TAM 也添加 UTS 地址，否则无需配置）。

2. UTS 产生原始日志及告警日志，并成功传送至 TAM

3. TAM 成功完成接收—解析—格式化—增强—事件每一步流程。

4. 满足场景管理中的内置规则，并且该规则已启用；符合复合事件或符合原子事件中的特定定义的属于重点事件；否则属于一般事件，在挖掘检索中查看的事件日志属于重点+一般事件，首页展示的均为重点事件。

TAM重点事件

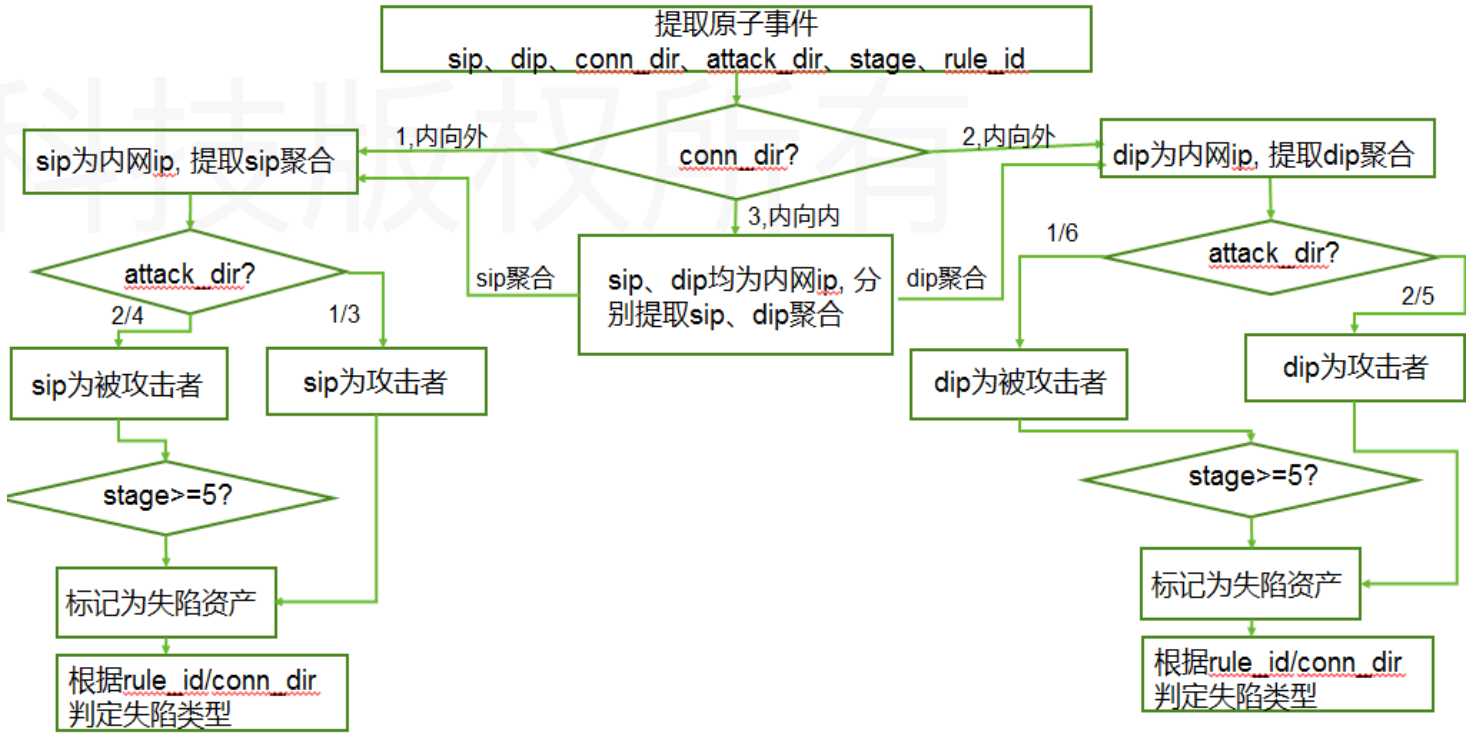


NSFOCUS

TAM疑似失陷资产

TAM 展示及产生疑似失陷资产：

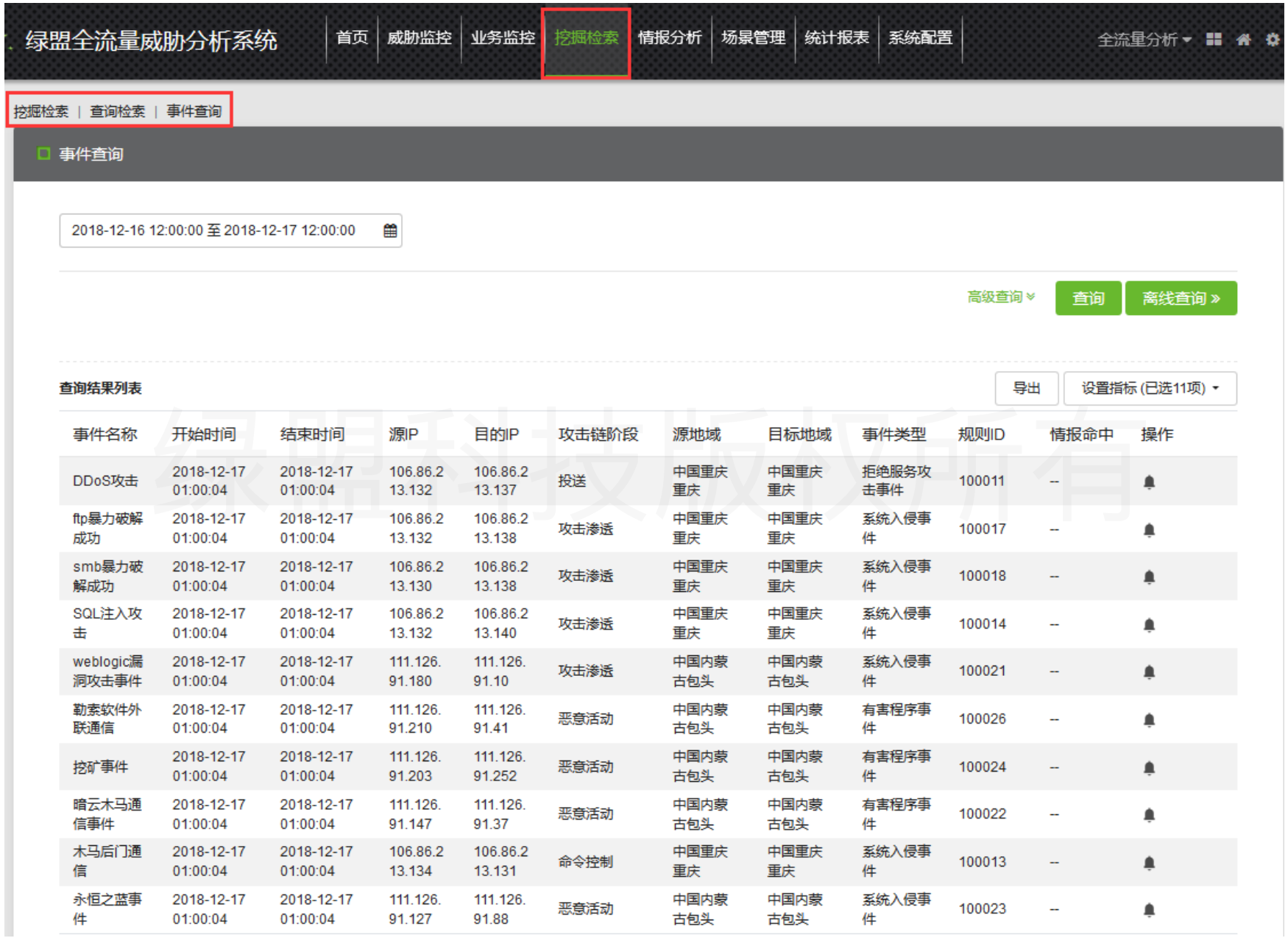
1. UTS 上配置资产范围是不是内网，如果不配置 TAM 首页无法展示疑似失陷资产
2. TAM 的资产管理配置资产，意义在于丰富资产的信息（不是必须）
3. 判断资产是否失陷，遵循以下原则

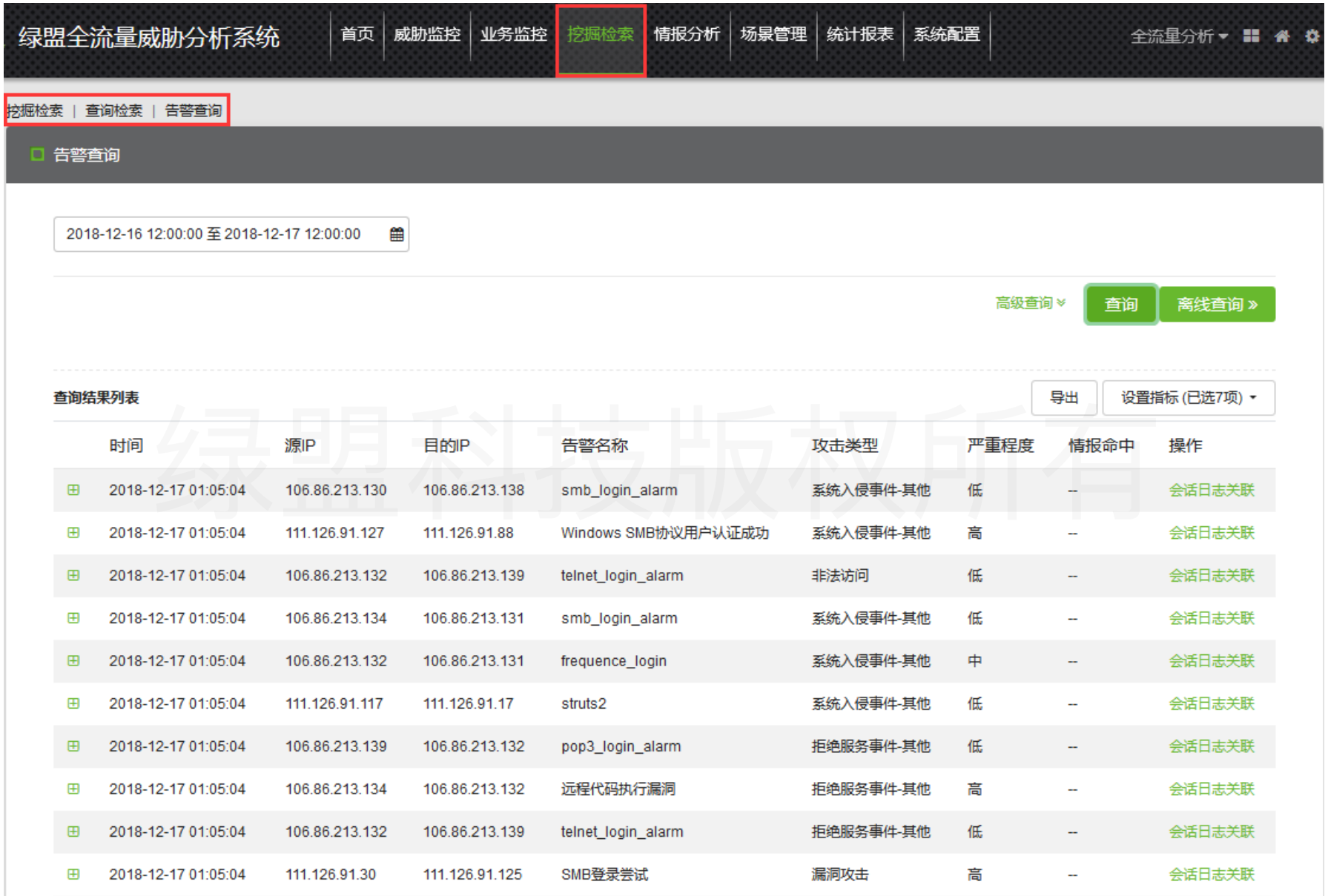


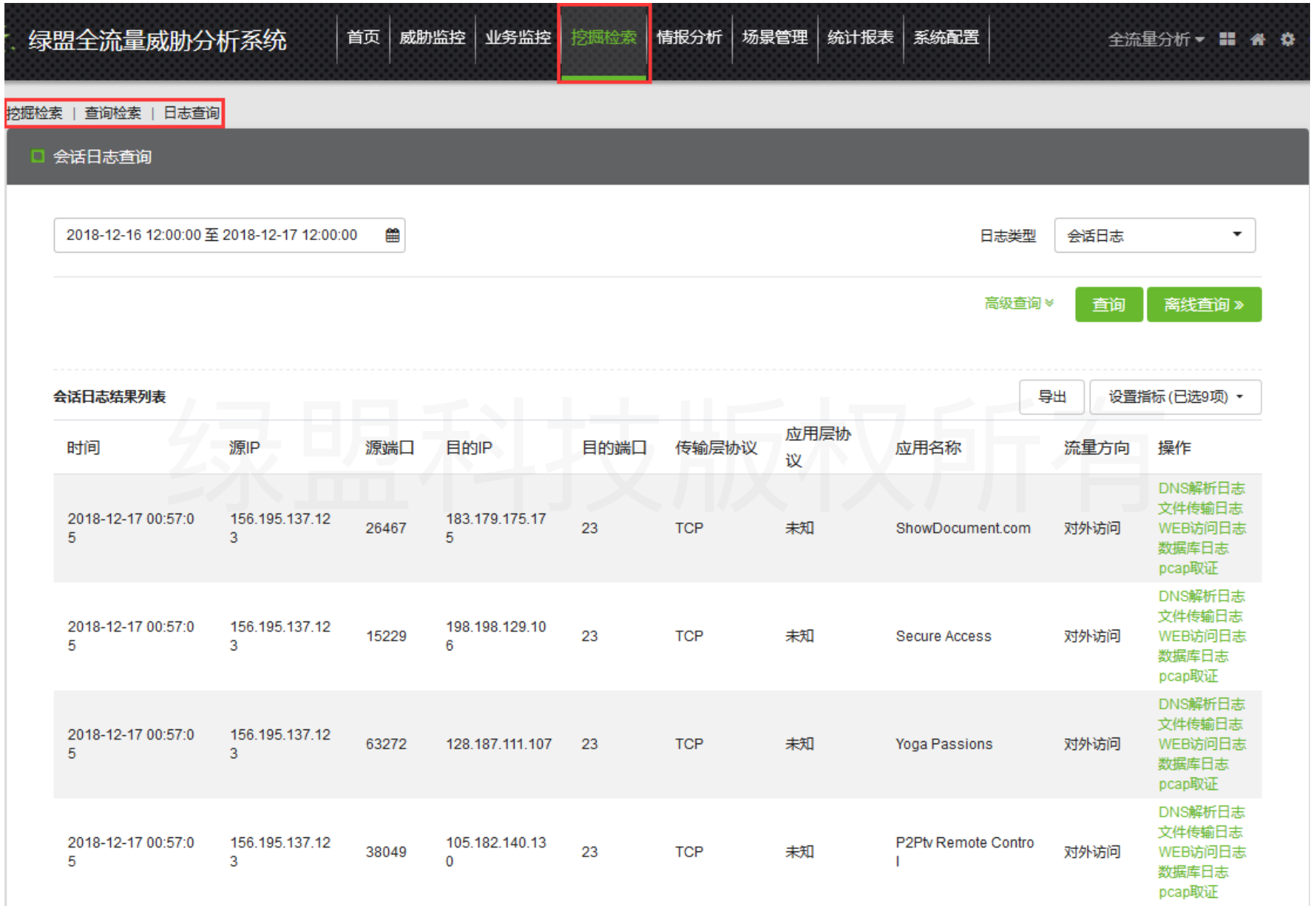
TAM攻击者画像

TAM 展示及产生攻击者画像：

1. 基于事件提取出攻击者，对该攻击者的一系列攻击事件根据攻击目标和事件类型进行聚合，提炼出攻击过程；目前只从告警日志和事件日志中提取，后续版本可能会在从原始日志中提取进行优化。
2. 结合 IP 地理库，提取该攻击者的地理位置；（非必须）
3. 再结合情报详情信息，获取该攻击者的其他背景信息丰富画像。（非必须）


绿盟全流量威胁分析系统
首页
威胁监控
业务监控
挖掘检索
情报分析
场景管理
统计报表
系统配置
全流量分析
挖掘检索 | 查询检索 | 事件查询
事件查询
2018-12-16 12:00:00 至 2018-12-17 12:00:00
高级查询
查询
离线查询 »
查询结果列表
导出
设置指标 (已选11项)
事件名称 开始时间 结束时间 源IP 目的IP 攻击链阶段 源地域 目标地域 事件类型 规则ID 情报命中 操作
DDoS攻击 2018-12-17 01:00:04 2018-12-17 01:00:04 106.86.213.132 106.86.213.137 投送 中国重庆 重庆 中国重庆 重庆 拒绝服务攻击事件 100011 --
ftp暴力破解成功 2018-12-17 01:00:04 2018-12-17 01:00:04 106.86.213.132 106.86.213.138 攻击渗透 中国重庆 重庆 中国重庆 重庆 系统入侵事件 100017 --
smb暴力破解成功 2018-12-17 01:00:04 2018-12-17 01:00:04 106.86.213.130 106.86.213.138 攻击渗透 中国重庆 重庆 中国重庆 重庆 系统入侵事件 100018 --
SQL注入攻击 2018-12-17 01:00:04 2018-12-17 01:00:04 106.86.213.132 106.86.213.140 攻击渗透 中国重庆 重庆 中国重庆 重庆 系统入侵事件 100014 --
weblogic漏洞攻击事件 2018-12-17 01:00:04 2018-12-17 01:00:04 111.126.91.180 111.126.91.10 攻击渗透 中国内蒙古包头 中国内蒙古包头 系统入侵事件 100021 --
勒索软件外联通信 2018-12-17 01:00:04 2018-12-17 01:00:04 111.126.91.210 111.126.91.41 恶意活动 中国内蒙古包头 中国内蒙古包头 有害程序事件 100026 --
挖矿事件 2018-12-17 01:00:04 2018-12-17 01:00:04 111.126.91.203 111.126.91.252 恶意活动 中国内蒙古包头 中国内蒙古包头 有害程序事件 100024 --
暗云木马通信事件 2018-12-17 01:00:04 2018-12-17 01:00:04 111.126.91.147 111.126.91.37 恶意活动 中国内蒙古包头 中国内蒙古包头 有害程序事件 100022 --
木马后门通信 2018-12-17 01:00:04 2018-12-17 01:00:04 106.86.213.134 106.86.213.131 命令控制 中国重庆 重庆 中国重庆 重庆 系统入侵事件 100013 --
永恒之蓝事件 2018-12-17 01:00:04 2018-12-17 01:00:04 111.126.91.127 111.126.91.88 恶意活动 中国内蒙古包头 中国内蒙古包头 系统入侵事件 100023 --


绿盟全流量威胁分析系统
首页
威胁监控
业务监控
挖掘检索
情报分析
场景管理
统计报表
系统配置
全流量分析
挖掘检索 | 查询检索 | 告警查询
告警查询
2018-12-16 12:00:00 至 2018-12-17 12:00:00
高级查询
查询
离线查询 »
查询结果列表
导出
设置指标 (已选7项)
时间 源IP 目的IP 告警名称 攻击类型 严重程度 情报命中 操作
2018-12-17 01:05:04 106.86.213.130 106.86.213.138 smb_login_alarm 系统入侵事件-其他 低 -- 会话日志关联
2018-12-17 01:05:04 111.126.91.127 111.126.91.88 Windows SMB协议用户认证成功 系统入侵事件-其他 高 -- 会话日志关联
2018-12-17 01:05:04 106.86.213.132 106.86.213.139 telnet_login_alarm 非法访问 低 -- 会话日志关联
2018-12-17 01:05:04 106.86.213.134 106.86.213.131 smb_login_alarm 系统入侵事件-其他 低 -- 会话日志关联
2018-12-17 01:05:04 106.86.213.132 106.86.213.131 frequence_login 系统入侵事件-其他 中 -- 会话日志关联
2018-12-17 01:05:04 111.126.91.117 111.126.91.17 struts2 系统入侵事件-其他 低 -- 会话日志关联
2018-12-17 01:05:04 106.86.213.139 106.86.213.132 pop3_login_alarm 拒绝服务事件-其他 低 -- 会话日志关联
2018-12-17 01:05:04 106.86.213.134 106.86.213.132 远程代码执行漏洞 拒绝服务事件-其他 高 -- 会话日志关联
2018-12-17 01:05:04 106.86.213.132 106.86.213.139 telnet_login_alarm 拒绝服务事件-其他 低 -- 会话日志关联
2018-12-17 01:05:04 111.126.91.30 111.126.91.125 SMB登录尝试 漏洞攻击 高 -- 会话日志关联


绿盟全流量威胁分析系统
首页
威胁监控
业务监控
挖掘检索
情报分析
场景管理
统计报表
系统配置
全流量分析
挖掘检索 | 查询检索 | 日志查询
会话日志查询
2018-12-16 12:00:00 至 2018-12-17 12:00:00
日志类型
会话日志
高级查询
查询
离线查询 »
会话日志结果列表
导出
设置指标 (已选9项)
时间 源IP 源端口 目的IP 目的端口 传输层协议 应用层协议 应用名称 流量方向 操作
2018-12-17 00:57:05 156.195.137.123 26467 183.179.175.175 23 TCP 未知 ShowDocument.com 对外访问 DNS解析日志 文件传输日志 WEB访问日志 数据库日志 pcap取证
2018-12-17 00:57:05 156.195.137.123 15229 198.198.129.106 23 TCP 未知 Secure Access 对外访问 DNS解析日志 文件传输日志 WEB访问日志 数据库日志 pcap取证
2018-12-17 00:57:05 156.195.137.123 63272 128.187.111.107 23 TCP 未知 Yoga Passions 对外访问 DNS解析日志 文件传输日志 WEB访问日志 数据库日志 pcap取证
2018-12-17 00:57:05 156.195.137.123 38049 105.182.140.130 23 TCP 未知 P2Ptv Remote Control 对外访问 DNS解析日志 文件传输日志 WEB访问日志 数据库日志 pcap取证

系统状态

日常运维

- 关注的后台:

df -h查看硬盘空间；
free -g查看内存空间；
date -R查看时区及时间；
hostname及hostname -i查看主机和ip是否唯一;
top 查看CPU是否正常；
iotop 查看IO是否正常；

日常运维

关注的前台

在设置-集群管理-组件下查看查看当前组件的运行状态，确定所有组件运行状态正常。

在设置-应用管理下查看所有应用，确定要使用的应用已安装且为启动状态。

在综合态势下查看态势地图、事件类型分布图、资产风险分布图、最新安全事件列表，确定图表都有数据。

在设置-集群管理-全流程监控下查看当前对应的入库情况确认对应的数据源数据入库正常

在风险态势-态势子系统下通过查询分析查找数据，确定TSA能正常接受平台产品的日志数据。

组件状态检查

查看组件是否都正常运行是平台是否正常运行的一个标准，每个组件都对应着不同的功能，平台的正常运行需要保证各组件都是正常运行中；组件页面状态，红色为异常，绿色为正常

还可以查看组件详情
Hadoop ： 除了启用和停组件实例外， 还可以查看Hadoop分布式文件系统 (HDFS) 的节点状态、总块数、丢失块数，查看YARN的节点状态、总CPU核数和CPU已用核数、总内存和已用内存、Job总数和Job挂起数目、Job运行数目和 Job完成数目、各个运行Job的详细信息。

主机状态检查

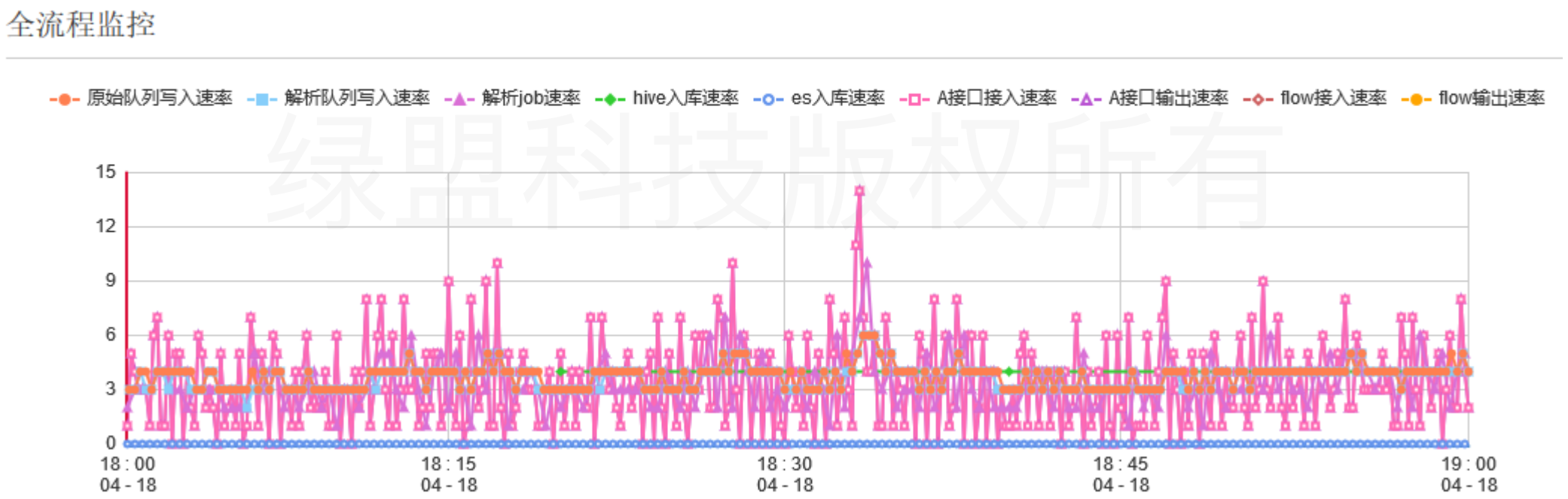
进入相应主机信息展示页面

分别查看主机基本信息、主机CPU（包括该主机的物理CPU以及逻辑CPU的总数）、实例列表、主机内存、主机硬盘容量、主机硬盘IO、主机网络IO、主机负载信息、主机磁盘详情、每块磁盘的IO使用率

全流程监控

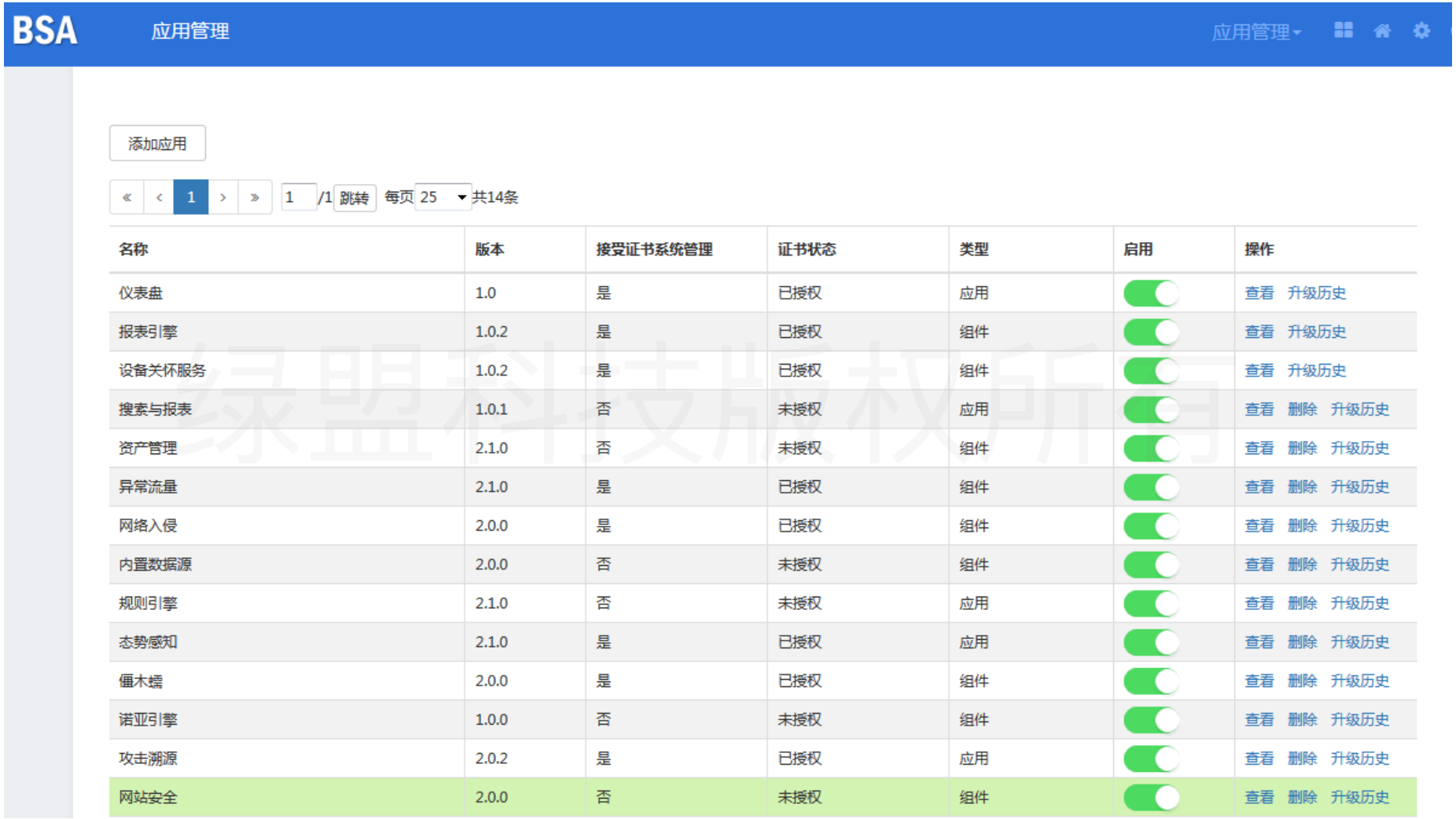
- 集群管理-全流程监控，选择需要查看的数据源

bsaata_tcp



查看指定数据源的全流程监控信息 ，可查看最近一个小时内，该数据源的全流程监控信息，即数据源的各个topic的速度和组件解析速度对应的曲线

各应用启用状态检查

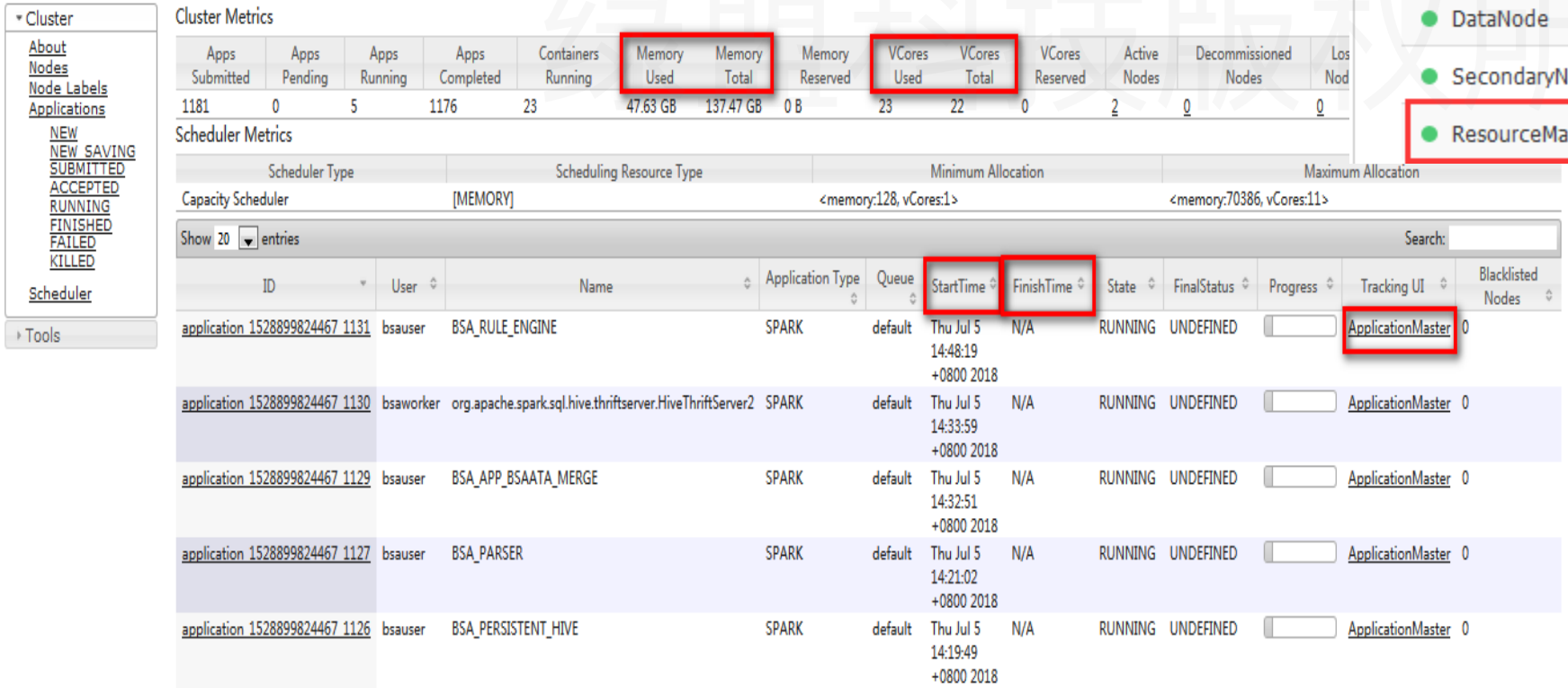


名称	版本	接受证书系统管理	证书状态	类型	启用	操作
仪表盘	1.0	是	已授权	应用		查看 升级历史
报表引擎	1.0.2	是	已授权	组件		查看 升级历史
设备关怀服务	1.0.2	是	已授权	组件		查看 升级历史
搜索与报表	1.0.1	否	未授权	应用		查看 删除 升级历史
资产管理	2.1.0	否	未授权	组件		查看 删除 升级历史
异常流量	2.1.0	是	已授权	组件		查看 删除 升级历史
网络入侵	2.0.0	是	已授权	组件		查看 删除 升级历史
内置数据源	2.0.0	否	未授权	组件		查看 删除 升级历史
规则引擎	2.1.0	否	未授权	应用		查看 删除 升级历史
态势感知	2.1.0	是	已授权	应用		查看 删除 升级历史
僵木蠕	2.0.0	是	已授权	组件		查看 删除 升级历史
诺亚引擎	1.0.0	否	未授权	组件		查看 删除 升级历史
攻击溯源	2.0.2	是	已授权	应用		查看 删除 升级历史
网站安全	2.0.0	否	未授权	组件		查看 删除 升级历史

不同的应用对应着不同的功能模块，如果发现功能模块异常，需要先检查应用是否为启动状态；

Hadoop检查，ip:8088

- 可以查看start time和finish time判断job是否运行；查看内存和核数使用；
- 通过点击ApplicationMaster查看数据是否入库，如果点完无法访问，记得改下URL将hostname改成ip；
- ResourceManager部署在哪个节点，hadoop就在哪个节点。



NSFOCUS

TAM 单机场景

Logged in as: dr.who

RUNNING Applications

- Cluster
  - About
  - Nodes
  - Node Labels
  - Applications
    - NEW
    - NEW_SAVING
    - SUBMITTED
    - ACCEPTED
    - RUNNING
    - FINISHED
    - FAILED
    - KILLED
  - Scheduler
- Tools

Cluster Metrics

Apps Submitted	Apps Pending	Apps Running	Apps Completed	Containers Running	Memory Used	Memory Total	Memory Reserved	VCores Used	VCores Total	VCores Reserved	Active Nodes	Decommissioned Nodes	Lost Nodes	Unhealthy Nodes	Rebooted Nodes
10	0	8	2	38	81.38 GB	94.73 GB	0 B	38	27	0	1	0	0	0	0

Scheduler Metrics

Scheduler Type	Scheduling Resource Type	Minimum Allocation	Maximum Allocation
Capacity Scheduler	[MEMORY]	<memory:128, vCores:1>	<memory:97000, vCores:27>

Show 20 entries Search:

ID	User	Name	Application Type	Queue	StartTime	FinishTime	State	FinalStatus	Progress	Tracking UI	Blacklisted Nodes
application_1545335101808_0017	bsauser	bsa_tam2_UTS_ALARM_FORMAT	SPARK	default	Fri Dec 21 03:54:48 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0016	bsauser	bsa_tam2_ALARM_PERSISTENT_HIVE	SPARK	default	Fri Dec 21 03:54:48 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0015	bsauser	bsa_tam2_EVTMERGE_REALTIME_3	SPARK	default	Fri Dec 21 03:54:46 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0014	bsauser	bsa_tam2_ENHANCE_ALARM	SPARK	default	Fri Dec 21 03:54:44 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0013	bsauser	bsa_tam2_STATISTICS	SPARK	default	Fri Dec 21 03:54:44 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0012	bsauser	BSA_PARSER	SPARK	default	Fri Dec 21 03:49:02 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0011	bsauser	BSA_PERSISTENT_HIVE	SPARK	default	Fri Dec 21 03:47:49 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0
application_1545335101808_0009	bsaworker	org.apache.spark.sql.hive.thriftserver.HiveThriftServer2	SPARK	default	Fri Dec 21 03:45:54 +0800 2018	N/A	RUNNING	UNDEFINED		ApplicationMaster	0

Showing 1 to 8 of 8 entries First Previous 1 Next Last

TAM 集群场景

13+2+1（13是各功能job数量，2是开启诺亚后增加两个job，1是thriftserver查询job）

192.168.100.242:8088/cluster/apps/RUNNING

application_1540257944033_0120	bsauser	bsa_tam2_UTS_ALARM_FORMAT	SPARK	default	Wed Nov 14 15:38:17 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0113	bsauser	BSA_PERSISTENT_HIVE_bsatam_session	SPARK	default	Mon Nov 12 13:43:40 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0112	bsauser	BSA_PARSER_V2	SPARK	default	Mon Nov 12 13:42:53 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0111	bsauser	BSA_PERSISTENT_HIVE	SPARK	default	Mon Nov 12 13:41:52 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0110	bsauser	BSA_PARSER	SPARK	default	Mon Nov 12 13:40:49 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0109	bsauser	bsa_tam2_EVTMERGE_REALTIME_3	SPARK	default	Mon Nov 12 13:26:24 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0108	bsauser	bsa_tam2_EVTMERGE_REALTIME_1	SPARK	default	Mon Nov 12 13:25:34 +0800	N/A	RUNNING	UNDEFINE

TAM 集群场景

192.168.100.242:8088/cluster/apps/RUNNING

application_1540257944033_0107	bsauser	bsa_tam2_STATISTICS	SPARK	default	Mon Nov 12 13:21:19 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0106	bsauser	bsa_tam2_ENHANCE_ALARM	SPARK	default	Mon Nov 12 13:21:01 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0011	bsauser	BSA_PERSISTENT_HIVE_bsatam_dns	SPARK	default	Tue Oct 23 09:28:09 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0008	bsauser	BSA_PERSISTENT_HIVE_bsatam_http	SPARK	default	Tue Oct 23 09:27:35 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0007	bsauser	bsa_tam2_ALARM_PERSISTENT_HIVE	SPARK	default	Tue Oct 23 09:27:48 +0800 2018	N/A	RUNNING	UNDEFINE
application_1540257944033_0005	bsauser	bsa_tam2_TI_REALTIME_DETECT	SPARK	default	Tue Oct 23 09:27:35 +0800 2018	N/A	RUNNING	UNDEFINE

NSFOCUS

谢谢！

NSFOCUS