ITOA数据来源有哪些?

厉梦如 2019-05-19 发表

问题描述

Q：ITOA数据来源有哪些?

解决方法

A：ITOA系统数据来源是网络安全设备、服务器、操作系统、应用系统等一切产生日志的对象。依赖DataEngine提供的大数据基础能力，通过各种采集手段进行数据采集、加工、存储到数据仓库，在进行上层的业务分析、挖掘、展示。

Ø 对于网络安全设备的系统日志，设备本身具备主动上报功能，采用UDP、TCP协议将其自身的系统日志以及业务日志上报至ITOA系统，ITOA系统使用Rsyslog进行被动接收。

Ø 对于网络设备基础信息，例如CPU、内存、温度等，存在于设备的MIB表中，这部分需要使用SNMP协对于没有日志上报能力的日志。

Ø 如应用的系统日志、部分操作系统日志等就需要采用下发beat形式进行主动采集。

Ø 流量日志（流日志）不同的厂商采用了不同的协议标准：华三和华为采用netstream协议、思科采用netflow协议。这部分数据由单独的程序进行采集。

Ø 存储在网管系统，或认证系统中，用户的上下线数据。这部分数据多存储于认证系统的数据库中。ITOA系统会通过Restful接口来采集这部分数据