工控日志审计系统

《需求说明书》

2018年5月18日

北京航空航天大学计算机学院

**修订版本**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订人** | **日期** | **备注** |
| V1 | 张群轼 | 2018.5.18 | 初稿 |
| V2 | 周文浩 | 2018.8.30 | 草稿 |
|  |  |  |  |
|  |  |  |  |

**目录**

[1 引言 5](#_Toc523648983)

[1.1 编写目的 5](#_Toc523648984)

[1.2 读者对象 5](#_Toc523648985)

[1.3 项目背景 5](#_Toc523648986)

[1.4 参考文献 5](#_Toc523648987)

[2 任务概述 6](#_Toc523648988)

[2.1 目标 6](#_Toc523648989)

[2.2 用户特点 6](#_Toc523648990)

[2.3 假设和依赖 6](#_Toc523648991)

[3 系统特性 7](#_Toc523648992)

[3.1 功能描述 7](#_Toc523648993)

[3.1.1 系统首页显示内容 7](#_Toc523648994)

[3.1.2 日志检索 7](#_Toc523648995)

[3.1.3 日志监控 7](#_Toc523648996)

[3.1.4 可视化统计 8](#_Toc523648997)

[3.1.5 事件告警 8](#_Toc523648998)

[3.1.6 日志报表 8](#_Toc523648999)

[3.1.7 资产管理 8](#_Toc523649000)

[3.1.8 系统管理 8](#_Toc523649001)

[3.1.9 消息中心 8](#_Toc523649002)

[3.1.10 日志存储 8](#_Toc523649003)

[3.2 性能描述 8](#_Toc523649004)

# 引言

## 编写目的

此文档是对日志审计系统功能、性能、用户界面以及运行环境，系统部署条件等信息作出详细说明。为系统设计阶段提供依据和指导。帮助开发人员、测试人员和相关人员了解系统实现的功能，并作为验证产品是否能满足用户需求的依据。

## 读者对象

此文档面向的读者人群为：参与此项目的前端开发人员、后端开发人员、测试人员、项目经理以及市场营销人员。

## 项目背景

随着信息化的快速发展，当今的企业和组织在IT信息安全领域面临比以往更为严峻的挑战，一方面是来自于企业和组织外部的层出不穷的入侵和攻击手段，一方面是来自企业和组织内部的违规和泄露。

为了应对不断的挑战，企业和组织部署了防病毒系统、入侵检测系统、防火墙等一系列安全系统。这些安全系统仅仅是防堵某个方面的安全威胁，形成了一个个安全防御孤岛，无法产生协同效应。这些安全系统在运行过程中还产生了大量的日志，安全管理人员面对大量的、彼此割裂的安全信息，操作着产品自带的控制台界面和告警界面，显得束手无策，工作效率低下，难以发现真正的安全隐患。这就产生了对日志审计系统迫切的需求。日志审计系统能够收集来自企业和组织IT资源中设备和应用的日志，并进行存储、监控、审计、分析、报警、响应和报告，能够满足企业和组织对安全领域的需求。

## 参考文献

[1] <https://blog.csdn.net/c1052981766/article/details/51177974/>.

[2] 赖均、陶春梅、刘兆宏、胡峰，软件工程[M].清华大学出版社，2016.1.

[3] 绿盟安全审计系统[日志审计]用户手册

[4] 杨舒琴，基于日志的安全审计管理系统的研究与实现[D],2011.1.

# 任务概述

## 目标

本系统的目的是研发一款对企业的设备和应用的日志进行存储、监控、审计、分析、报警、响应和报告的日志审计系统。本系统可以用于对企业内部员工操作、IT系统操作等活动进行监控，及时发现异常和违规操作，最大程度的减少内部原因引起的安全隐患。

根据项目的计划，项目的目标主要有实现以下几个方面：

1.日志检索；

2.日志监控；

3.日志的可视化统计；

4.事件告警；

5.日志报表；

6.资产管理；

7.系统管理；

8.消息中心；

9.串口管理；

10.日志存储；

## 用户特点

主要用户是各个企业的安全管理人员、系统运维人员。用户需要对系统运维、linux操作系统、windows操作系统以及Internet协议有一定的了解。

## 假设和依赖

本项目能否成功实施取决于以下条件:

1. 研发团队掌握了先进的能适用于该项目的技术，这是系统的性能是否优化、项目能否完成的根本保证；
2. 团队成员的积极配合，为了项目的开发和实施，合理规划个人时间同时为团队做出合理牺牲，配合队友完成任务。

# 系统特性

## 功能描述

### 系统首页显示内容

本系统的首页显示内容包括以下内容：

1. 统计系统中日志总条数展示；
2. 当日(从0点开始至现在)日志增量；
3. 近7天(按天)每天的日志量；
4. 日志类型数量；
5. 当日(从0点开始至现在)所产生的事件中，源、目的IP统计出现次数最多的前五个；
6. 最新的5条事件展示，此外，点击查看更多的时间展示；
7. CPU、磁盘、内存总量及当前使用情况以及展示系统总资源占用率；
8. 展示资产最多的前5个分组；

### 日志检索

日志检索用于临时检查满足某些条件的日志。主要功能：

1. 查询语法

日志检索的查询语法应该支持全文检索、key-value检索、多key-value布尔组合、括弧、正则检索、模糊检索。全文检索是指将整行日志作为整体进行查询，既不区分键与数值，例如用户可提供一个ip地址如192.168.1.1进行查询，查询结果为包含该ip地址192.168.1.1的所有日志，但是这里的ip地址是源ip地址或者目的ip地址。key-value检索是指指定键和值情况下进行查询，例如指定源ip地址src\_ip:192.168.1.1，查询结果为源ip地址是192.168.1.1的所有日志。

1. 2.查询范围和辅助配置
2. 日志导出
3. 结果展示。

在日志检索之前应该支持选择待检索的日志类型和日志的所属时间范围，日志检索的条件支持保存，以便于下一次检索时调入。日志检索也支持多日志全文查询和单日志独立查询，查询结果按类别分页签打开。查询结果可以导出进行保存。对于当前的查询结果可以进行统计展示，可以按行式展示，也可以按列式展示。

### 日志监控

与日志检索不同的是，日志监控是对满足某些条件的日志进行多次快速查询。

日志监控支持对日志进行树状分组管理，并支持对分组的配置，查询树上的叶子结点可以直接查询日志。日志监控也支持日期时间范围选择和快捷日期选择，以及支持开启或关闭自动刷新。自动刷新可以设置刷新周期，包括：3、5、10、30分钟。当前的查询结果可以以列表形式进行展示、统计图展示以及支持时间、日志类型、上报设备等通用字段的展示。

主要功能：条件分组、手动操作、自动刷新、结果展示。

### 可视化统计

可视化统计，顾名思义就是对指定的日志进行统计并以指定的统计项进行展示。支持的统计项包括趋势图、柱状图、折线图、饼图和表格。

其中，趋势图、柱状图、折线图的要求一致：Y轴度量指标支持的聚合方式：count,min,max,sum,avg,unique count；度量指标支持自定义标签；支持多度量指标组合；度量刻度支持的聚合方式：时间等距划分、数据等距划分、时间范围划分、数字范围划分、枚举值划分、枚举值过滤划分。

饼图的要求：Y轴度量指标支持的聚合方式：count,min,max,sum,avg,unique count；X轴做饼图切分，支持的聚合方式：时间等距划分、数据等距划分、时间范围划分、数字范围划分、枚举值划分、枚举值过滤划分。

表格的要求：Y轴度量指标支持的聚合方式：count,min,max,sum,avg,unique count；X轴做行切分，支持的聚合方式：时间等距划分、数据等距划分、时间范围划分、数字范围划分、枚举值划分、枚举值过滤划分。

对于统计项，可以利用统计项树进行保存、自定义分类。统计项树也支持内置统计项(100多个)

主要功能：趋势图、柱状图、折线图、饼图、表格、统计项树。

### 事件告警

事件告警主要是对事件列表和时间规则的管理。它支持对事件名称、发生时间、源目的IP、风险等级进行查询。事件查询结果可以进行统计，统计结果展示不同日志类型在不同时间段的日志数量，支持今日、本周、本月等时间对统计结果进行过滤，也支持设置过滤TOP值。事件列表支持按时间倒序展示事件，包括事件名、风险级别、源目的IP、产生时间等。事件规则支持按日志设定，支持设置字段间布尔逻辑关系，支持设置key-value数学操作符，支持设置嵌套条件，支持设置分组条件，支持设置分组统计条件，也支持设置事件风险级别。

主要功能：事件查询、事件统计、事件列表、事件规则。

### 日志报表

日志报表主要完成的是创建和管理报表。报表的模板内容支持第三方报表的自定义，包括：支持编辑报表目录结构、支持引用统计项、支持设置报表标题、支持展示页眉和页码、支持报表配置基本内容（名称、描述等）。报表的生成任务可以立即执行任务、定时任务和周期性任务。数据时间过滤支持根据起止时间筛选数据，时间格式精确到分钟，支持起止时间以日历形态可视化展示，支持快捷选择过去3天、5天、7天数据并动态呈现到界面，支持展示已选择时间文字展示和图形展示。模板统计项配置支持报表模板统计项选择，支持多选、全选、取消、重置以及支持统计项搜索。

我的报表支持按日报、周报、月报分类，支持查看全部类型报表，支持报表名、模板名模糊检索，支持展示报表名称、模板名称、分类、所生成的文件格式、创建时间、通知，支持批量下载报表。报表任务的执行设置可以支持设置任务标题、任务描述、报表类型。生成的文件类型支持html，pdf，word格式的报表文件。报表任务支持以列表形态展示，包括任务名、执行方式、开始时间、下次执行时间、结果列表、状态、操作，支持按任务名筛选任务。报表任务支持查看任务结果清单，包括执行时间、执行结果以及支持批量下载任务结果。报表任务支持单选、多选、删除、翻页，支持查看任务、停止任务、查看在线报表、下载HTML/WORD/PDF报表文件。每个报表任务支持展示过滤器信息，包括数据时间、最近执行时间、总耗时、模板、描述、类型、通知信息。报表模板可按分组展示，可按分组查看不同的模板集合，也可查看全部模板。模板可新建，包括模板名称、模板分类、模板描述、模板文件上传；也可以编辑，可编辑模板名称、分类、描述，或替换模板文件。报表支持LOGO配置。

主要功能：报表模板内容、任务类型、数据时间过滤、模板统计项过滤、我的报表、执行设置、通知设置、文件类型、任务列表、任务列表结果、任务管理、任务详情、报表模板内容、模板操作、个性化。

### **资产管理**

资产管理即是对资产进行管理。资产管理支持对资产进行增删改查，支持视图方式查看资产，支持自定义视图和内置视图。每个资产可以查看资产相关的日志、事件。

主要功能：资产管理、视图管理、数据关联。

### 系统管理

系统管理主要完成的是对安全设备、采集器、日志评审系统等全局性参数进行配置。

数据接入部分支持查看绿盟设备接入情况，包括：设备名称、IP、类型、内存使用率、CPU使用率、流量、在线状态等。一次数据接入作为数据源，每个数据数据源支持统计信息展示，包含：接入的日志类型数、设备数、未识别日志条数、解析失败日志数、接收速率、范式化速率、入库速率。数据源支持以列表展示：包含日志类型、接收速率、范式化速率、已处理数、未识别数、解析失败数，支持的操作包括：启停、删除、编辑，支持导出规则、备份数据源、恢复数据源。支持接入的日志类型包括绿盟设备、第三方安全设备、网络设备、数据库、windows/linux主机日志、web服务器日志、虚拟化平台日志、网络设备流量(netflow等)、以及自定义日志。agent管理支持agent列表呈现，包括：IP、主机名、最后请求时间、操作系统、版本号,支持上传agent、删除agent。

证书支持证书导入向导、证书导出、证书状态查看。系统状态支持展示系统各核心服务状态，支持展示系统端口情况。超限管理支持日志容量超限删除策略配置。系统升级支持离线手动升级，支持在线自动升级，支持当前版本展示，支持升级包信息展示，支持向导式升级。

用户管理支持支持基于角色的帐户管理，内置管理员、帐户管理员、系统审计员、安全员、非登录用户(用来通知)，也支持帐号管理，支持新建、删除、停用、启用帐号，支持帐号列表展示，包括帐号名、角色、邮箱、手机号码、可登录IP、状态，支持帐号编辑，支持帐号查询，支持当前帐号信息展示。

网络支持配置网口IP、掩码、网关，支持配置路由。通知配置支持配置邮件服务器信息，支持邮件配置验证，支持配置FTP服务器信息。系统监控支持设置CPU、内存告警阈值和持续时间，支持磁盘容量监控告警阈值设置。系统备份支持远程FTP备份，备份路径可展示，支持按日期、类型两个维度进行备份，支持日志类型多选，支持按日期、按日志类型进行日志恢复，支持资产的备份恢复。系统配置支持NTP配置，支持配置主备服务器地址，支持配置同步方式。日志可按日期、按类型删除，日志类型可多选。报表LOGO可以个性化配置。

诊断工具包括网络诊断、远程协助、快照收集。网络诊断支持ping、tenet等方式诊断连通性。远程协助包含SSH服务、远程调试功能的开启或关闭。快照收集可收集系统快照，然后提交给系统支持人员进行问题诊断。

主要功能：数据接入、证书管理、系统状态、超限管理、升级管理、用户管理、网络配置、通知配置、系统监控、备份管理、NTP配置、日志删除、个性化、诊断工具。

### 消息中心

消息中心主要是完成提醒用户的功能，当有需要通知用户的消息产生时消息中心才会提醒。消息中心还支持系统消息列表展示，包括标题内容、严重级别、创建时间、类型，支持消息操作，包括标记为已读、删除，支持未读消息和已读消息分类查看；支持消息按类型过滤。

主要功能：消息展示、消息操作。

### 串口管理

串口管理主要管理与外设间的通讯。串口管理支持系统配置，包括SSH服务启停、支持设备关怀报务启停，支持上传离线升级包升级，支持配置在线升级策略自动升级，支持系统诊断、网络连接诊断，支持展示产品信息、系统服务状态、端口状态、快照信息等，支持配置管理口IP、掩码、网关，支持配置管理口路由，支持恢复WEB界面管理员密码，支持设置系统时钟，支持进行网络诊断，支持将系统中数据(除证书、版本、网络配置)进行删除，支持重新生产设备，将设备生产至出厂状态，支持支持重启系统、关闭系统。

主要功能：系统配置、系统升级、诊断工具、系统状态、网络配置、密码恢复、时钟设置、网络诊断、数据清除、重新生产、系统管理。

### 日志存储

日志存储主要是对日志存储的配置，主要功能：

1. 支持原始日志存储，支持范式化日志存储；
2. 自定义存储周期，最长6个月。

## 性能描述

本产品分为两个型号，分别是SASNX3-L1\*00型和SASNX3-L2\*00型。

1.SASNX3-L1\*00型

该型号性能规格：

默认可接入40个日志源，可购买授权扩展，扩展上限受日志平均处理能力（1000EPS）限制。单台日志处理性能：平均1000EPS，10亿背景数据指定字段查询最快可在5秒内响应。

硬件规格：

1U标准式机架，冗余双电源，专用硬件平台和安全操作系统，1个Concole口，2GE口，1CF卡，32G内存，支持多端口采集，可支持14千兆数据采集口或4个万兆数据采集口，存储容量4TB，支持存储容量定制扩展。

2.SASNX3-L2\*00型

该型号性能规格：

默认可接入40个日志源，可购买授权扩展，扩展上限受日志平均处理能力（5000EPS）限制。单台日志处理性能：平均5000EPS，10亿背景数据指定字段查询最快可在5秒内响应。

硬件规格：

2U标准式机架，冗余双电源，专用硬件平台和安全操作系统，1个Concole口，2GE口，1CF卡，32G内存，支持多端口采集，可支持34千兆数据采集口或8个万兆数据采集口，存储容量12TB(RAID5)，支持存储容量定制扩展。