★完全公开

# 网神 SecFox 日志收集与分析系统 V5.0-日志采集器-快速上线部署手册 V1.0-软件版

创建时间：2022 年 9 月 4 日

修改时间：2024 年 5 月 14 日

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：100044

## ● 版权声明



## ● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操**

**作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。**

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利： **在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**
8. 本声明受中华人民共和国法律的约束并依据其解释。
9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

# 目录

# 1 产品概述

## 1.1 产品简介

网神 SecFox 日志收集与分析系统 V5.0R7.4.0 是奇安信网神信息技术（北京）股份有限公司（以下简称“奇安信网神”）基于在安全分析和审计技术的长期积累，结合中国政企行业的客户需求，自主研发的基于大数据技术和机器学习技术的日志审计产品，满足了客户针对日志的集中采集、存储、审计、分析和展示的需求。

网神 SecFox 日志收集与分析系统作为一个统一日志监控与审计平台，能够实时不间断地将政企客户 IT 网络中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合日志审计。

网神 SecFox 日志收集与分析系统能够实时地对采集到的不同类型的日志信息进行归一化处理和实时关联分析，协助安全管理人员从海量日志中迅速准确地识别安全事件，大幅降低了日志分析和管理对安全管理人员的技术能力要求，提高了工作效率。日志收集与分析系统为用户在统一的控制台界面进行实时、动态的可视化呈现，消除了管理员在多个控制台之间来回切换的烦恼。 日志收集与分析系统帮助用户满足安全审计的合规要求，可帮助用户快速出具满足国家法律法规，行业标准的多种合规报表和报告，帮助安全人员对内部管理的合规情况一览无余。

网神 SecFox 日志收集与分析系统实现了针对海量、高速、异构日志和事件的高吞吐量采集、高效的长期存储和快速实时的数据分析。系统采集和存储日志事件，支持搜索、检索和报告。系统记录原始日志，支持未修改数据的即席查询，以获取高质量的调查取证数据。

网神 SecFox 日志收集与分析系统既可以单机部署，也可以分布式部署，有多种可选的分布式组件，包括分布式日志采集器软件、分布式计算与存储节点软件、流量采集器设备、日志采集代理程序等。

## 1.2 适用产品

本手册适用于软件版本为网神 SecFox 日志收集与分析系统 V5.0R7.4.0 的分布式日志采集器。

## 1.3 读者对象

本文适用于使用奇安信网神信息技术（北京）股份有限公司网神 SecFox 日志收集与分析系统 V5.0R7.4.0 的使用人员，包括企业和组织的安全管理人员、安全分析员、安全审计人员和安全运维人员等。

## 1.4 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

| 符号名称 | 说明 |
| --- | --- |
|  警告 | 以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。 |
|  注意 | 以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。 |
|  说明 | 以本标志开始的文本是正文的附加信息，是对正文的强调和补充。 |
|  窍门 | 以本标志开始的文本能帮助您解决某个问题或节省您的时间。 |

# 2 设备上架

## 2.1 安装前准备

### 2.1.1 工具准备

表 2-1 工具说明

| 工具名称 | 数量 | 用途 |
| --- | --- | --- |
| 网线 | 1 | 用于连接设备的以太网接口和其他设备，例如连接 PC 用来调试设备。或连接其他设备用于检查设备是否配置正确。 |
| | | |
| | | |

### 2.1.2 安装环境确认

#### 2.1.2.1 服务器硬件要求

硬件配置需要保持一致，标准配置如下：

表 2-2 硬件配置说明

| 配置 | 描述 |
| --- | --- |
| 内存 | 最低要求 4GB，推荐 8GB 以上 |
| CPU | x86 架构多核多线程 CPU，最低配置为双核 4 线程，推荐使用 Intel i5 以上 CPU |
| 存储空间 | 至少 200GB 以上存储空间，不限于物理机和虚拟化存储空间。 |
| 网卡 | 1000Base-T 及以上 |

#### 2.1.2.2 操作系统版本要求

目前支持 CentOS_7.X_x64、 Redhat_7.X_x64、Ubuntu18_server_x64 或 Ubuntu20_server_x64 操作系统。要求为“基础设施服务器安装”，具体安装过程请参考《网神 SecFox 日志收集与分析系统 V5.0-操作系统安装手册 V1.1》文档。

#### 2.1.2.3 操作系统账户要求

确保使用 root 用户进行安装操作。

#### 2.1.2.4 浏览器要求

支持以下浏览器访问日志采集器管理页面。

表 2-3 浏览器说明

| 浏览器 | 版本 |
| --- | --- |
| Google Chrome | 70 及以上 |

#### 2.1.2.5 软件版本要求

快速部署版本对软件的要求：

当前安装包为：LAS-PBL-V5.0R7.4.0-202308030010-linux-x86-64-singleton.tar.gz

#### 2.1.2.6 安装准备

安装 LAS-PBL 前准备工作：

1、 操作系统禁用 SELinux
禁用 SElinux 命令：sed -i "s/\=enforcing/\=disabled/g" /etc/selinux/config

2、 查看 SELinux 和防火墙状态
执行命令：getenforce，查看 SElinux 状态为 Disabled，修改后需要执行 reboot 重启服务器让禁用 SELinux 生效。

**说明**

SElinux 是个安全机制，如果不禁用的话更新了更新了 ssh 会导致某些命令无法输出，比如 ip addr，或者你在目录 A 创建了文件，mv 到目录 B 以后 tomcat 这种应用程序就没有权限访问了

```
[root@localhost ~]# getenforce
Disabled
```

图 2-1 防火墙状态图

firewall 防火墙执行命令：systemctl status firewalld.service，查看防火墙状态为 active

```
[root@localhost ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-09-02 02:27:18 CST; 3 days ago
     Docs: man:firewalld(1)
 Main PID: 1161 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─1161 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid

Sep 02 02:27:05 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Sep 02 02:27:18 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Sep 02 02:27:21 localhost.localdomain firewalld[1161]: WARNING: ICMP type 'beyond-scope' is not supported by the kernel for ipv6.
Sep 02 02:27:22 localhost.localdomain firewalld[1161]: WARNING: beyond-scope: INVALID_ICMPTYPE: No supported ICMP type., ignoring for run-time.
Sep 02 02:27:22 localhost.localdomain firewalld[1161]: WARNING: ICMP type 'failed-policy' is not supported by the kernel for ipv6.
Sep 02 02:27:22 localhost.localdomain firewalld[1161]: WARNING: failed-policy: INVALID_ICMPTYPE: No supported ICMP type., ignoring for run-time.
Sep 02 02:27:22 localhost.localdomain firewalld[1161]: WARNING: ICMP type 'reject-route' is not supported by the kernel for ipv6.
Sep 02 02:27:22 localhost.localdomain firewalld[1161]: WARNING: reject-route: INVALID_ICMPTYPE: No supported ICMP type., ignoring for run-time.
[root@localhost ~]#
```

图 2-2 firewall 防火墙状态图

ufw 防火墙执行命令：ufw status，查看防火墙状态为 active

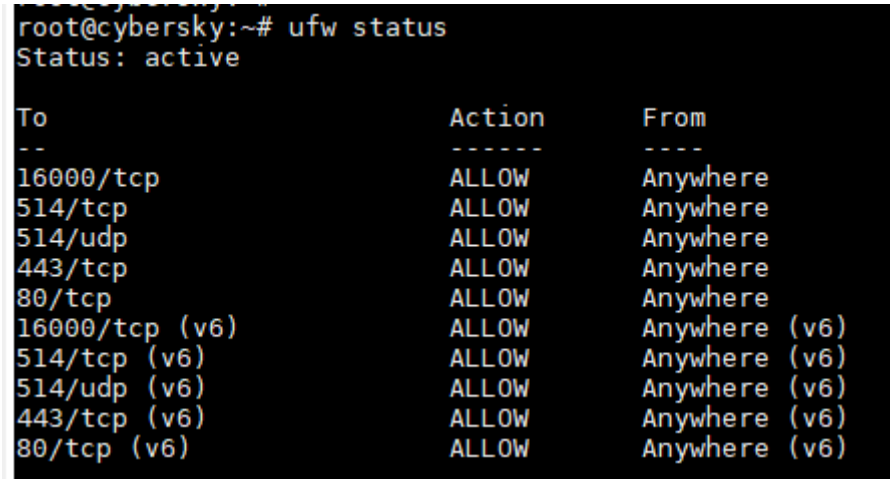


图 2-3 ufw 防火墙状态图

3、 操作系统网络环境需开放相应的网络访问控制策略。具体的网络访问控制策略参考下表，根据需要开通策略：

表 2-4 网络访问控制策略表

| 源 | 源端口 | 目的 | 目的端口 | 协议 | 描述 |
|---|---|---|---|---|---|
| LAS-PBL | Any | LAS | 443 | https | LAS 与 LAS-PBL 之间进行通信 |
| LAS-PBL | Any | LAS | 9514 | TCP、UDP | 管理中心通过 9514 端口接收日志采集器采集上来的日志信息 |
| LAS-PBL | Any | LAS-DCS | 9514 | TCP、UDP | 分布式计算存储节点通过 9514 端口接收日志采集器采集上来的日志信息 |
| LAS-PBL | Any | 时间服务器 | 123 | UDP | 连接时间服务器，同步时间 |
| 被采集设备 | Any | LAS-PBL/LAS | 161 | UDP | 用于接收 SNMP 信息的端口 |
| 被采集设备 | Any | LAS-PBL/LAS | 162 | UDP | 用于接收 SNMP Trap 告警的端口 |
| 被采集设备 | Any | LAS-PBL/LAS | 514 | TCP、UDP | 用于接收 syslog 日志 |
| 被采集设备 | Any | LAS-PBL/LAS | 2055 | UDP | 用于接收 flow 数据及部分二进制日志 |
| LAS-PBL/LAS | Any | 被采集设备 | 页面配置的端口 | TCP | 用于 JDBC 采集任务采集数据 |
| LAS-PBL/LAS | Any | 被采集设备 | 页面配置的端口 | TCP | 用于 kafka 采集任务采集数据 |

firewall 防火墙添加访问控制策略示例：

firewall-cmd --permanent --add-rich-rule="rule family="ipv4" source address="LAS 的 ip " port protocol="tcp" port="21" accept"

添加策略后需要执行 firewall-cmd –reload 重启防火墙让策略生效

ufw 防火墙添加访问控制策略示例：

ufw allow from ip 地址 to any port 端口号

添加策略后需要执行 ufw reload 重启防火墙让策略生效

## 2.2 设备上架

该章节内容请按照标题顺序执行。

### 2.2.1 上传安装包

通过 sftp 工具使用 root 账户登录系统，将安装包上传至/root 目录。

### 2.2.1 解压安装包

通过命令：

cd /root

tar zxf LAS-PBL-V5.0R7.4.0-202308030010-linux-x86-64-singleton.tar.gz

### 2.2.2 执行安装

通过命令：

cd /root/LAS-PBL-V5.0R7.4.0/scripts/

./install --data <path>

<path>为安装目录，例如安装目录为 /data ，则执行./install --data /data ,安装后程序目录为 /data/secfoxpbl

--data 指定软件安装的目录，如果安装目录不存在则执行安装命令时会自动创建，系统程序和数据都存放在该目录下，需要保证足够的磁盘空间。

软件安装前，会自动对系统进行如下检测:

1. 检查系统是否安装软件所需依赖包：libaio、fontconfig、rsync、traceroute，如果是 Ubuntu 系统除以上依赖包外还需要 libncurses5

2. 检查当前系统 umask 是否设置为 0022。

3. 检查--data 指定目录是否为最大分区，检查通过则继续安装，反之给出提示并询问是否继续。

4. 检查当前系统时区非东八区（上海/重庆/乌鲁木齐或香港）时，给出相关提示并自动修改时区为 Asia/Shanghai。

注：以上其中 1、2 项不符合要求时自动退出安装,3、4 项根据提示自行选择是否退出。

如何查看空间相对较大的目录?

执行命令：df -h，查看系统目录挂载情况，选取空间相对较大的目录，进行安装，如下图所示：

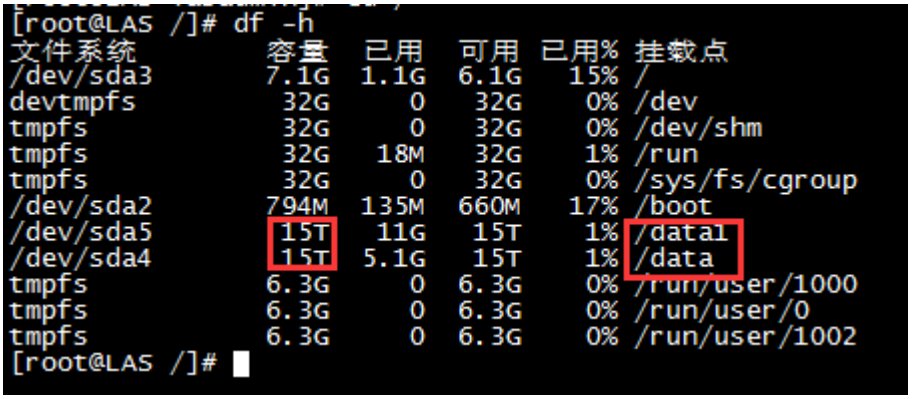
[root@LAS /]# df -h
文件系统 容量 已用 可用 已用% 挂载点
/dev/sda3 7.1G 1.1G 6.1G 15% /
devtmpfs 32G 0 32G 0% /dev
tmpfs 32G 0 32G 0% /dev/shm
tmpfs 32G 18M 32G 1% /run
tmpfs 32G 0 32G 0% /sys/fs/cgroup
/dev/sda2 794M 135M 660M 17% /boot
/dev/sda5 15T 11G 15T 1% /data1
/dev/sda4 15T 5.1G 15T 1% /data
tmpfs 6.3G 0 6.3G 0% /run/user/1000
tmpfs 6.3G 0 6.3G 0% /run/user/0
tmpfs 6.3G 0 6.3G 0% /run/user/1002
[root@LAS /]#

图 2-4 磁盘空间图

# 3 首次使用

## 3.1 登录系统

安装完毕后，LAS-PBL 系统自动启动。在管理主机上使用谷歌浏览器 Chrome 访问 https://[IP]。

默认登录账号为：admin，密码为：!1fw@2soc#3vpn

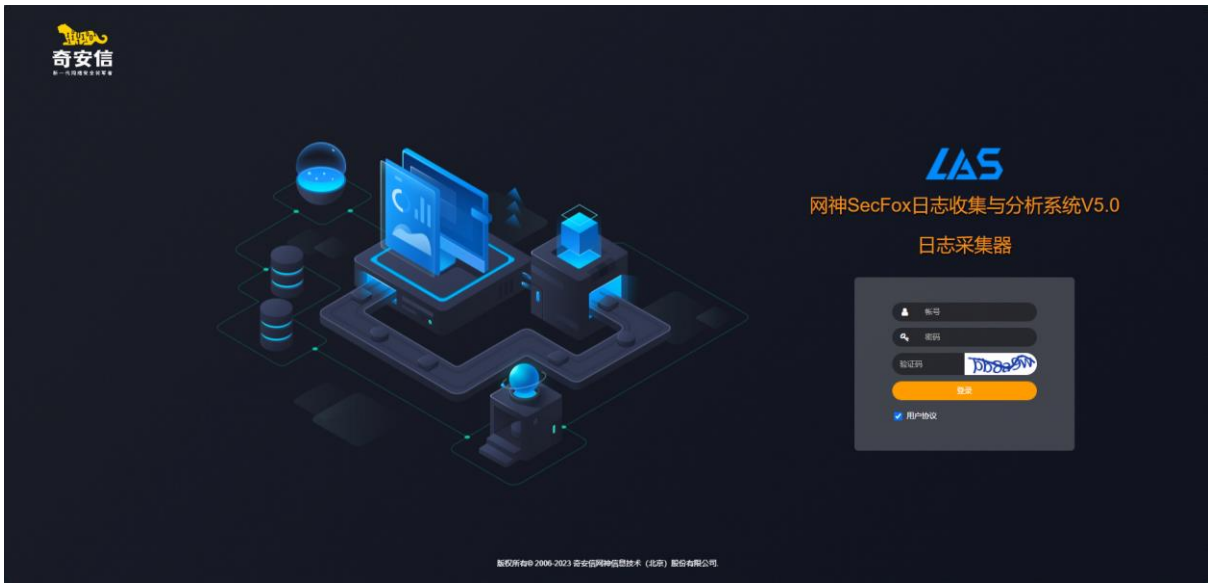


图 3-1 登录系统展示图

## 3.2 采集器管理

用于实现日志采集，并把事件转发给管理中心。采集方式包括主动采集数据库日志、文件日志、主机日志等，被动接收 Syslog、SNMP Trap 等协议数据包。日志采集器可以安装在被采集设备上，也可以独立部署在另外的服务器上。

日志收集与分析系统（管理中心），“配置”->“节点管理”模块下进行采集器的注册和管理。

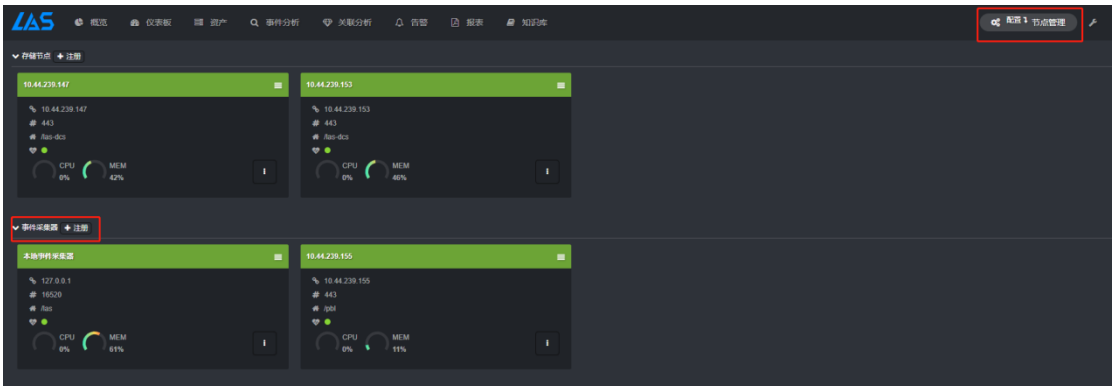

图 3-2 采集器管理展示图

### 3.2.1 注册/修改日志采集器

注册/修改日志采集器需要配置如下信息：

1、 节点类型

2、 名称

3、 描述

4、 主机（日志采集器访问地址）

5、 端口（日志采集器访问端口）

6、 协议（可选择 http、https）

7、 反向访问主机（如果从日志采集器反向访问管理中心需要地址转换，需要填写）

8、 反向访问端口

### 3.2.2 配置日志采集器

可以对采集任务、转发及接收参数、过滤策略、日志代理进行配置。详细见《网神 SecFox 日志收集与分析系统 V5.0_用户手册》中“采集管理”章节。

### 3.2.3 事件采集器卡片列表

点击 [配置] - [节点管理] 菜单，即可进入事件采集器列表页面。事件采集器列表中每个卡片中显示了事件采集器的。

1、 名称

2、 地址

3、 端口

4、 访问路径

5、 状态（绿色表示正常，红色表示日志采集器出现故障）

6、 CPU 利用率及内存利用率

7、 在卡片右上角可以对该采集器进行操作，对于分布式采集器可以进行配置、修改、删除操作，对于本地事件采集器可以进行配置操作。

8、 在卡片右下角按钮可以点击查看该采集器的详细监控信息，包括：

(1) 当前 CPU 利用率及最近 1 小时 CPU 利用率趋势

(2) 当前内存利用率及最近 1 小时内存利用率趋势

(3) 当前磁盘使用情况

(4) 当前系统负载情况及最近 1 小时系统负载趋势

(5) 最近 1 小时网卡流量趋势

# 4 软件维护

## 4.1 系统升级

在 web 管理界面选择“系统-系统升级”菜单。

在展开的升级界面，点击“浏览”按钮，选择升级包，点击“上传”按钮，上传完成后点击版本升级。

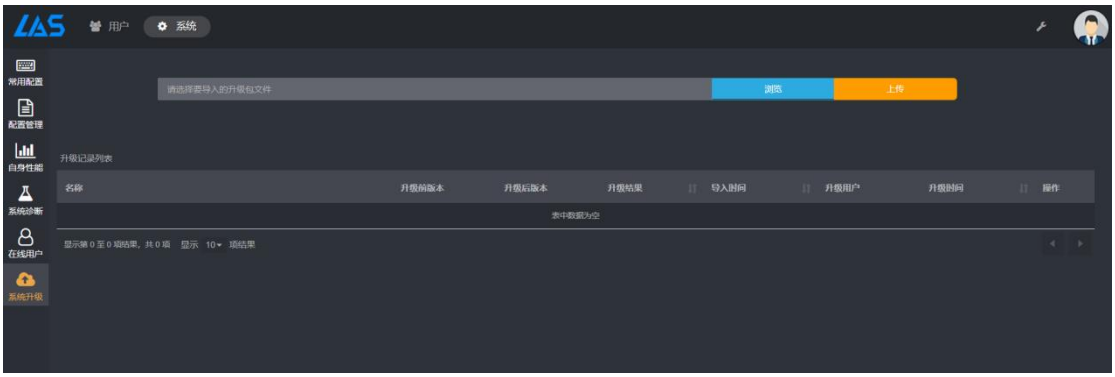


图 4-1 系统升级操作图