SANGFOR-LAS 用户手册

深信服智安全
SANGFOR SECURITY

目录

声明

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深信服科技股份有限公司技术服务部。

深信服科技股份有限公司（以下简称为深信服科技、SANGFOR）。

前言

手册内容

第 1 部分 SANGFOR 产品概述。该部分主要介绍 LAS 设备的外观特点，以及连接前的准备和注意事项。

第 2 部分 SANGFOR-LAS 功能说明。

本手册以 SANGFOR LAS-1000 为例进行配置。由于各型号产品硬件和软件规格存在一定差异，所有涉及产品规格的问题需要和深信服科技有限公司联系确认。

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服社区：bbs.sangfor.com.cn

深信服服务商及服务有效期查询：

http://bbs.sangfor.com.cn/plugin.php?id=service:query

公司网址：www.sangfor.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢

第 1 章　安装指南

本部分主要介绍了 SANGFOR-LAS 系列产品的构成与硬件安装。硬件安装正确之后，您才可以进行配置和调试。

1.1. 环境要求

SANGFOR-LAS 设备可在如下的环境下使用。

- 输入电压： 110V~230V
- 温度：0～45℃
- 湿度：5～90%

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放和使用。

1.2. 电源

SANGFOR-LAS 系列产品使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3. 产品外观

图 1：SANGFOR LAS 前面板（以 LAS-1000 为例）

1.CONSOLE(控制)口　　2. ETH0（默认管理口）　　3.ETH1（默认流量监听口）

4.ETH2（备用管理口）　5.ETH3（可配置为监听口）6.ETH4（可配置为监听口）

7.ETH5（可配置为监听口）

出厂默认 IP 地址：

接口	IP 地址
(ETH0)管理口	10.251.251.128/24
ETH1	默认镜像口
（ETH2）备用管理口	10.252.252.126/24
ETH3	
ETH4	
ETH5	

告警灯在设备启动期间是红灯长亮的。一般一两分钟后红灯熄灭，说明正常启动。如红灯长时间不熄灭，请关闭设备等待 5 分钟后重新开机。如果还是长亮，请联系深信服科技客服部确认是否设备损坏。正常启动后，有时红灯会闪烁，这是正常现象，红灯闪烁表示设备正在写系统日志。

控制口仅供开发和测试调试使用。最终用户需从网口通过控制台接入。

1.4. 配置与管理

在配置设备之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用（如 Internet Explorer），然后把电脑与 SANGFOR-LAS 连接在同一个局域网内，通过网络对设备进行配置。

设备出厂的默认 IP 见下表：

接口	LAS
(ETH0)管理口	10.251.251.128/24
（ETH2）备用管理口	10.251.251.126/24
ETH1	默认镜像口

1.5. 单设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 ETH0 口与内部局域网电脑连接，对 LAS 设备进行配置。

设备正常工作时 POWER 灯常亮，接线的数据接口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。

第 2 章 登录 WEB 页面

2.1. 登录 web 配置界面

2.1.1. LAS 的 web 登录方式

LAS 支持安全的 HTTPS 登录，使用的是 HTTPS 协议的标准端口登录。如果初始登录从 ETH0 口登录，那么登录的 URL 为：https://10.251.251.128

HTTPS 登录界面管理 LAS 可以防止配置过程在传输过程中被截获而产生的安全隐患。

1、如何登录 LAS 设备页面？

按照前面所示方法接好线后，通过 WEB 界面来配置 SANGFOR LAS 设备。方法如下：

首先为本机器配置一个 10.251.251.X 网段的 IP（如配置 10.251.251.100），然后在 IE 浏览器中输入网关的默认登陆 IP 及端口 https://10.251.251.128。出现一个如下图的安全提示：

点击继续浏览此网站后出现以下的登录界面：

在登陆框输入『用户名』和『密码』，点击登录按钮即可登录 LAS 设备进行配置，默认情况下的用户名和密码均为 admin。

登录页面不需要安装任何控件，支持用非 IE 的浏览器登录。

2、如何消除登录页面的证书告警框？

登录页面时，浏览器上会弹出证书警告框，如何消除此警告框？

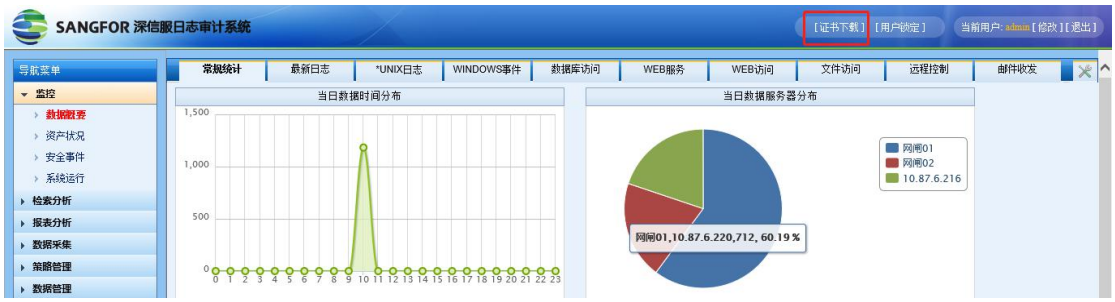
首先，登录页面，进入『系统配置』→『系统管理』→『证书生成』页面：

在『证书生成』中点击生成：

页面会提示生成成功，WEB 服务重启中

然后，点击确定，关闭浏览器重新打开。

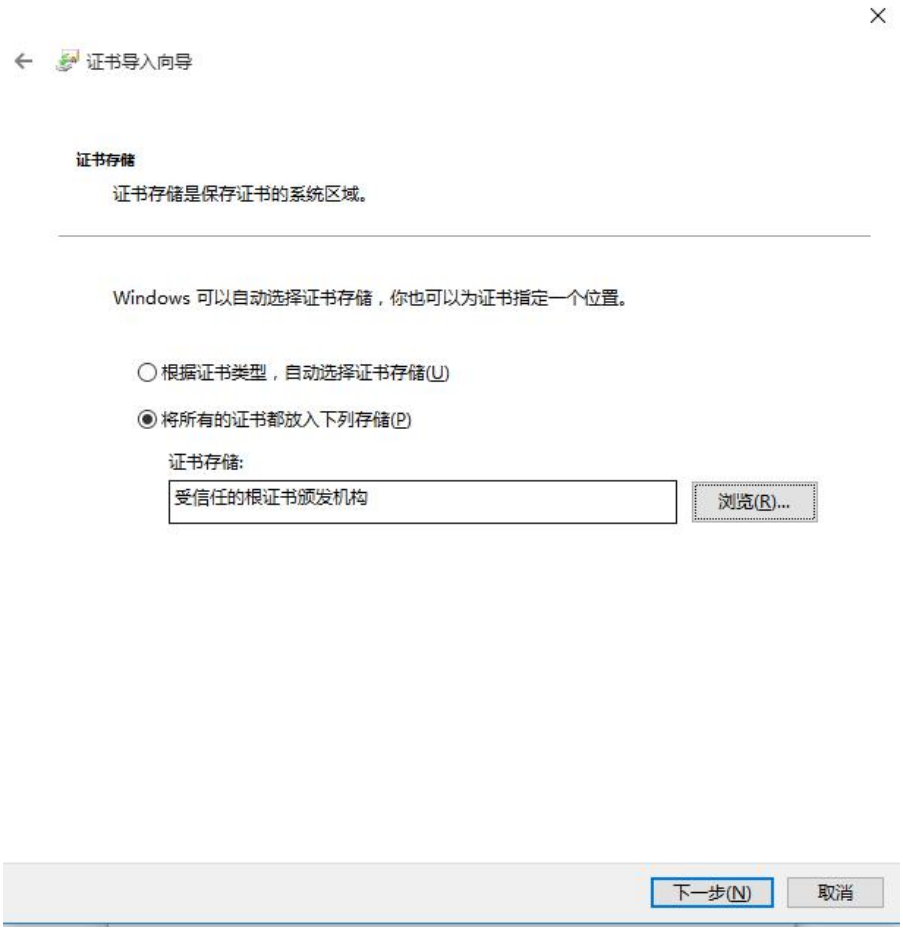
在次登录页面，点击证书下载

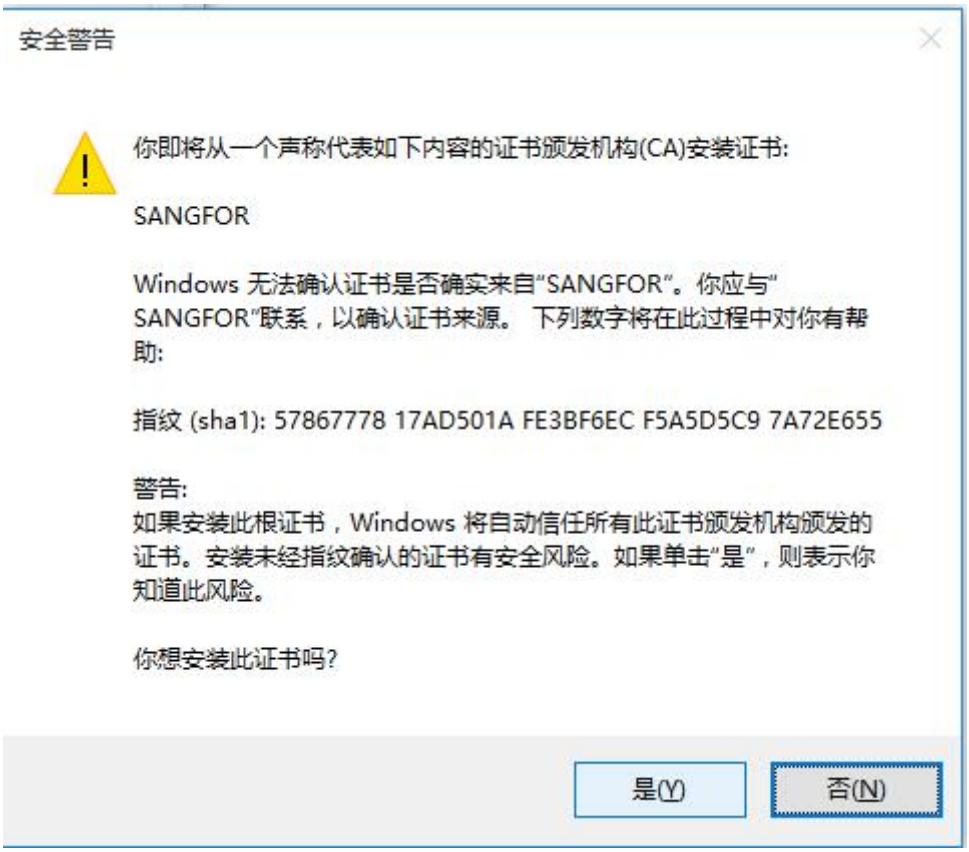


证书下载到本地后，双击证书进行安装，安装完成后再重新登录，就不会弹出警告框了。


证书
常规
详细信息
证书路径
证书信息
此 CA 根目录证书不受信任。要启用信任，请将该证书安装到"受信任的根证书颁发机构"存储区。
颁发给: SANGFOR
颁发者: SANGFOR
有效期从 2011/9/1 到 2028/10/30
安装证书(I)...
颁发者说明(S)
确定


证书导入向导
欢迎使用证书导入向导
该向导可帮助你将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储。
由证书颁发机构颁发的证书是对你身份的确认，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。
存储位置
当前用户(C)
本地计算机(L)
单击"下一步"继续。
下一步(N)
取消


证书导入向导
证书存储
证书存储是保存证书的系统区域。
Windows 可以自动选择证书存储，你也可以为证书指定一个位置。
根据证书类型，自动选择证书存储(U)
将所有的证书都放入下列存储(P)
证书存储:
受信任的根证书颁发机构
浏览(R)...
下一步(N)
取消



完成安装点击是，在重新登录浏览器就不会提示警告框。

登录页面的电脑安装过证书，警告框才会消除。如果从其他电脑登录设备页面，或者电脑上没有安装证书，那么登录页面还是会弹出警告框。

第 3 章 功能说明

3.1. 监控功能

【监控功能】主要用于查看当天采集日志情况，包括【数据概要】、【资产状况】、【安全事件】、【系统运行】。

3.1.1. 数据概要

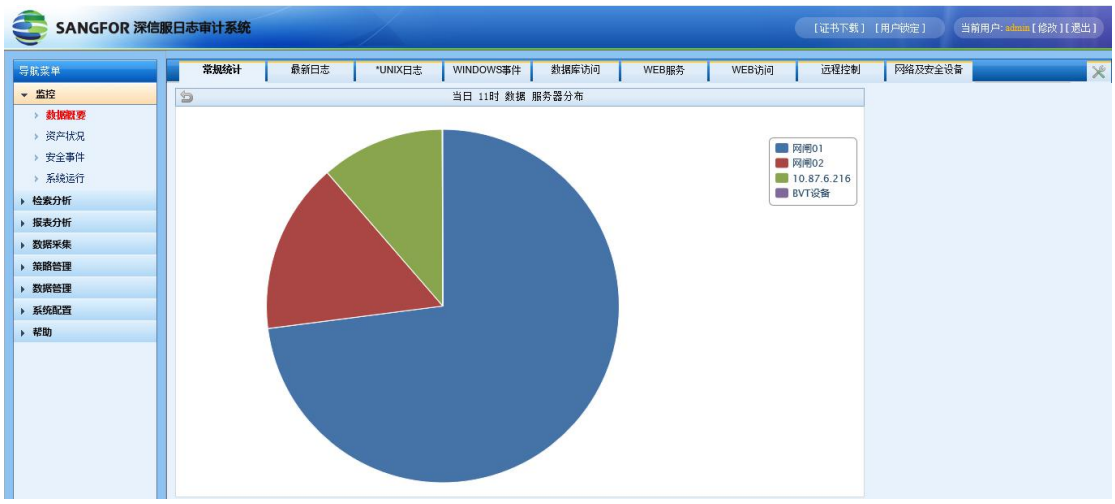
【数据概要】主要用于查看当天采集到的日志，可以实时看到采集的日志情况，包括【常规统计】、【最新日志】、【*Unix 日志】、【WINDOWS 事件】和【数据库访问】等。

3.1.1.1. 常规统计

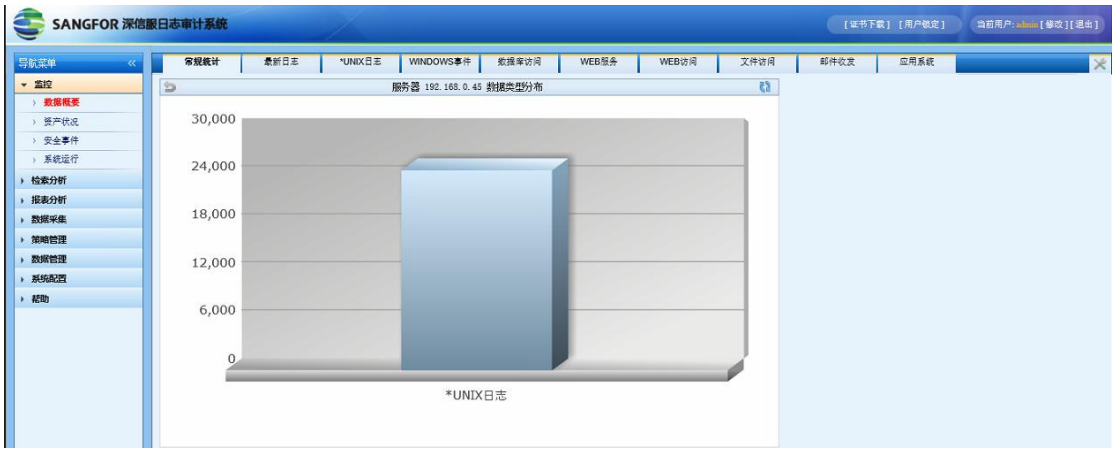
选择导航条上【监控】—>【数据概要】—>【常规统计】，如图所示：

整个首页界面显示 4 块内容 ，以图表形式展现出近期收集的日志数量以及当日系统性能概要

点击当日数据时间分布节点可查看当前目标产生的日志，如图所示：



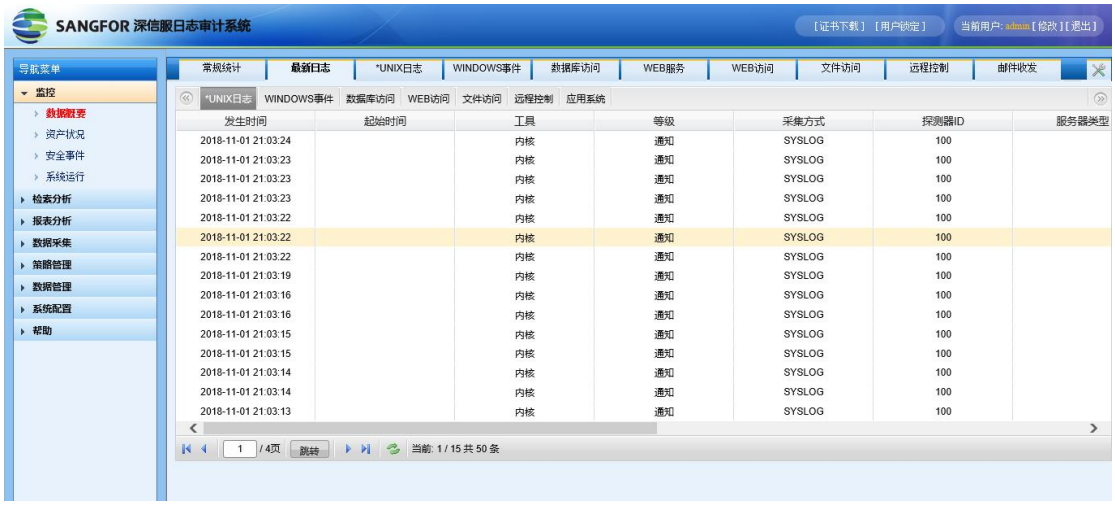
点击当日数据服务器分布其中的某台服务器饼状图，可单独显示这台服务器采集到的日志类型，点进柱状图可查看每个时间段的详细数据量，如图所示：



3.1.1.2. 最新日志

选择导航条上【监控】—>【数据概要】—>【最新日志】，如图所示：

实时动态显示最新采集到的日志列表，查看出最新产生的日志数据(包括*UNIX，WINDOWS事件，数据库访问、WEB 访问等）。

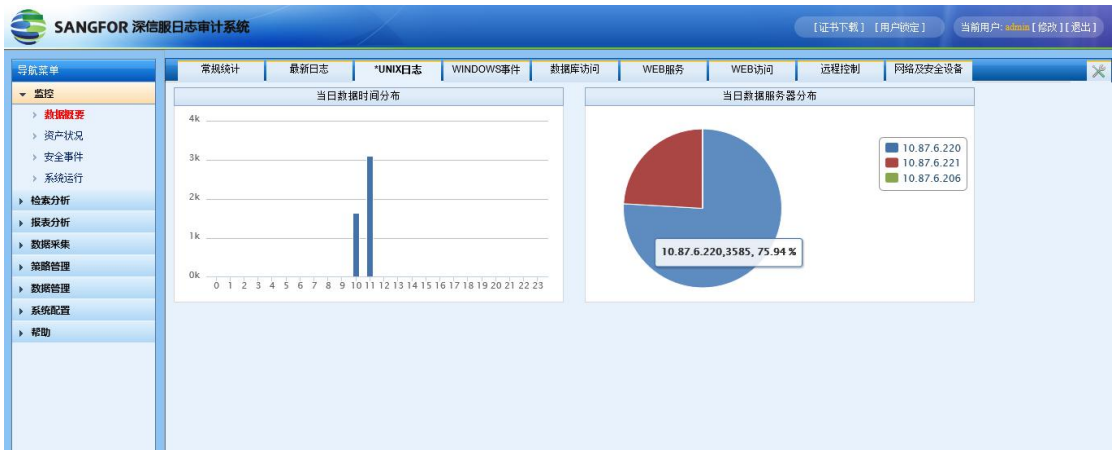


点击列表中任一条日志，可查看此日志的详细内容，如图所示：

3.1.1.3. *UNIX 日志

择导航条上【监控】—>【数据概要】—>【*UNIX 日志】，如图所示：

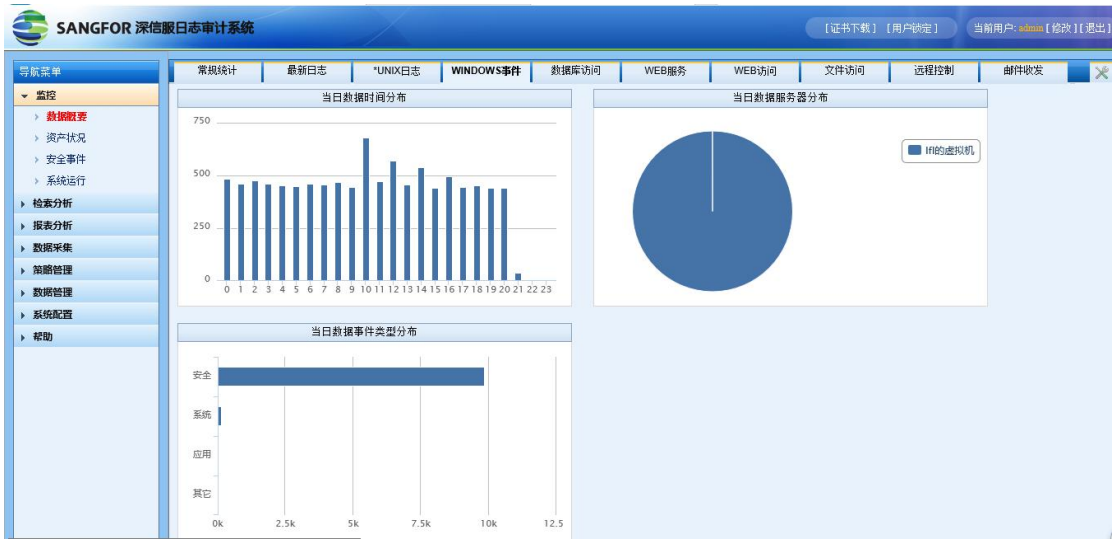
实时动态显示通过 syslog 协议发送过来的 linux、Unix 服务器日志 。



3.1.1.4. WINDOWS 事件

择导航条上【监控】—>【数据概要】—>【WINDOWS 事件】，如图所示：

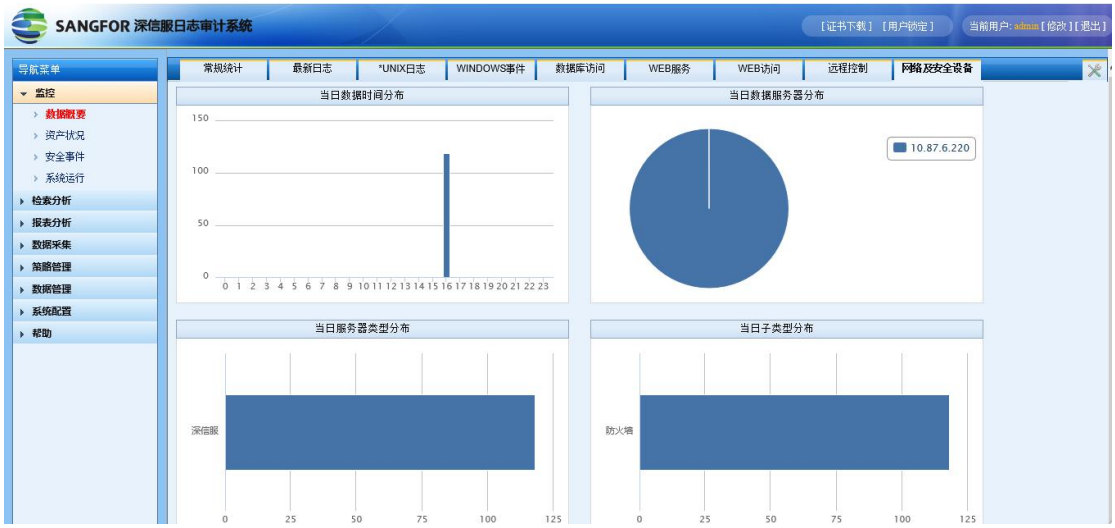
实时动态显示 WINDOWS 事件的日志列表，可查看应用，系统，安全类日志。



3.1.1.5. 网络及安全设备

择导航条上【监控】—>【数据概要】—>【网络及安全设备】，如图所示：

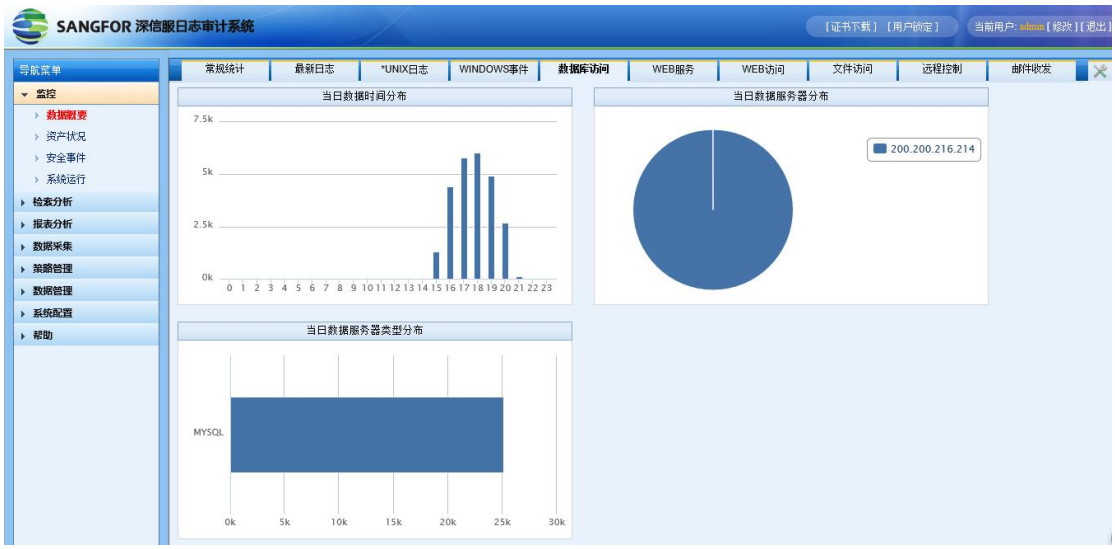
实时动态显示交换机、路由器以及安全设备日志



3.1.1.6. 数据库访问

择导航条上【监控】—>【数据概要】—>【数据库访问】，如图所示：

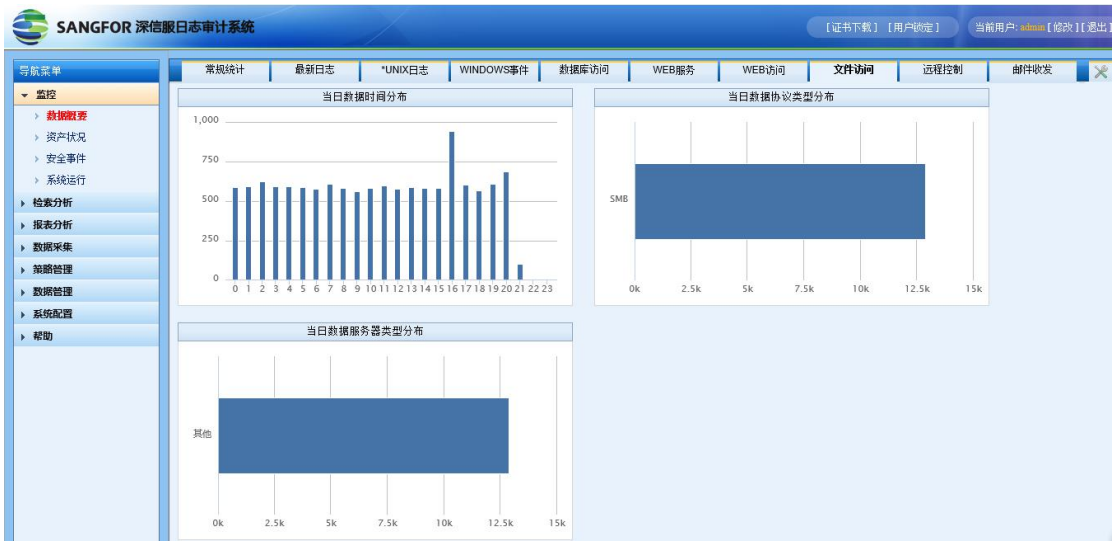
实时动态显示数据库的操作日志，包括查询、增加、删除、修改操作语句



3.1.1.7. 文件访问

择导航条上【监控】—>【数据概要】—>【文件访问】，如图所示：

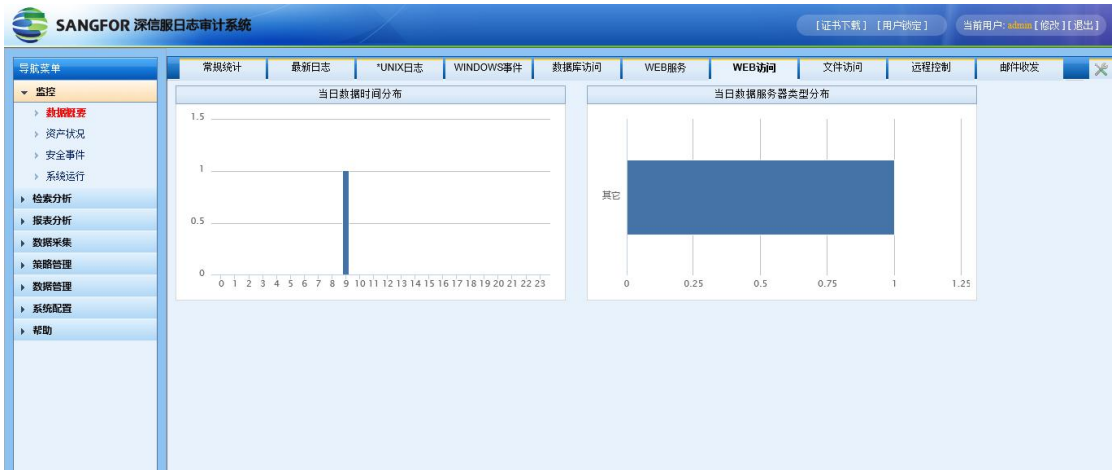
实时动态显示上传下载的文件，可查看 FTP,SMB,HTTP 协议文件访问日志



3.1.1.8. WEB 访问

择导航条上【监控】—>【数据概要】—>【WEB 访问】，如图所示：

实时动态显示客户端访问 web 服务器的 URL 连接信息



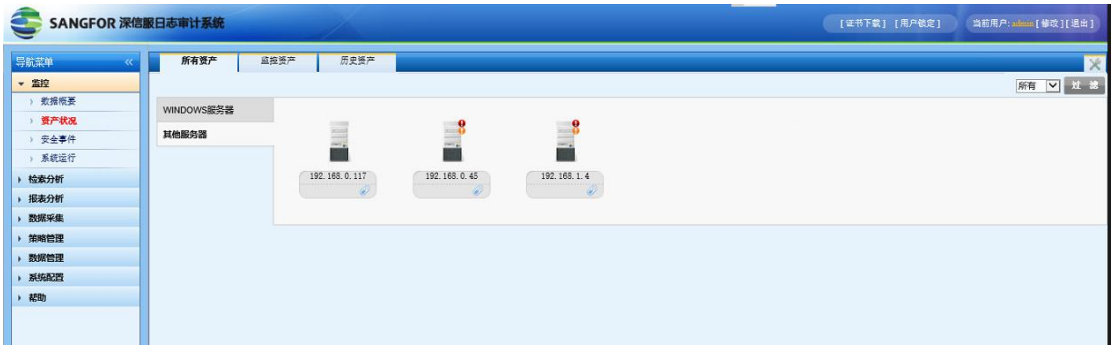
其它类型的模块日志和以上相同，以饼状图或柱状图展现

3.1.2. 资产状况

3.1.2.1. 所有资产

选择导航条上【监控】—>【资产状况】—>【所有资产】，如图所示：

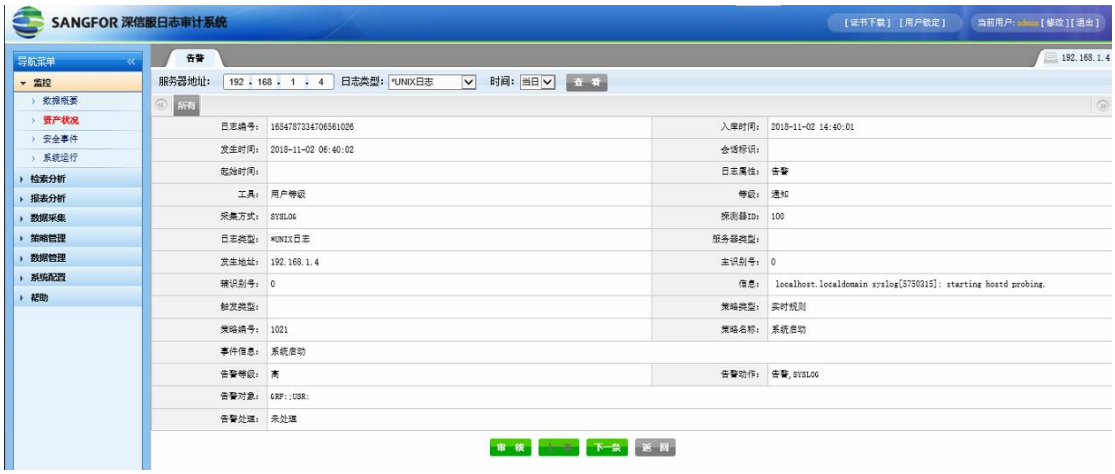
所有资产：可查看所添加的所有资产设备类型及 IP 地址，实时监测资产列表显示内容分为三部分：分为数据，告警及事件日志，区分主机资产的不同信息；



点击资产主机图标上红色感叹号，可查看告警日志，如图所示：

告警日志

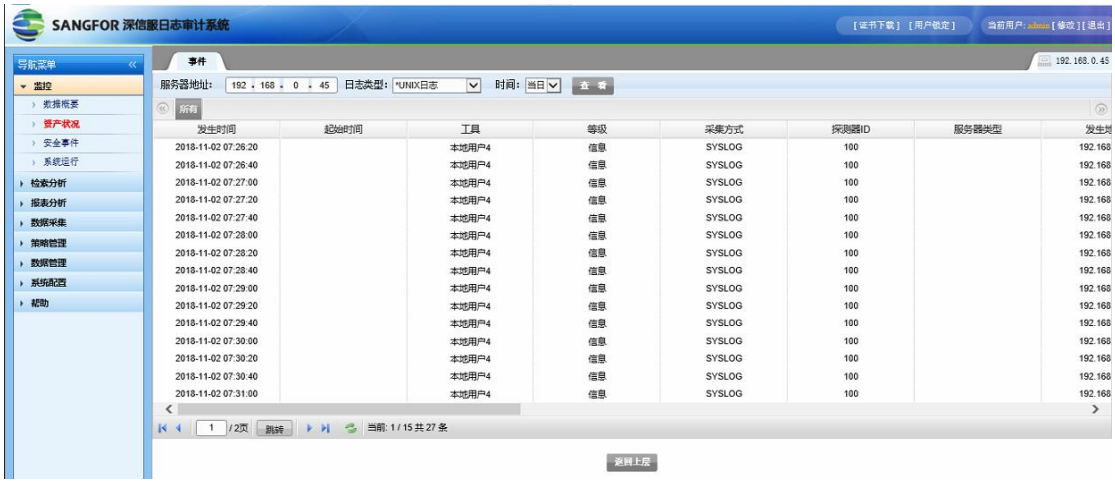
数据日志



日志信息

点击资产主机图标上黄色感叹号，可查看事件日志，如图所示：

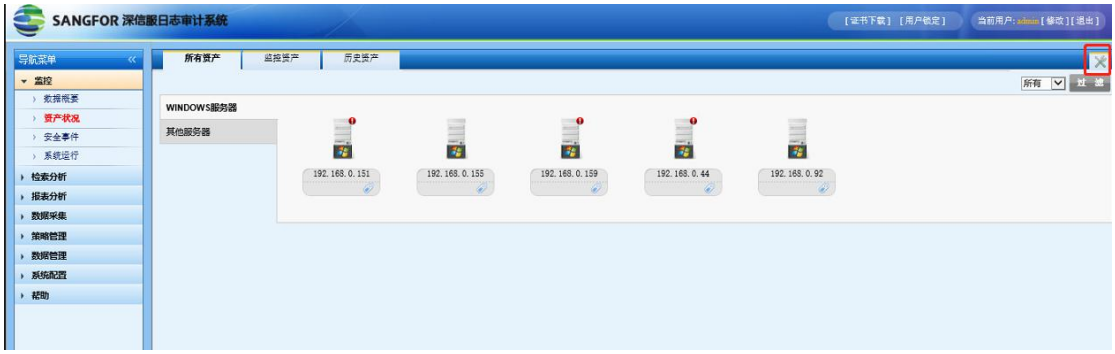
事件日志



数据日志

日志信息

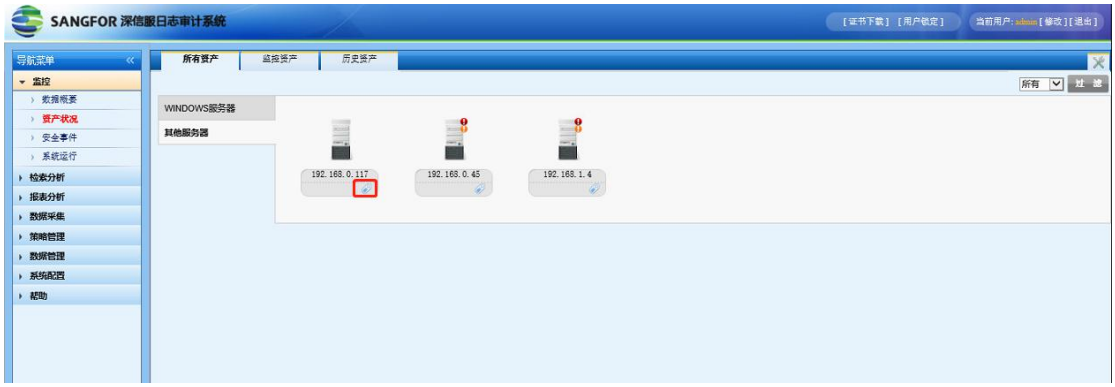
注意右上角标红的配置符号，点击后如下：

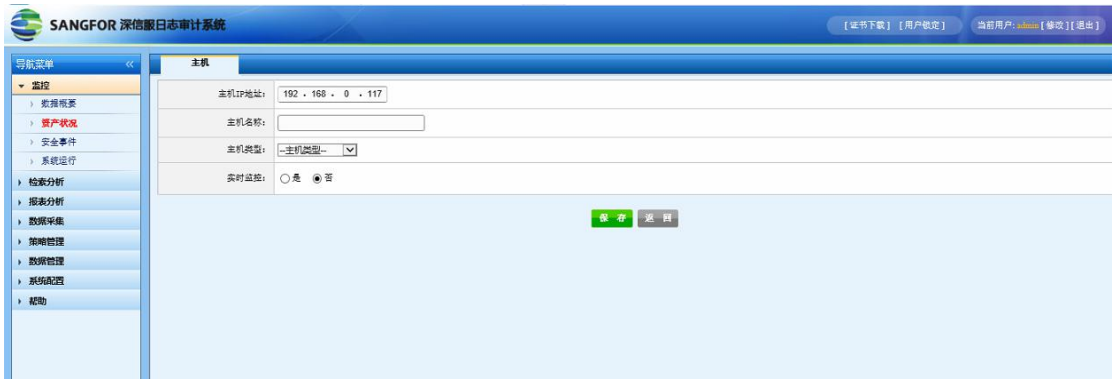


在配置管理里有分类显示与分组显示两种，需要注意的是分类显示情况下，windows 主机直接会被识别成 WINDOWS 服务器单独展现，其它采集过来的主机会默认放到其它服务器里，分组显示是根据【系统配置】--【资产管理】添加主机组，对采集过来的主机添加到不同的主机组里来显示

还有过滤按钮，目前支持对 IP 地址跟主机名两种过滤选项。

点击主机右下方的编辑按钮，可以编辑相关主机，内容与系统管理中的资产管理相同。如下所示：





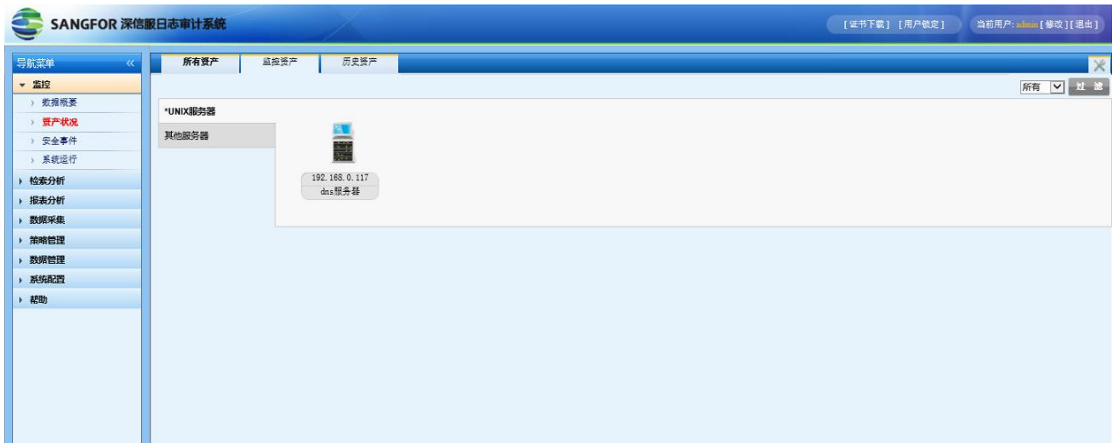
在【系统配置】--【资产管理】添加主机的界面

3.1.2.2. 监控资产

选择导航条上【监控】—>【资产状况】—>【监控资产】：

监控资产：可查看已分类的资产设备类型及 IP 地址，操作信息与【所有资产】相同。所有资产里设置了实时监控的主机将在监控资产里出现。

编辑主机

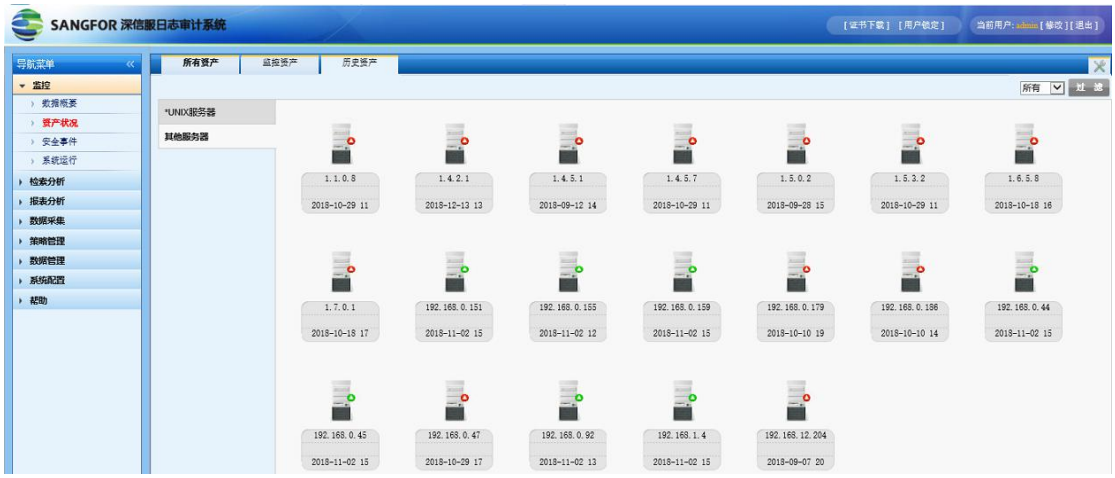


监控资产显示

3.1.2.3. 历史资产

选择导航条上【监控】—>【资产状况】—>【历史资产】，如下所示：

历史资产里的主机就是过去有管理过的主机，其中绿色三角号的说明今天有收到这个主机的日志，红色代表没有。



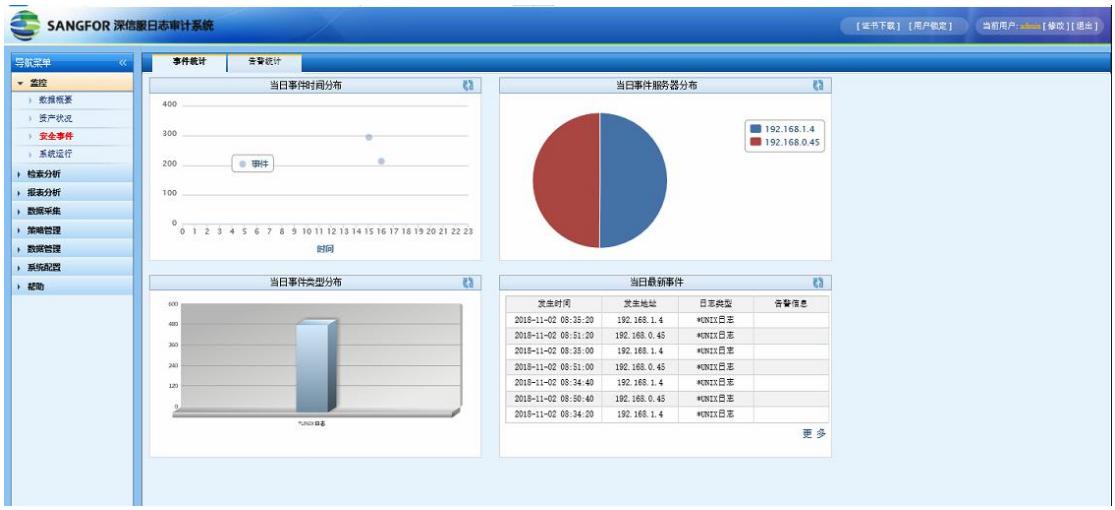
历史资产主机

3.1.3. 安全事件

3.1.3.1. 事件统计

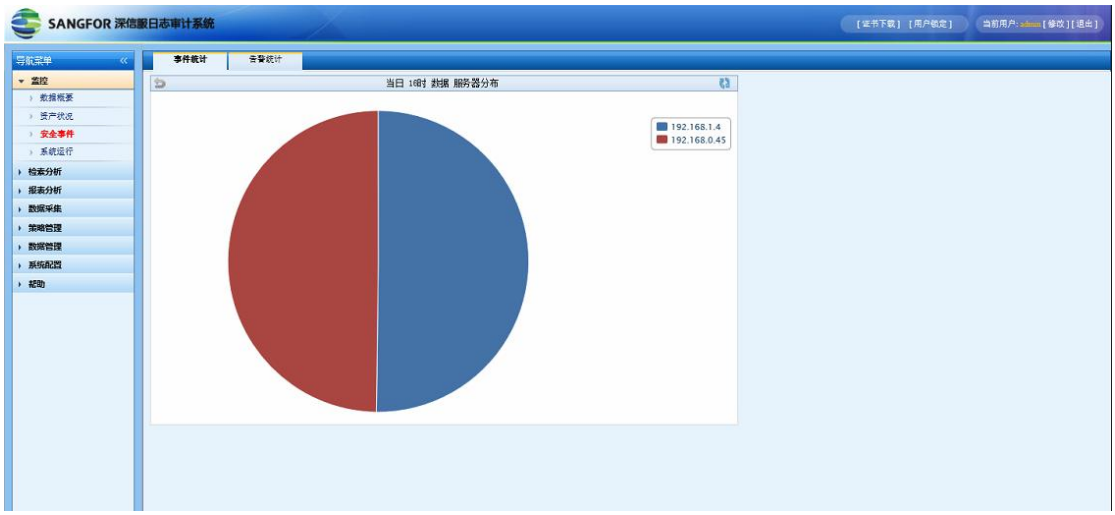
选择导航条上【监控】—>【安全事件】—>【事件统计】，如图所示：

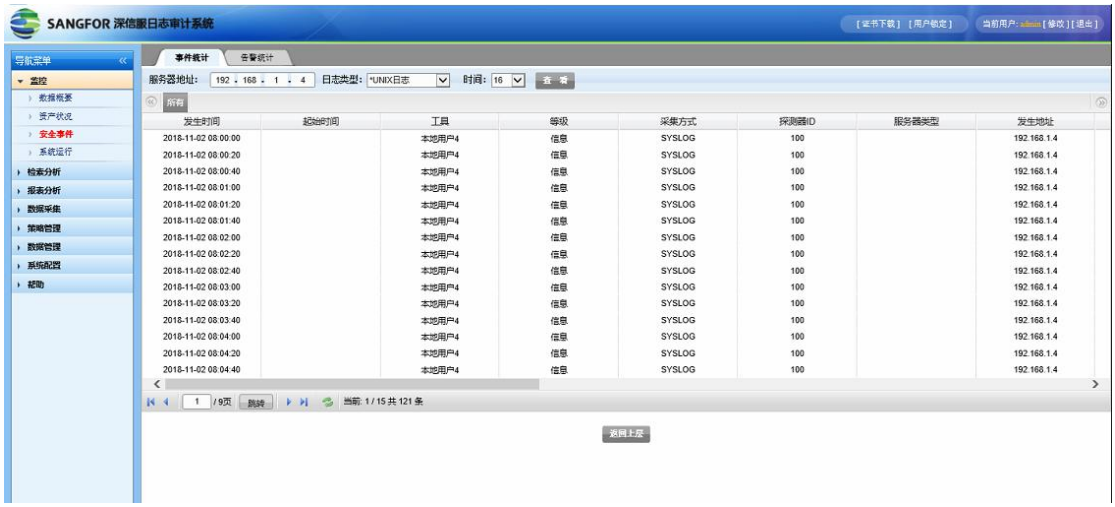
事件统计：查看显示的事件日志统计量，点击任意当日事件时间分布节点可查看当前时间点日志(包括*UNIX，WINDOWS 事件，网络及安全设备事件)，如图所示：



事件统计

显示当日 16 时数据服务器分布，点击饼状图可以看到具体的日志列表





日志列表

点击列表中任意一条日志，可查看此日志的详细内容，如图所示：

日志信息

点击当日最新事件栏目右下角的更多按钮可以查看更多的事件内容。

事件统计

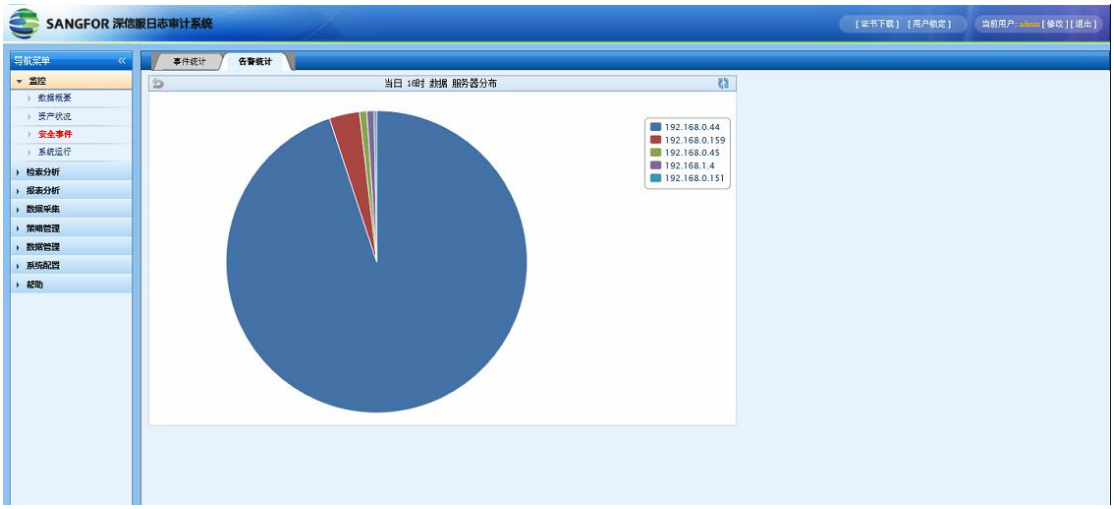
3.1.3.2. 告警统计

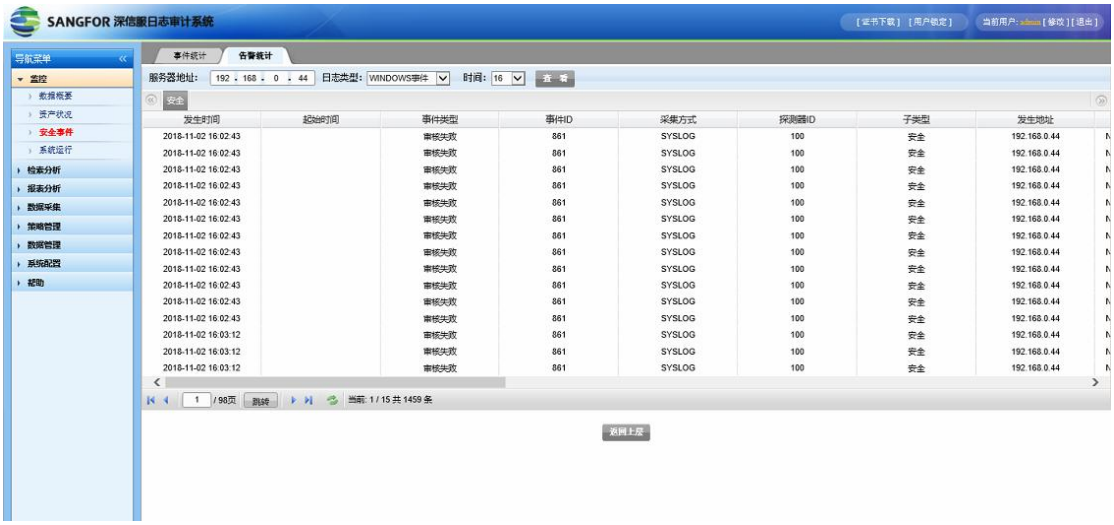
选择导航条上【监控】—>【安全事件】—>【告警统计】，如图所示：

告警统计：查看产生告警的日志统计量。

告警统计

显示当日 16 时数据服务器分布，点击饼状图可以看到具体的日志列表



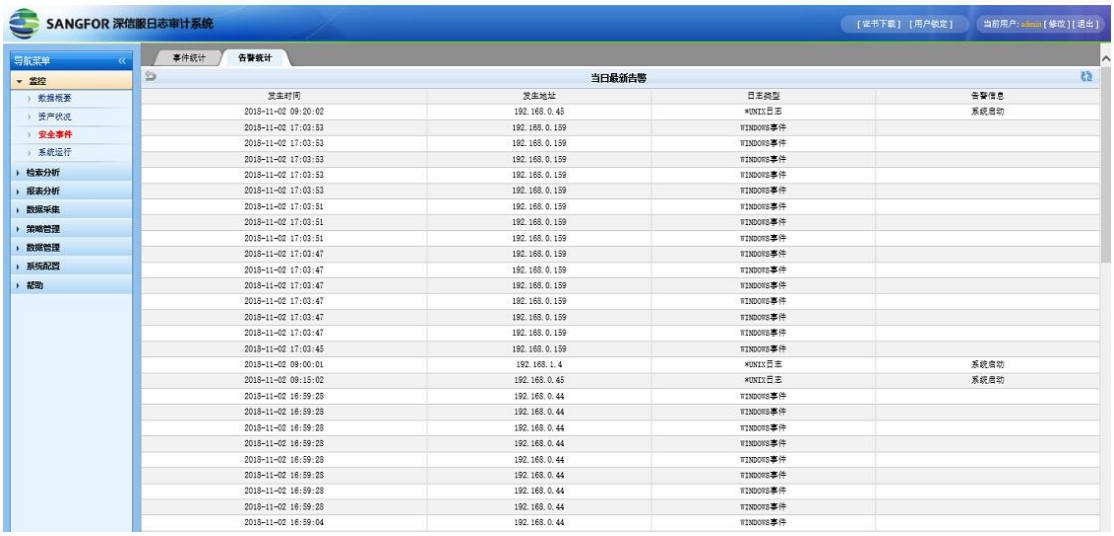


日志列表

点击列表中任意一条日志，可查看此日志的详细内容，如图所示：

日志信息

点击当日最新告警栏目右下角的更多按钮可以查看更多的事件内容。



告警统计

3.1.4. 系统运行

3.1.4.1. 设备状态

选择导航条上【监控】—>【系统运行】—>【设备状态】，如图所示：

设备状态：查看 CPU，内存，数据储存管理，系统储存信息，设备信息（包括客户名称，设备型号，设备序列号，起始时间，时间期限，当前版本编号）。

系统状态（包括运行时间，日志中心状态，raid 状态和网口状态），日志中心是代表日志主机能否正常收取日志的状态，状态的更迭一般要有 10 分钟左右的缓冲时间。

设备信息

3.1.4.2. 运行状态

选择导航条上【监控】—>【系统运行】—>【运行状态】，如图所示：

运行状态：查看审计设备的运行状态，加载的运行规则。

3.1.4.3. 最新日志

选择导航条上【监控】—>【系统运行】—>【最新日志】，如图所示：

最新日志：查看审计中最新的操作日志。

最新日志

点击列表中任意一条日志，可查看此日志的详细内容，如图所示：

日志信息

3.2. 检索分析

【检索分析】功能包括【日志检索】、【事件检索】、【告警检索】、【高级检索】。

日志检索：检索所有的日志入库信息包含系统日志、操作日志、应用日志等类型。

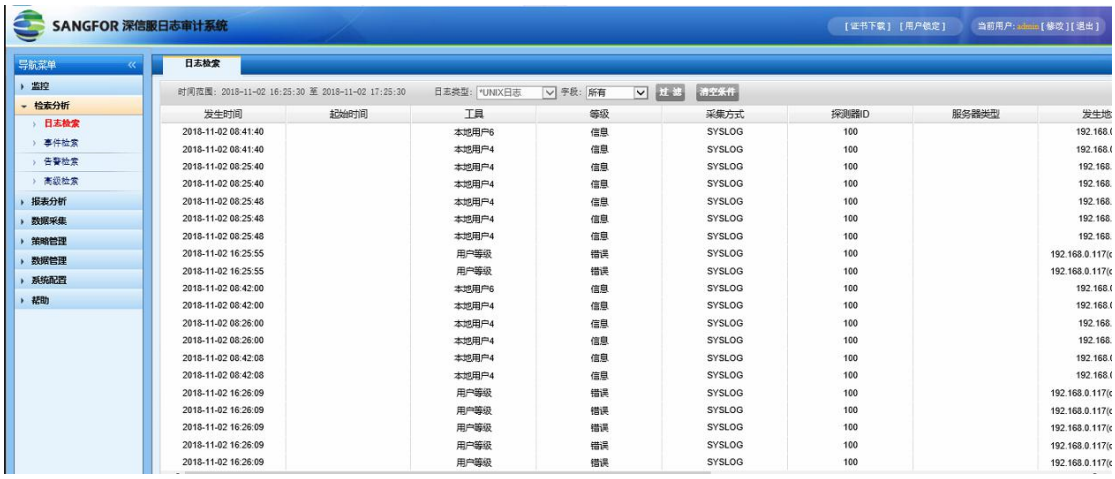
事件检索：基于【策略管理】—【实时规则】(详细配置参见第九章节)中定义的安全事件的检索。

告警检索：基于【策略管理】—【实时规则】(详细配置参见第九章节)中定义的安全事件的检索。

高级检索：基于日志属性、类型、时间以及日志所含关键字进行多重条件组合的检索。

3.2.1. 日志检索

选择导航条上【检索分析】—>【日志检索】，日志检索：通过条件筛选查看具体日志数据， 在检索中可选择“时间范围”、“日志类型”与日志类型配套的“字段”，通过“过滤”来筛选所需要的日志，可以通过“清空条件”来重新添加检索条件。选择“过滤”后，产生检索日志结果（在检索之后还可以在之前的检索结果中继续进行检索），如图所示：



日志列表

点击列表中任意一条日志，可查看此日志的详细内容，如图所示：

日志信息

日志检索示例：查询 2018-11-1 至 2018-11-2 日志类型为 WINDOWS 事件，发生在

192.168.0.159 上的日志。

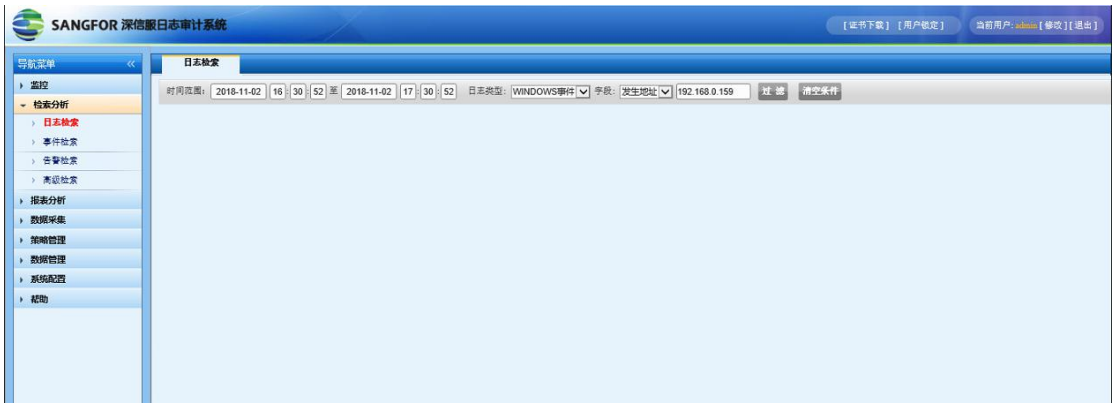
1、先点击“清空条件”

2、选择时间范围：2018-11-1 至 2018-11-2。

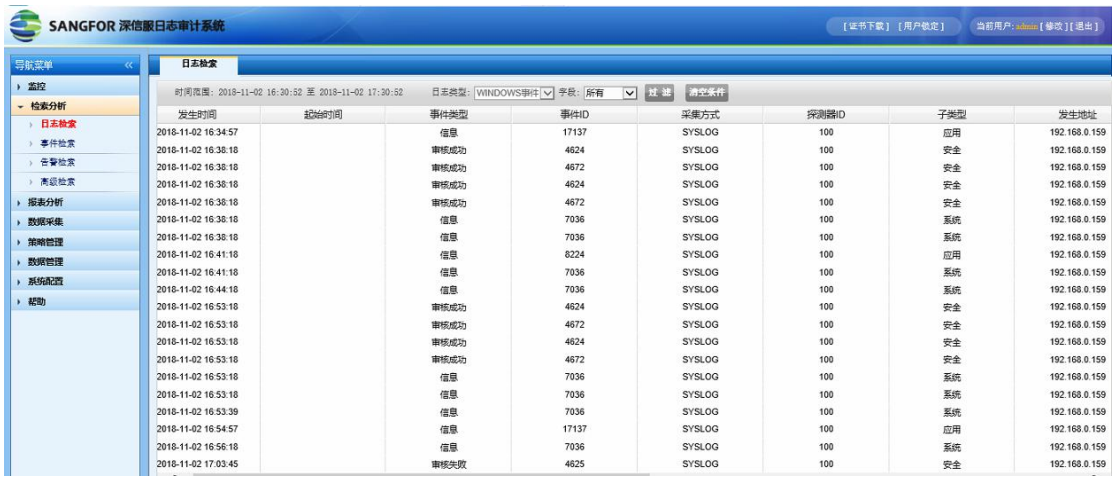
3、日志类型栏选择 WINDOWS 事件；

4、字段栏中选择发生地址：192.168.0.159，点击过滤；

5、即可在过滤列表中点击查看日志的详细内容。如图、、所示。



日志查询条件

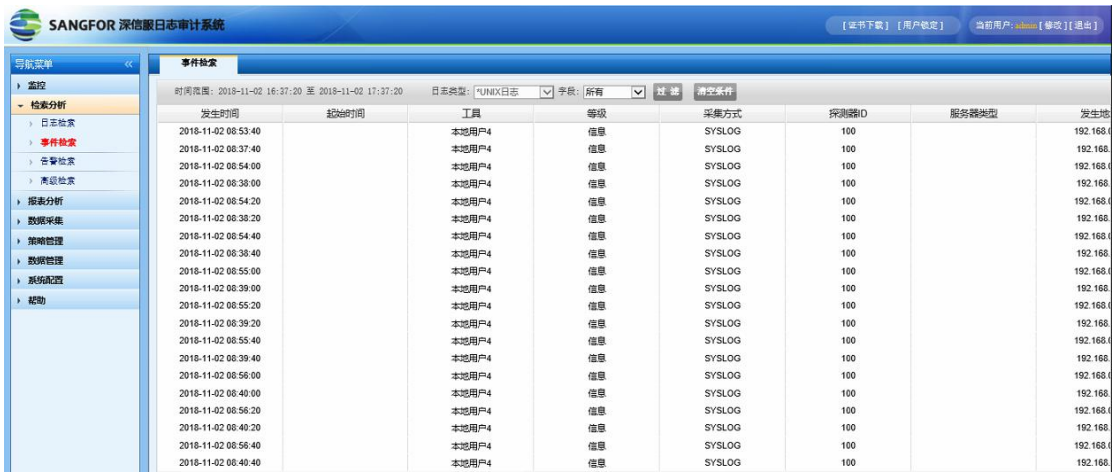


日志查询结果

日志详细信息

3.2.2. 事件检索

选择导航条上【检索分析】—>【事件检索】；检索方式如日志检索功能；选择“过滤”后，产生检索日志结果（在检索之后还可以在之前的检索结果中继续进行检索），如图所示：



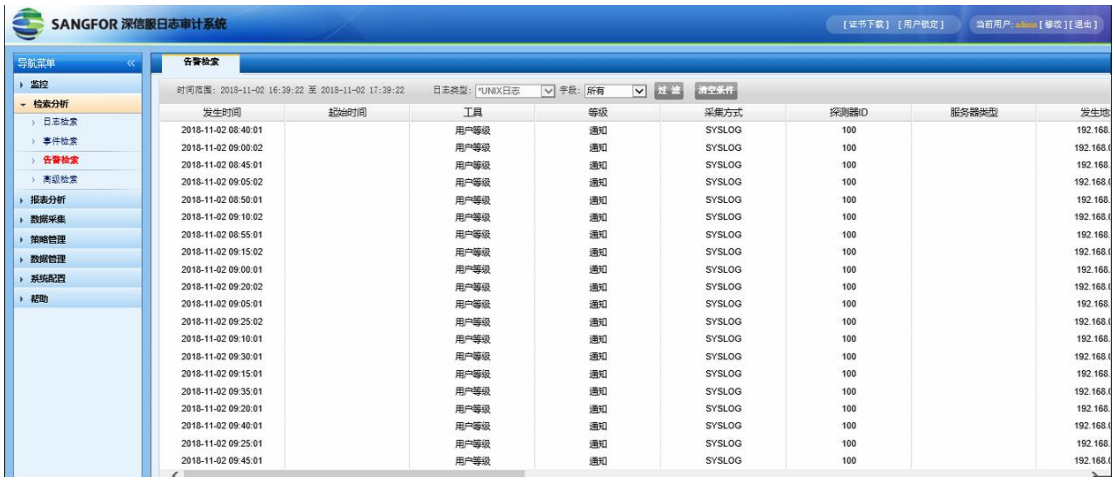
日志列表

点击列表中任意一条日志，可查看此日志的详细内容：如图所示：

日志详细信息

3.2.3. 告警检索

选择导航条上【检索分析】—>【告警检索】；选择“过滤”后，产生检索日志结果（在检索之后还可以在之前的检索结果中继续进行检索），如图所示：



日志列表

点击列表中任意一条日志，可查看此日志的详细内容：如图所示：

日志详细信息

3.2.4. 高级检索

选择导航条上【检索分析】—>【高级检索】—>【高级检索】，如图所示：

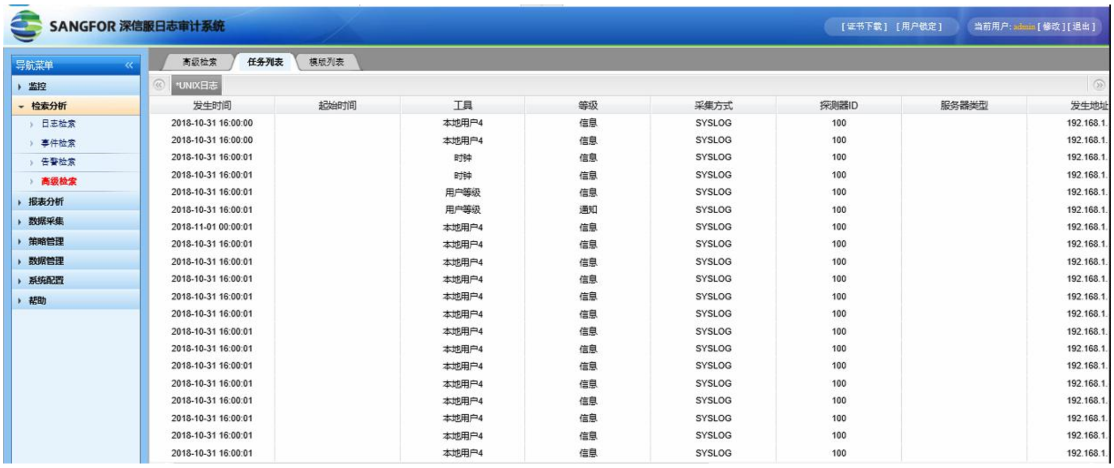
高级检索：通过条件筛选查看各种组合条件下的日志，可生成模版供以后检索，包括【日志属性】选择，【入库时间】调整，【日志类型】选择，【模版】保存。在数据比较大的情况下检索会先显示部分日志

高级检索

在日志类型中还有【插入同级条件】及【添加子条件】，可供多样选择条件同时查询及分类细致查询。如图所示：

同级条件及子条件

选择好查询条件后，点击【检索】，检索的结果会显示在【任务列表】中，如图所示：



日志列表

点击列表中任一条日志，可查看此日志的详细内容：如图所示：

日志详细信息

查询 2018-11-1—2018-11-2 日志类型为 WINDOWS 事件日志，事件类型为“审核失败”，

发生地址为“192.168.0.44”，事件 ID 为“861”的日志。

1、选择入库时间范围，2018-11-1—2018-11-2；

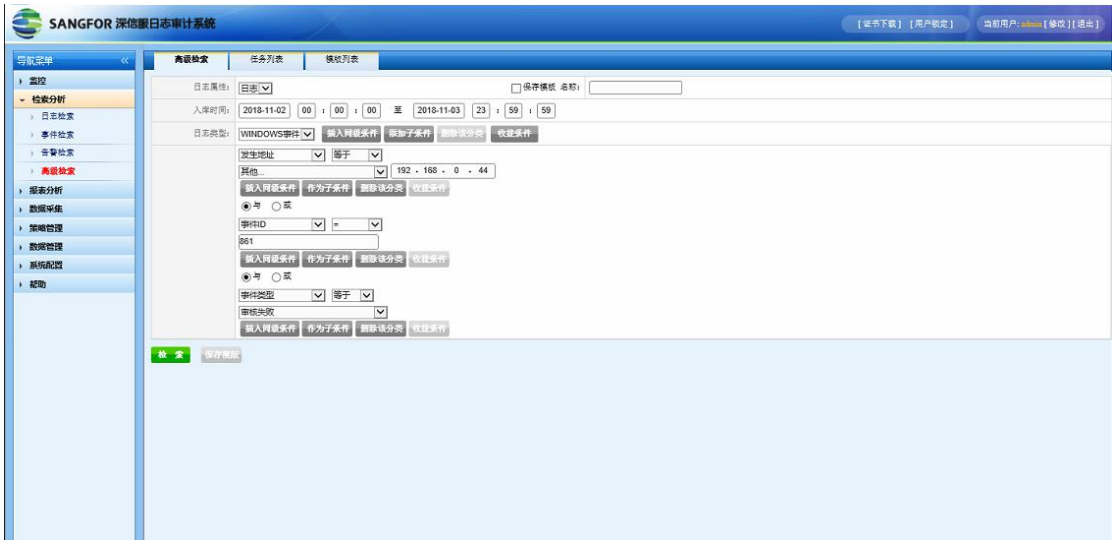
2、日志类型栏选择 WINDOWS 事件；

3、添加子条件，服务字段中选“事件类型”“发生地址”“事件 ID”；

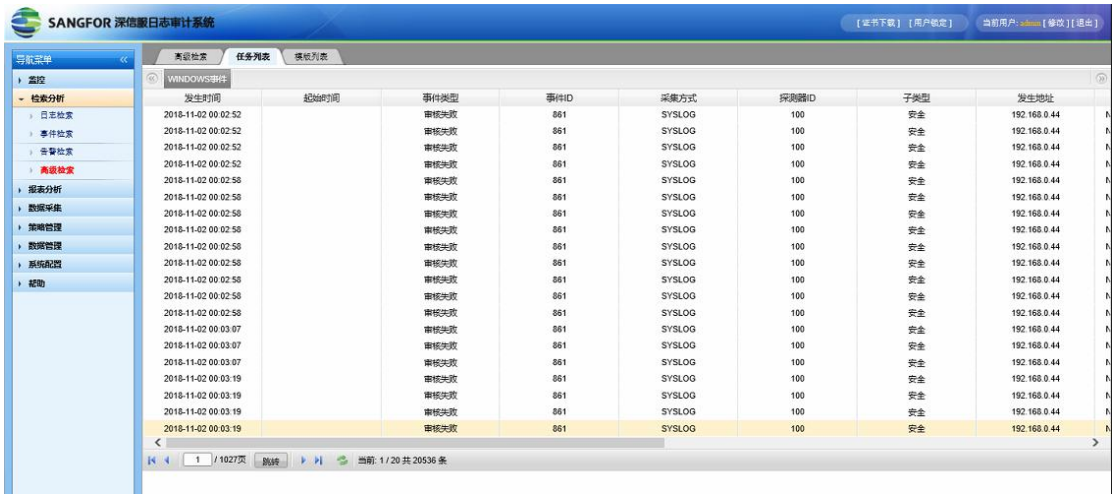
4、再插入同级条件，条件选择“与”，在字段中选择“事件类型”“等于”“审核失败”；

5、再插入同级条件，条件选择“与”，在字段中选择“事件 ID”“=”“861”，点击检索或保存此模板。

7、在过滤出来的列表中可查询其中日志的详细内容。如图,,



高检检索条件



查询结果列表

查询日志详细信息

3.3. 报表分析

【报表分析】功能主要用于事后的日志审计通过报表的形式展现出来，包括【手动任务】、【计划任务】、【报表管理】。

SANGFOR-LAS 日志管理审计系统拥有强大的报表功能，内置能够满足不用客户审计需求的安全审计报表模板，支持自动或手工方式生成日志审计报表，审计报表还可以根据各行业审计需求、国家法律法规相关要求进行专门设计。

- ✓ 支持报表自定义扩展；
- ✓ 支持柱状、饼、折线等多种方式对统计数据进行展示；
- ✓ 支持按天、周、月自动周期性生成报表；
- ✓ 支持报表自动发送功能；
- ✓ 支持生成的格式为 HTML、PDF、CSV、XML

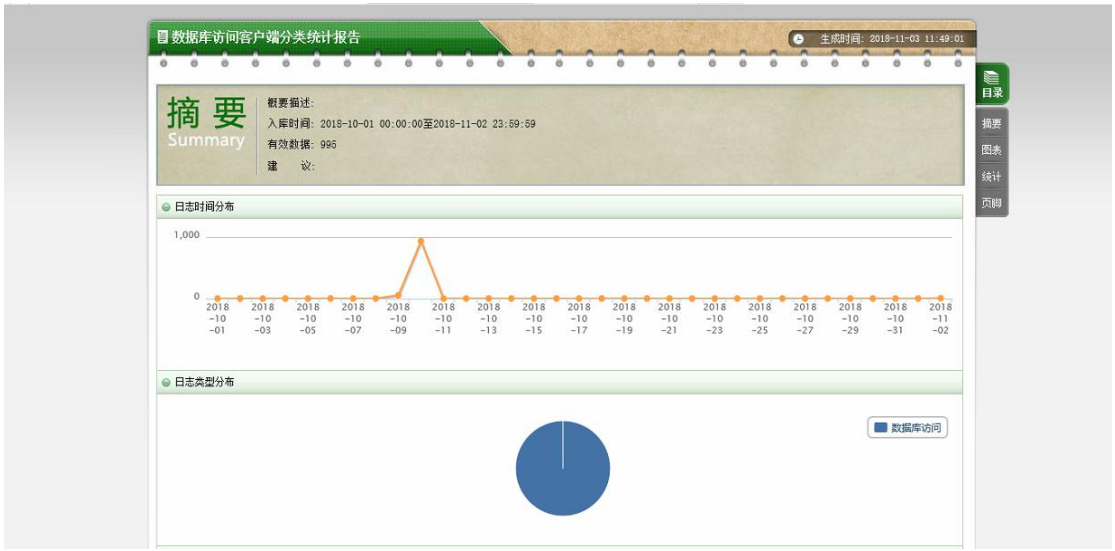
3.3.1. 手动任务

选择导航条上【报表分析】—>【手动任务】—>【手动生成】，如图所示：

手动任务：查看手动生成的历史任务报表

报表列表

生成的报表在“动作”下提供【查看】与【下载】，点击【查看】，如图所示



3.3.2. 计划任务

选择导航条上【报表分析】—>【计划任务】，如图所示：

计划任务

计划任务：查看定期自动生成的任务报表，可分为：D 日报，W 周报及 M 月报三种。需要注意的是计划任务最多只记录 20 条，所有用户加起来的总数不会超过 20 条。

计划任务报表的配置是在手动生成报表时设置的，如下，勾选计划任务，里面有选择每日，每周以及每月

计划任务配置

计划任务下面还有个邮件接收选项，勾选后如下所示：

可以看到有个合并发送，意思是比如两个报表需要对比或者同时查看，选择合并发送就会把两个报表同时发到邮箱，方便做对比分析。

3.3.3. 报表管理

选择导航条上【报表分析】—>【报表管理】—>【模板配置】，如图所示：

报表配置：针对不同需求定制报表模版；

模板配置

点击“添加分类”，增加报表大类选项，如图所示：

添加分类

点击“添加模版”，增加报表模版选项，如图所示：

添加模板

【回显】里显示当前模版设置的具体内容，如图所示：

回显模板

选择导航条上【报表分析】—>【报表管理】—>【全局设定】，如图所示：

- ✓ 报表背景：可给该上传背景取名称
- ✓ 报表图片：点击“浏览”可上传模版背景图片
- ✓ 全局设定里的背景和图片是指生成 PDF 格式报表时里面的背景字样和图片。如果有客户认为不需要可以删掉，这样生成的报表不会有背景。

3.4. 数据采集

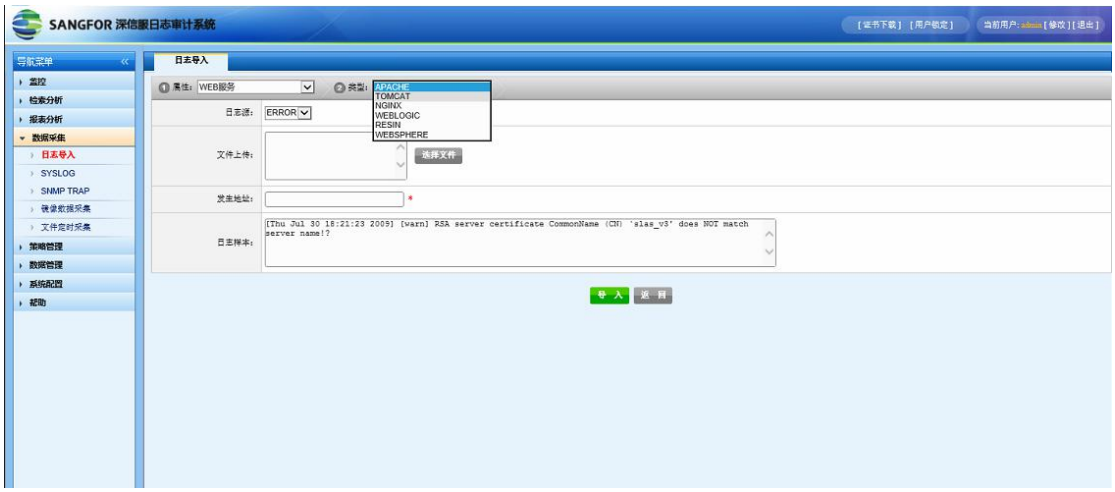
【数据采集】功能包括【日志导入】、【SYSLOG】、【SNMP TRAP】、【镜像数据采集】、【文件定时采集】。

3.4.1. 日志导入

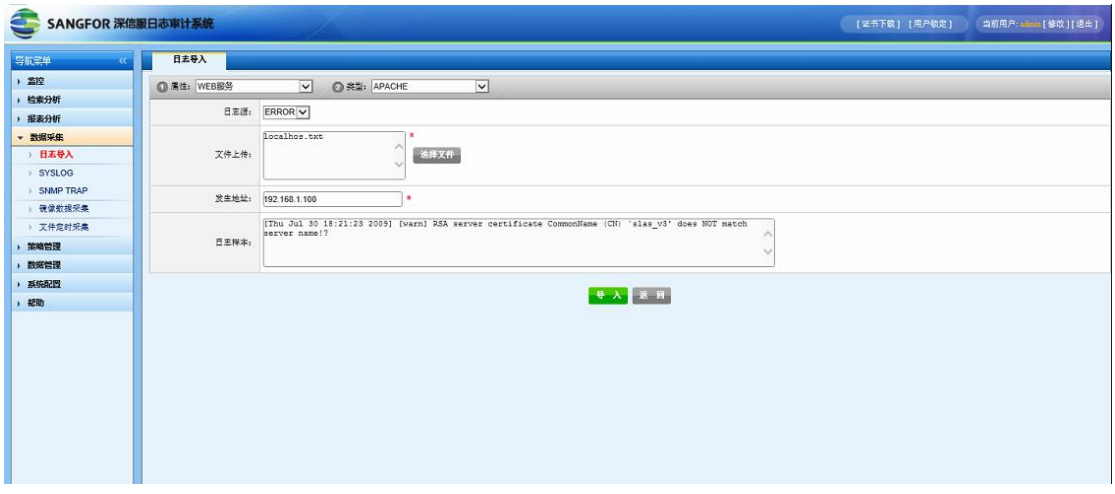
选择导航条上【数据采集】—>【日志导入】，如图所示：

用户可以点击【添加】将原始日志文件导入到 SANGFOR-LAS 日志审计系统中，再通过日志审计系统去对日志进行检索、分析；

点击【添加】如图所示：

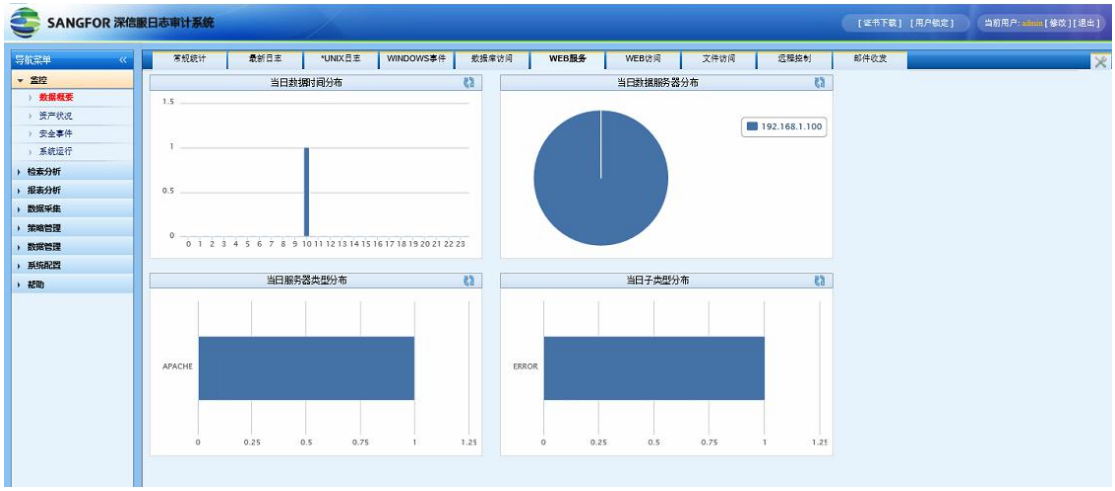


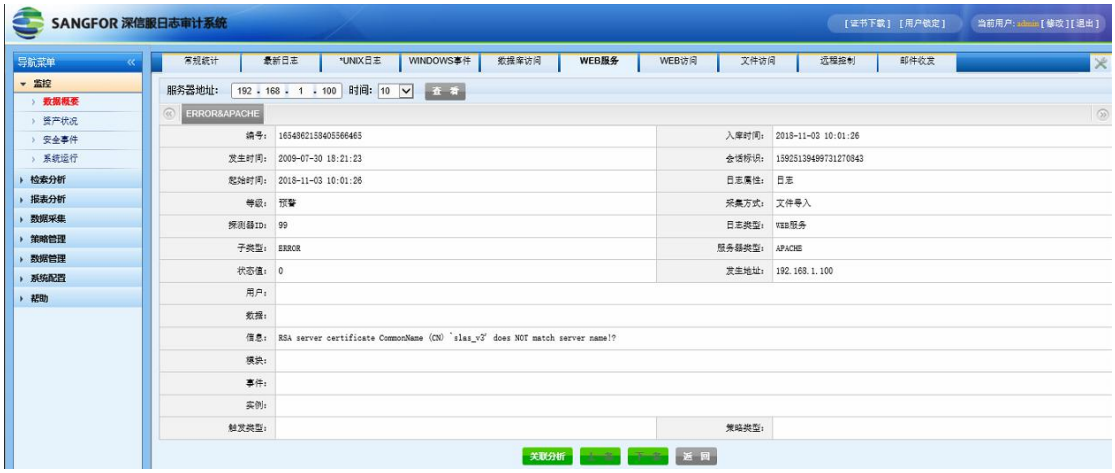
添加 WEB 服务 APACHE 的文件日志，添加完成点击导入



返回日志导入可以看到状态是成功还是失败

在【数据概要】—>【WEB 服务】里可以看到导入的 APACHE 文本日志





可选择文件的属性和类型如下表：

属性	类型
*UNIX	
Windows 事件	Windows xp、Windows VISTA、

	Windows 2003、Windows 2003、windows 2008 等
网络安全设备	CISCO、H3C、神州数码等
AS400 日志	AS400
数据库访问	MYSQL
WEB 访问	APACHE、IIS、TOMCAT 等
文件访问	VSFTPD、IISFTPD、SERV-U 等
数据库服务	ORACLE、SYBASE、MSSQL 等
WEB 服务	APACHE、TOMCAT、NGINX 等
FTP 服务	VSFTPD、NCFTPD、PROFTPD 等
应用系统	Log4j

导入日志时需选择相应的日志属性、类型和日志源否则会导入失败，日志导入可以单个文本导入，也可以用压缩包导入，如果一个压缩包中有不同类型的日志，SANGFOR-LAS 审计系统只会导入符合的日志文件，填写日志发生的服务器地址或网站域名，检索时可辨识日志的所属。

支持的压缩格式：rar、zip、tgz、tar、gz、tar、tbz、tar、bz2、gz、tar、gz、bz2、tar、bz2、7z。

3.4.2. SYSLOG

选择导航条上【数据采集】—>【SYSLOG】，如图所示：

【syslog】可以自定义设置需要采集的 syslog 日志的属性、类型和日志源，以及日志的特征和发生的服务器地址，如图所示：

编码：安全设备采集过来的日志信息中会包含中文，如果不配置编码那日志信息中包含中文的会显示为乱码

过滤信息：将采集过来的日志通过固定长度和固定字符串的方式，去掉日志信息前面部分的内容

特征信息：针对信息中匹配的内容进行采集，不匹配的不会采集

原始文件：采集过来的日志会在后台以文本的形式在 ORIGIN 目录保存，不做解析。

默认 syslog 采集过来的日志会统一放到*UNIX 日志下，采集网络及安全设备日志需要通过配置 syslog 进行分类，放到网络及安全设备模块下。

Syslog 常被称为系统日志或系统记录，是一种用来在互联网协定（TCP/IP）的网络中传递记录文档讯息的标准。

syslog 提供了一个便于管理员理解日志的机制。系统日志消息中有标准格式的消息（称为系统日志消息、系统错误消息或简单系统消息），也有从调试命令输出的消息。这些消息是在网络运作过程中生成的，旨在指明网络问题的类型和严重程度，或者帮助读者用户检测

路由器的活动，比如配置的变更。

3.4.3. SNMP TRAP

选择导航条上【数据采集】—>【SNMP TRAP】，如图所示：

【SNMP TRAP】的用法和 SYSLOG 是一样的，对采集过来的网络及安全设备进行分类，包括网络安全设备日志的源、类型和发生地址，如图所示：

3.4.4. 镜像数据采集

选择导航条上【数据采集】—>【镜像数据采集】，如图所示：

该功能通过交换机和镜像口获取网络流量，选择启用或停用来开启对应协议的日志采集功能；若存在多个端口则用逗号分开。

采集的类型日志如下表：

模块名称	协议类型	记录说明
数据库模块	ORACLE、MSSQLINFORMIX、SYSBASE、DB2、MYSQL、DM	记录查询、增加、修改、删除操作日志
文件传输模块	FTP、SMB、HTTP	记录文件上传、下载日志
邮件模块	SMTP、POP、HTTP	简单记录时间、发送者、接收者以及邮件主题日志
远程控制模块	TELNET	记录远程 telnet 到交换机或路由器操作日志
应用服务模块	DNS	记录 DNS 解析日志
网站访问模块	HTTP	记录浏览网页 url 日志

【特定服务器】用于有长连接应用的数据库服务器，即某些应用在审计系统上线前已经连接至数据库服务器且长期保持连接会话。配置特定服务器可以使审计系统能够准确捕获、分析长连接操作记录。由于系统上线时，长连接应用已经完成数据库登陆过程，所以对于长连接数据库访问，审计系统无法分析出数据库用户名等信息，只能记录时间、IP、端口、操作信息。

【流量监控】可以采集指定服务器的所有网络流量，如图所示：

【数据缓存】针对分布式部署的情况，在流量较大日志审计系统采集不过来的时候可以开启数据缓存功能，在指定时间点将日志推送过来，减轻日志审计系统的压力。

3.4.5. 文件定时采集

选择导航条上【数据采集】—>【文件定时采集】，如图所示：

文件定时采集

此功能会将客户端发送至 SANGFOR-LAS 日志审计系统的日志存储至指定目录下，并定时去扫描目录下的日志，对日志进行检析，点击【添加】进行详细的设定如图所示：

文件定时采集设置

添加时选择相应的日志属性、类型和日志源，可以在【文件目录】下指定存储的目录，【文件名格式】中自定义指定文件名格式，如添加 localhost.log，填写【发生地址】或【网站域名】以便得知日志的所发生的服务器，目前时间格式只支持连续的 YYYYMMDD，即 20181018 这种，中间不能加符号。

3.5. 策略管理

【策略管理】功能包括【内置规则】、【实时规则】、【知识库】。

3.5.1. 内置规则

选择导航条上【策略管理】—>【内置策略】，设置关联分析如图所示：

内置策略

【归并策略】默认启用对 HTTP 访问数据对同一会话的日志进行归并。

【关联分析】可以设置用户在登陆数据库的规定时间内因多次操作错误而产生告警或事件；可以通过短信网关、邮件、SYSLOG、SNMP TRAP 将告警信息日志进行外发。

3.5.2. 实时规则

选择导航条上【策略管理】—>【实时规则】，设置关联分析和数据策略如图所示：

实时规则

用户可在此增加、删除、修改和导入导出实时分析规则；规则定义通过多重条件匹配，根据用户关注点对海量日志进行筛选、定义、告警或者丢弃；规则定义可将采集到的日志类型分成丢弃、事件、告警三类；实时分析规则可包含两层规则定义，第一层规则下可添加子类规则；点击【编辑】可查看、修改现有规则条件；点击【添加】，如图所示：

点击【添加】增加新规则，如图所示：

增加新规则

增加新规则：输入易识别的<规则编号>、<名称>、<描述>信息；规则条件可选择所有服务列表并相应的服务字段来定义；通过勾选<增加条件>可添加无穷层级规则条件匹配；新规则定义应优先定义大类规则，如：数据库类、SYSLOG 类、网络行为类、系统日志类等；然后在此大类下增加子类规则进行细分。告警日志规则定义：若此规则定义为产生告警，则需

要选择告警等级、输入选择告警信息、告警方式选择短信网关、邮件、SYSLOG、SNMP TRAP 告警（已配置好告警接口）；

设置规则条件：需要注意逻辑关系以及运算顺序（括号的操作），以保证规则正常的被使用；丢弃规则拥有最高优先级；子类规则应该是对上层规则的细化，脱离了上层规则是无效的；规则设置需要注意：规则以树型结构设计；对后续规则的设定要仔细：如日志不符合当前规则定义，此规则是否跳转或结束，跳转会继续匹配到下一条规则定义；定义不当会引起日志是否正确的被反应在实时审计中；严重情况会出现定义的敏感日志信息没有产生告警，破坏系统的实时性与功能性；

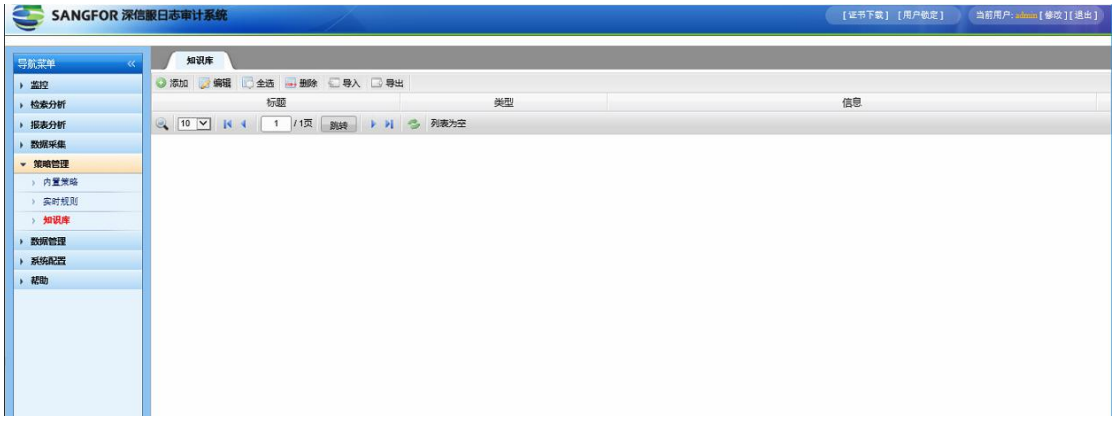
选择要增加子类规则的项，点击【子类查看】，查看，修改、增加此规则下的子类规则；如图所示：

子类规则列表

子类规则是对父规则的细化定义，增加了规则定义的灵活性；新子类规则的增加操作方法同父规则。

3.5.3. 知识库

选择导航条上【策略管理】—>【知识库】，如图所示：



知识库

用户可以在知识库内添加自己的案例，可以自由的修改和删除，支持导入和导出在知识库内还可以自定义类型进行分类、方便查找。

3.6. 数据管理

【数据管理】功能包括【数据备份】、【数据恢复】、【数据归档】、【归档设置】。

3.6.1. 数据备份

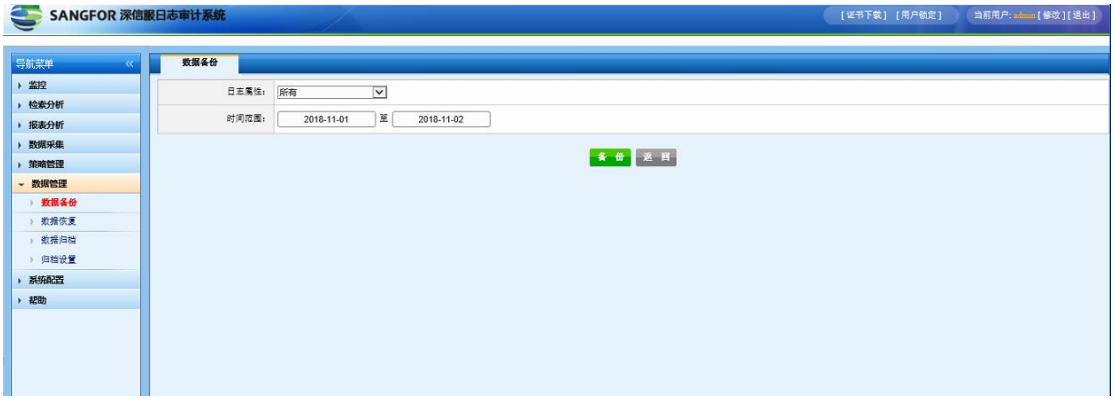
选择导航条上【数据管理】—>【数据备份】，如图所示：

日志备份

管理员可自主选择日志类型、时间范围来备份日志数据，并可以选择备份、备份并删除或直接删除日志数据。故使用此项功能权限的管理员需谨慎。备份任务完成后可下载，或者

选择删除这个备份任务。

日志备份功能是备份文本形式的日志，添加备份，如图所示：



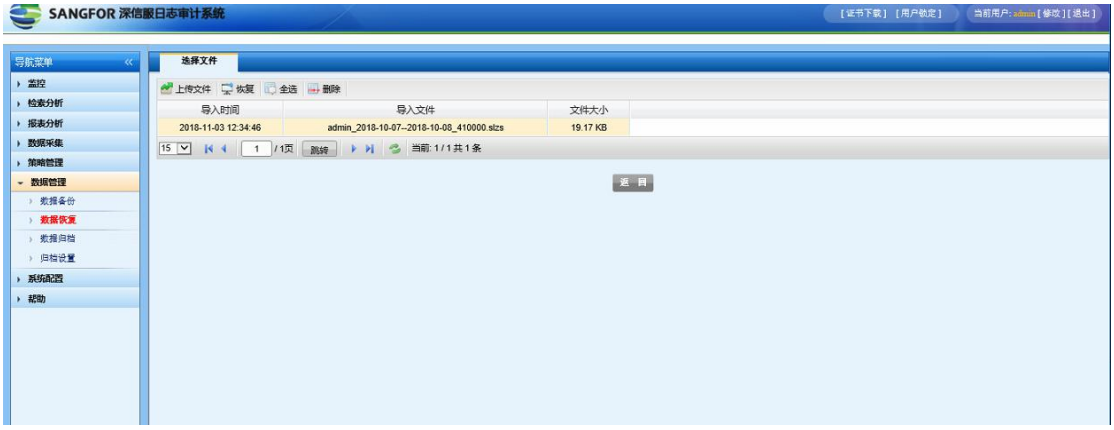
添加备份

3.6.2. 数据恢复

选择导航条上【数据管理】—>【数据恢复】，如图所示：

日志恢复

日志恢复是将日志备份文件重新加载到 SANGFOR-LAS 审计系统中；文件恢复是将【选择文件】的文件重新加载到 SANGFOR-LAS 审计系统中，如图所示：



导入文件

3.6.3. 数据归档

选择导航条上【数据管理】—>【数据归档】，如图所示：

数据归档

【数据归档】可查看、下载和删除归档的数据信息。

3.6.4. 归档设置

选择导航条上【数据管理】—>【归档设置】如图所示：

归档设置

归档策略功能是当磁盘存储空间达到触发条件后，自动处理日志文件。可选择的处理方式为：自动丢弃、本地保存、FTP 上传、SFTP 上传。触发条件在【磁盘配额】中设置。若不设置，默认为当磁盘存储空间达到 90%时触发归档机制。

若不设置归档策略，默认策略为自动丢弃。一旦磁盘存储空间达到 90%之后，将会自动覆盖时间最早的日志。选择本地保存的话，会在日志审计系统将最早采集到的日志进行打包归档，还是会占用存储空间， 启用周期存储的话，会让填写存储的天数以及勾选清除数据，假如填写的天数为 180 天，那表示日志审计系统只保留 180 天的日志，超过的会清除掉

3.7. 系统配置

【系统配置】功能包括【用户管理】、【资产管理】、【安全策略】、【系统管理】。

3.7.1. 用户管理

3.7.1.1. 用户

选择导航条上【系统配置】—>【用户管理】—>【用户】；查看当前系统用户列表，如图所示：

用户管理界面

选中需要查看的用户，在页面下部可查看到该账号的角色、权限等相关信息。

点击【添加】，输入新用户的基本信息、所属角色等；如图所示：

添加用户

添加审计管理员

点击【下一步】，勾选赋予该账号相应功能权限，如图所示：

审计管理员用户功能权限

点击【保存】生成用户。

审计管理员只有监控、检索分析、数据管理功能。实际添加时按功能需求添加。

添加系统管理员用户如图所示：

添加系统管理员用户

点击【下一步】，勾选赋予该账号相应功能权限，如图所示：

系统管理员用户功能权限

系统管理理员用户功能权限包括监控、检索分析、数据采集、策略管理、数据管理、系统

配置。

1、系统管理员可根据用户的岗位职权来分配相应用户帐号的功能权限，保障 SANGFOR-LAS 审计系统的安全及用户网络信息的安全。用户加入用户组后，此用户将自动继承用户组的所有日志权限；

2、密码长度建议位 8 以上的字母、数字、大小写、特殊字符；对功能权限设置应该规范，审计管理员与系统管理员的权限设置必须权限分明，以防止越权行为；

如需对某用户信息和权限进行修改或补充，选择该账号，点击【编辑】，进入编辑页面，最后【保存】修改，也可在页面删除某个用户或停用某个用户，如需重新启用该账号，选中该账号，点击【启用】即可。

针对用户进行日志管理权限的配置，选择未加入用户组的账号，点击【日志权限】，该用户账号下所有日志类型的日志权限默认全部允许，如图所示：

用户日志权限

针对所有日志类型，都可选择【全部允许】、【全部限制】及【部分允许】。

- ✓ 【全部允许】指此用户可以操作此类日志的所有功能（实时、综合、查询）；
- ✓ 【全部限制】指此用户将看不到此类日志的任何信息、更无法审计；
- ✓ 【部分允许】指根据条件来限制此用户可操作某些发生地址 IP 的此类日志；

若在对应日志类型前的下拉列表中选择【部分允许】，点击其后的【修改】，弹出该日志类型的修改对话框，如图所示：

设置【部分允许】权限

在修改对话框中可以选择【允许部分 IP】，此用户将只能操作这部分 IP 内的此类日志内容；或选择【限制部分 IP】，即此用户将只能操作除这部分 IP 外的此类日志内容。如图所示：

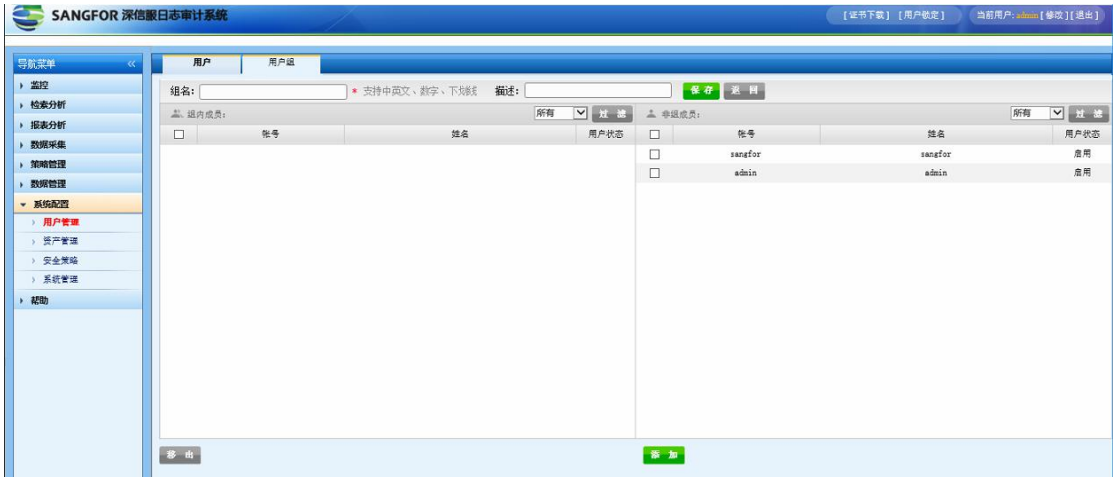
部分允许规则配置

在 IP 规则列表中，可以选择输入单个 IP 或 IP 段，点击【确定】保存，该类型日志的规则生成。

3.7.1.2. 用户组

选择导航条上【系统配置】—>【用户管理】—>【用户组】如图所示：

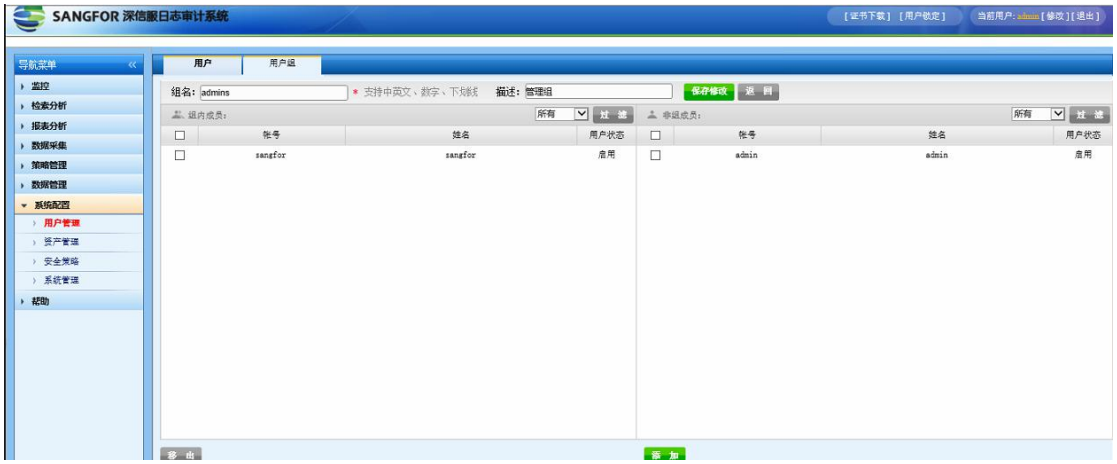
点击【添加】即可添加用户组，如图所示：



添加用户组界面

输入组名和描述，其中带*为必填项，点击【保存】，提示保存成功。

在右边非组成员列表框内勾选尚未加入组的成员账号后，点击【添加】，被勾选账号将移入到组内成员列表框中，成为该组成员。反之勾选组内成员，点击【移出】，则该组内成员被移出到非组成员列表框中。如图所示：



添加组成员

在如图中，选择需要更改的组，点击【编辑】，进入编辑页面，界面如图和 2 所示，最

后【保存修改】即可。

用户组【全选】、【删除】、【日志权限】同小节的**用户**【全选】、【删除】、【日志权限】，详细操作方法请参见上节**用户**操作说明；

已添加入【用户组】的系统用户的日志权限不能独立管理，只能继承所属组的日志权限；系统用户移出用户组后，将恢复默认日志权限。若直接删除用户组，组中的用户仍保持原有的日志权限，直到该用户加入其它用户组，继承新的日志权限；

添加系统用户组只需添加组名及组描述，组名具有唯一性。

3.7.2. 资产管理

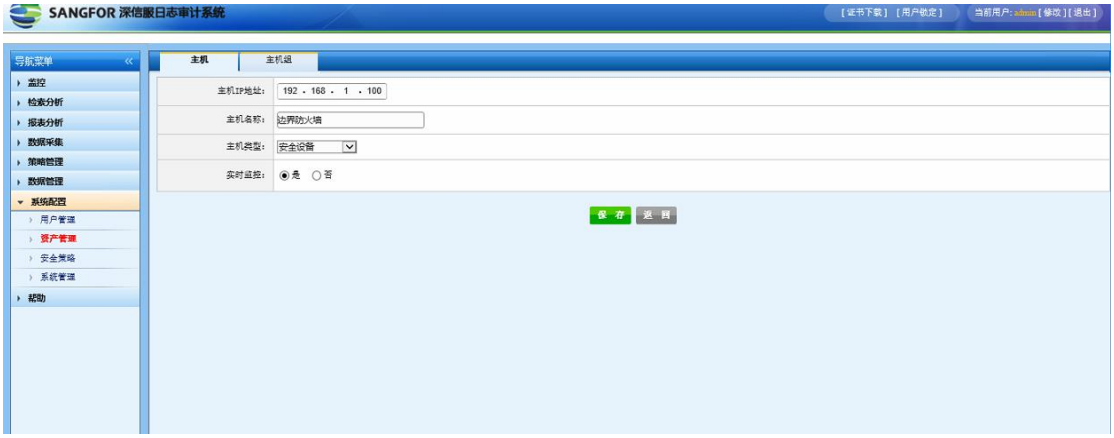
3.7.2.1. 主机

选择导航条上【系统配置】—>【资产管理】—>【主机】，如图所示：

主机列表

可查看并添加、编辑、全选、删除、导入、导出主机列表；主机列表信息包括：IP 地址、主机名、主机类型、实时监控状态。

点击【添加】，输入主机信息，如图所示：



添加主机

- ✓ 主机 IP 地址：输入所要添加的主机 IP 地址；
- ✓ 主机名称：添加的主机的名称，以便辨别；
- ✓ 主机类型：所添加主机的主机类型（下拉列表中有：Windows 服务器、类 Unix 服务器、网络设备、安全设备）；
- ✓ 实时监控：选择是或否，可对该主机进行日志的实时监控，在监控>资产状况可查看被监控主机。

添加完毕后，点击【保存】，在主机列表中生成该主机。

3.7.2.2. 主机组

选择导航条上【系统配置】—>【资产管理】—>【主机组】，如图所示：

主机组列表

【主机组】的配置同小节中【用户组】的配置类似，详情可见该小节。

3.7.3. 安全策略

选择导航条上【系统配置】—>【安全策略】，如图所示：

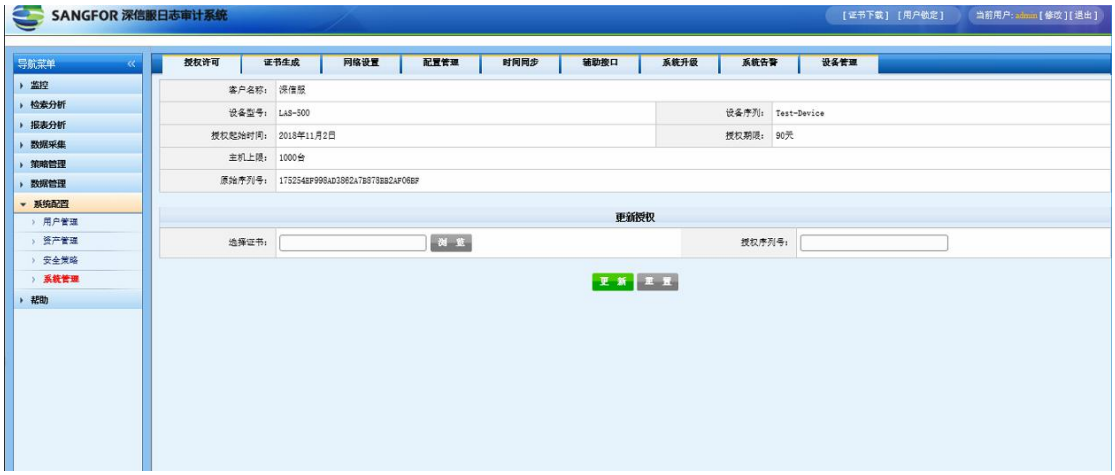
安全策略

- ✓ 密码长度：对页面账号登陆密码进行设置，密码长度在 8-32 之间；
- ✓ 密码复杂度：勾选启用后，可选择小写字母、大写字母、数字、特殊字符以提高密码的复杂度；
- ✓ 自动锁定：勾选启用后，可对账号进行条件锁定和解锁；
- ✓ 系统超时：页面在设定时间内未作任何操作，系统将会超时退出。
- ✓ 访问限制：勾选启用后，可选允许或限制访问，可在文本框内输入启用条件下的 IP 或 IP 段。

3.7.4. 系统管理

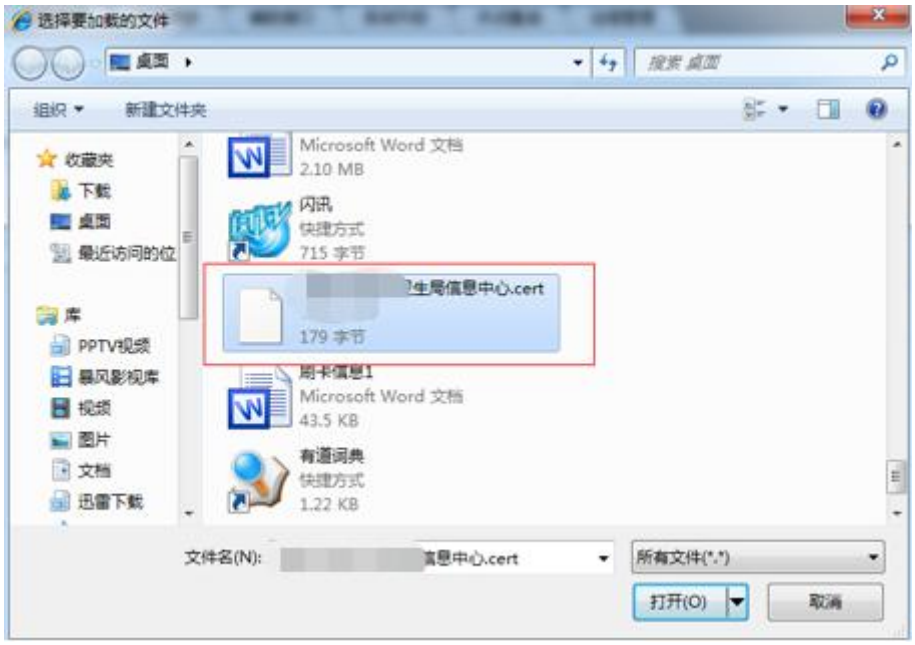
3.7.4.1. 授权许可

选择导航条上【系统配置】—>【系统管理】—>【授权许可】，可看到该设备的授权信息，如图所示：



授权许可

需要更新证书时，点击选择文件后面浏览按钮，选择证书，如图所示：



选择证书

点击更新后会提示导入成功

系统需要延长测试授权或更换正式授权，请在页面提取原始序列号，发给深信服技术。

3.7.4.2. 证书生成

证书生成用于生成设备的根证书，如下所示：

证书生成

如果设备有多个 ip，则可生成对应的根证书，添加多个 IP、域名如图所示：

生成多个证书

点击上中 可以删除生成的证书。这个证书和页面显示的证书错误有关，生成与 IP 相同的证书，并按照下面的操作进行，即可去掉证书错误的提示。

单击页面右上角证书下载，如图所示：

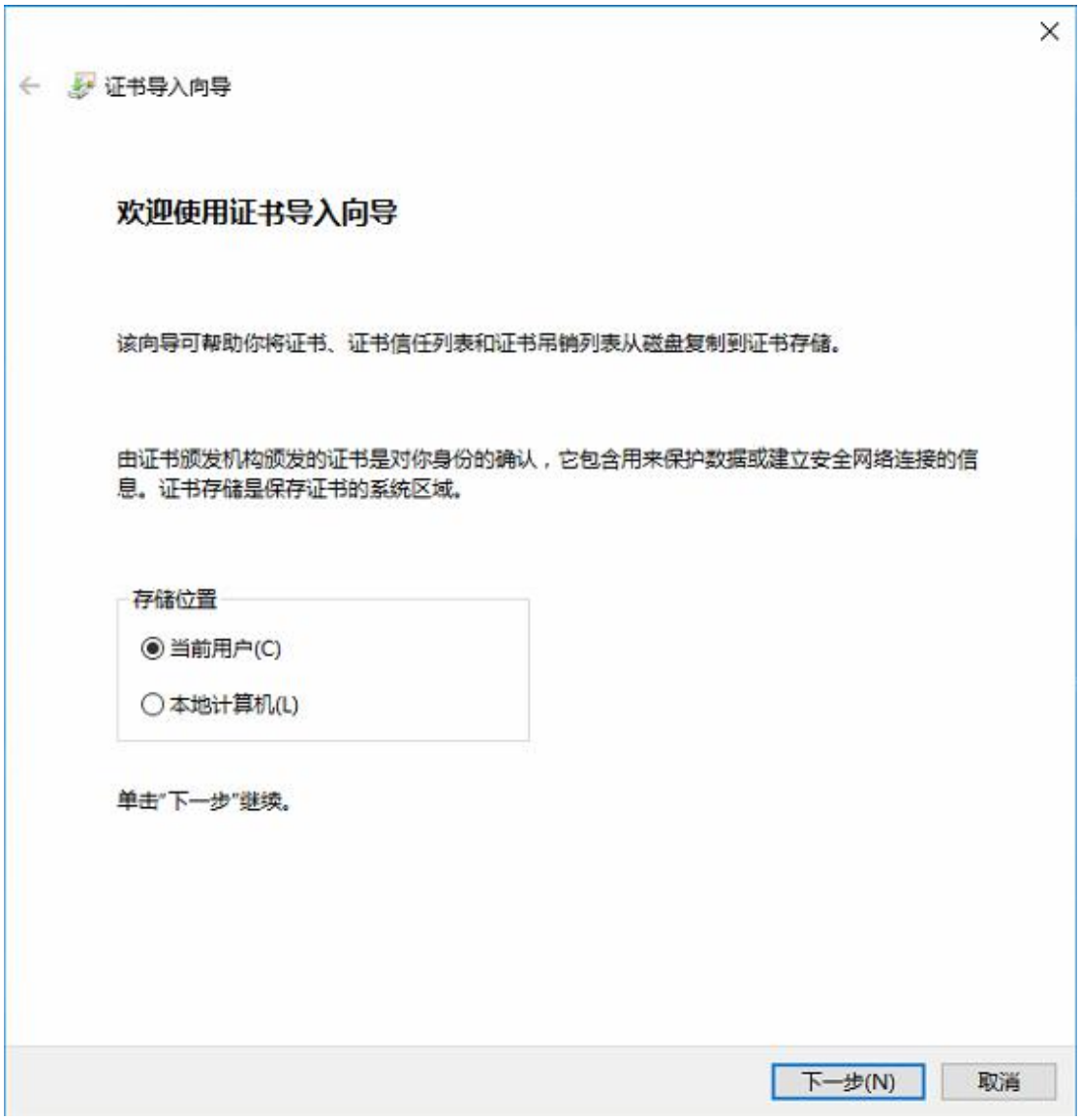
点击下载

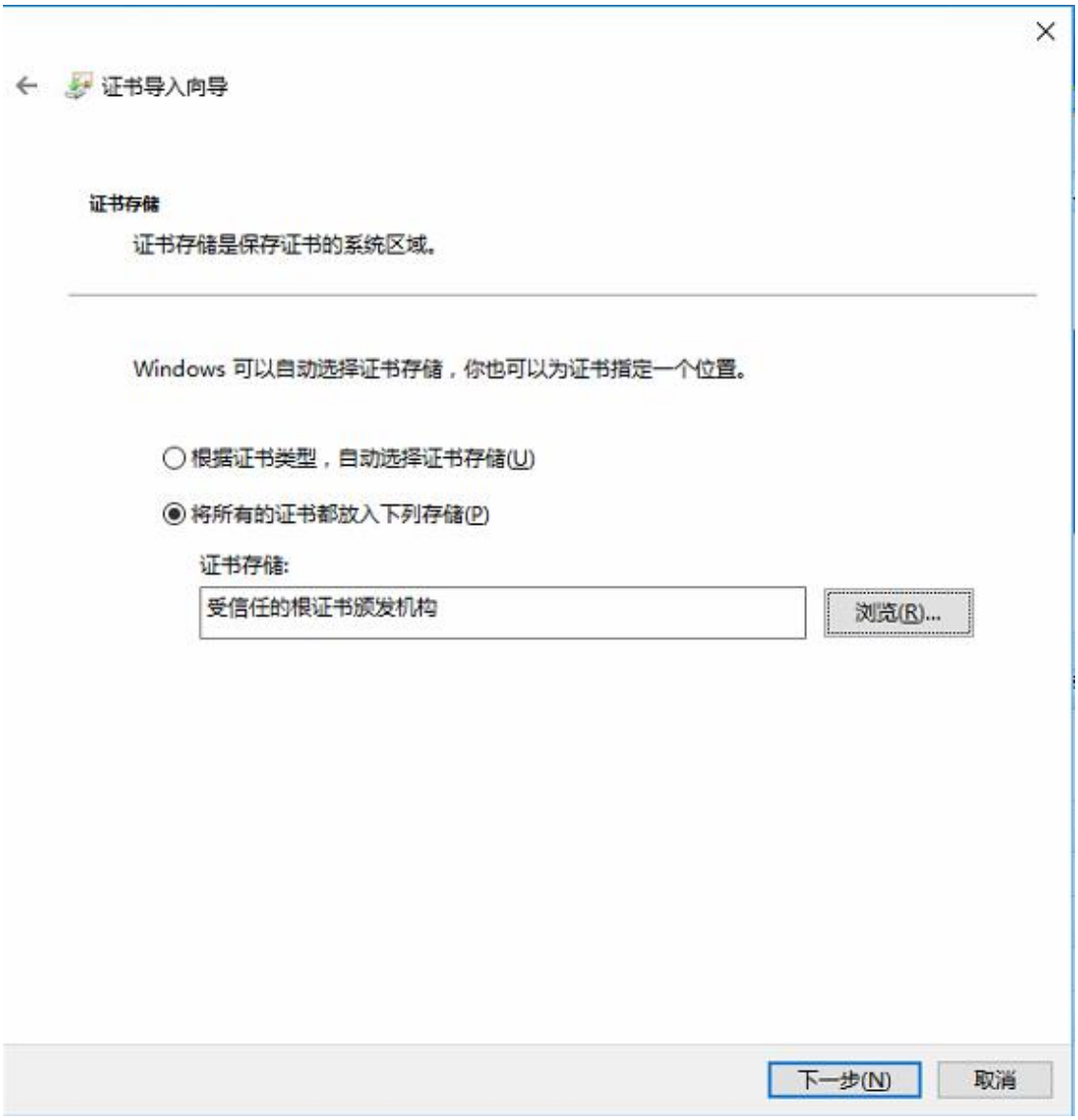
证书下载

点击【保存】，选择文件保存路径。证书下载成功后，可以实施证书的安装工作。双击下载的证书文件，进入证书导入步骤，如图所示：

SANGFOR 证书信息

点击【**下一步**】，进入【**证书存储**】向导，选择【**将所有的证书放入下列存储**】，如图所示：

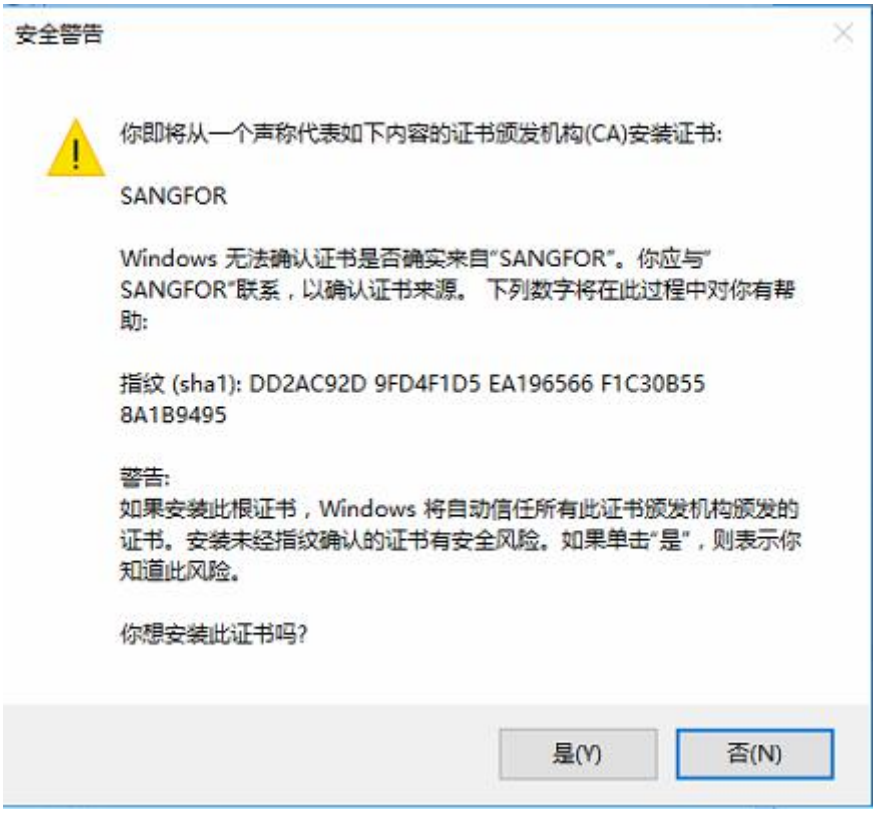




选择证书存储

点击**【浏览】**，将证书选择放入**【受信任的根证书颁发机构】**

点击**【确定】**后，返回**【证书导入向导】**，点击**【下一步】**，至最终完成证书导入，选择是，弹出证书导入成功提示，完成证书安装。如图所示：



证书安装完成

证书安装成功后，需要重启浏览器后生效。

3.7.4.3. 网络设置

选择导航条上【系统配置】—>【系统管理】—>【网络设置】，如图所示：

网络设置

可以在页面上对网口的 IP 地址、掩码以及默认路由进行修改。

3.7.4.4. 配置管理

选择导航条上【系统配置】—>【系统管理】—>【配置管理】—>【配置备份】，如图所示：

配置备份

点击【备份】，即可对当前系统的所有配置进行备份，备份成功后，在备份列表框中可显示配置备份的序号、备份时间、备份大小。选中备份文件，可对备份文件进行下载、删除等操作。

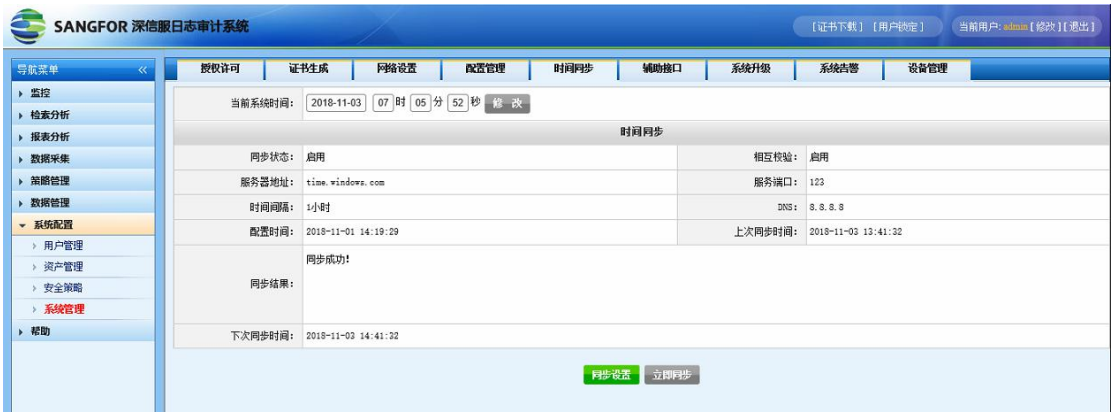
选择导航条上【系统配置】—>【系统管理】—>【配置管理】—>【配置恢复】，如图所示：

配置恢复

配置恢复有两种方式：1.选择本地配置文件上传，点击【恢复】即可；2.选择系统保留的备份文件，点击【恢复】即可。

3.7.4.5. 时间同步

选择导航条上【系统配置】—>【系统管理】—>【时间同步】，可查看系统时间及时间同步配置信息，如图所示：



时间同步

时间同步方式有两种：1.手动修改，**当前系统时间**显示的是当前系统时间，手动更改为正确时间后点击【修改】，系统时间将手动更新；2.自动同步，点击【同步设置】，弹出如图所示：

时间同步配置

勾选**启用**后，可对服务器地址（可配置 URL 或固定 IP）、服务器端口、时间间隔（时间同步的间隔时间）、DNS 进行配置。

3.7.4.6. 辅助接口

3.7.4.6.1.邮件接口

选择导航条上【系统配置】—>【系统管理】—>【辅助接口】；查看并配置系统告警输出接口，支持通过邮件、短信网关、SYSLOG、SNMP　TRAP 等方式输出。如图所示：

邮件告警接口输出设置

邮件输出配置流程：

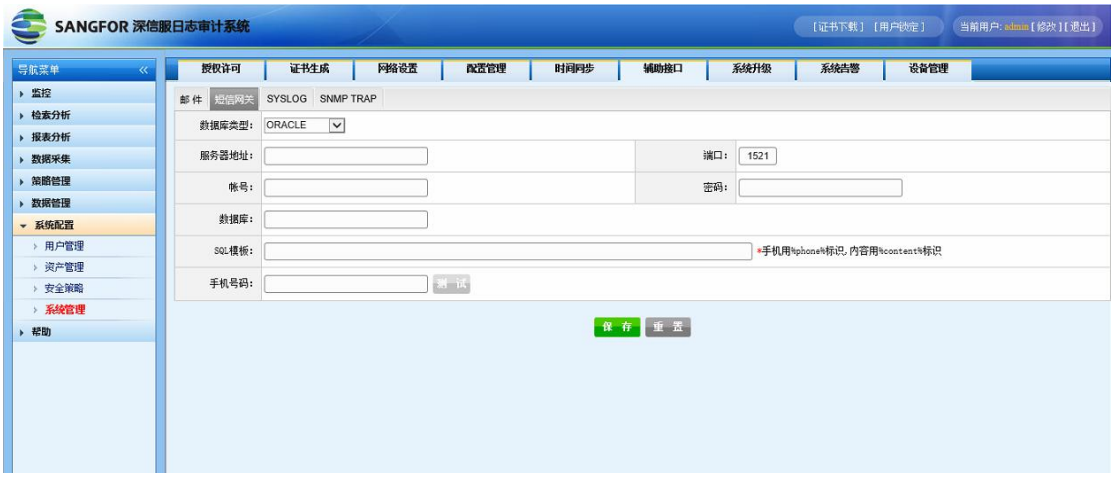
- ✓ 服务器地址（SMTP）：告警信息邮件发送服务器，可为 URL 或固定 IP。（获取相应地址的方式可以 ping 相关邮箱的 smtp 域名）
- ✓ DNS：可用的 DNS 服务器 IP。
- ✓ 发送邮件地址：发送告警信息的邮箱地址。
- ✓ 用户名：发送告警信息的邮箱相对应用户。

- ✓ 发送邮箱密码：发送告警信息的邮箱相对应的邮箱密码。
- ✓ 邮件接收地址：输入测试的邮箱地址后。
- ✓ 点击【**保存**】完成配置。
- ✓ 点击【**测试**】，可验证邮件设置是否正确，如正确，则显示测试成功打开测试 Email，查看是否接收到发送方 Email 地址发送的告警邮件。

发送方 Email 地址为发送告警信息的邮箱地址，接收该告警信息的邮件地址配置异常事件请在策略管理>实时规则>动作>方式中对“邮件”，勾选接收告警用户即可；

3.7.4.6.2.短信网关

选择【短信网关】，选择数据库类型、填写服务器等，如图所示：



告警接口-短信网关

- ✓ 数据库类型：可在下拉列表中选择数据库类型
- ✓ 服务器：填写服务器的 ip
- ✓ 端口：填写服务器的端口号
- ✓ 帐号：数据库接口的账号
- ✓ 密码：数据库接口的密码
- ✓ 数据库：填写数据库名
- ✓ SQL 模板：INSERT INTO lqq(message,mobilephone)

VALUES('%content%','%phone%') （以 MYSQL 为例）其中 mobilephone 为号码字

段%phone%，message 为信息内容字段%content%。

- ✓ 手机号码：填写要发送短信的手机号码
- ✓ 点击【**保存**】完成配置。
- ✓ 点击【**测试**】可验证短信网关设置是否正确。

主要需要知道手机号码字段名、信息内容字段名，以及在插入语句执行时必填字段，这些在数据库表结构中都有注明。

3.7.4.6.3.SYSLOG

选择【SYSLOG】，如图所示：

告警接口-SYSLOG

填入服务器地址、端口，点击【**保存**】完成配置

3.7.4.6.4.SNMP TRAP

选择【SNMP TRAP】，如图所示：

告警接口-SNMP TRAP

填入服务器地址、点击【**保存**】完成配置

3.7.4.7. 系统升级

选择导航条上【系统配置】—>【系统管理】—>【系统升级】，导入系统更新程序，对系统进行升级，如图所示：

系统升级

- ✓ 选择文件：点击【浏览】选择系统升级文件，导入系统中；
- ✓ 文件序列号：输入升级文件的正规标识序号；
- ✓ 升级文件导入：开始导入升级文件；
- ✓ 重置：重新选择文件及输入文件序列号；

3.7.4.8. 系统告警

选择导航条上【系统配置】—>【系统管理】—>【系统告警】；从页面上选择是否启用

告警，如图所示：

系统告警配置

系统告警是指通过上面所介绍的几个方式来收取有关的报警，如一段时间内日志主机没有新的日志采集，就会通过上述方式来提醒管理员来查看问题。

3.7.4.9. 设备管理

选择导航条上【系统配置】—>【系统管理】—>【设备管理】，如下所示：

对设备进行关闭和重启操作。

设备管理