思福迪

LogBase 日志管理综合审计系统

快速使用手册

杭州思福迪信息技术有限公司

1.登陆系统

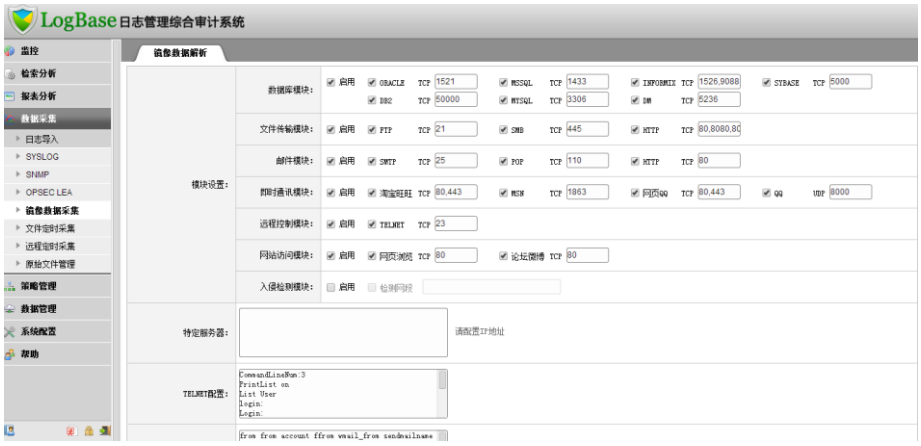
打开 IE 浏览器,输入 LogBase 地址,(如 https://192.168.1.6),以 LogBase 管理员角色登录，默认用户名：admin；密码：safetybase;

如下图所示，点击【登录】:

2.数据采集

2.1.镜像数据采集

选择导航条上【数据采集】—>【镜像口数据采集】，如下图所示：



数据口的镜像采集

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

【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。

2.2.Syslog 日志

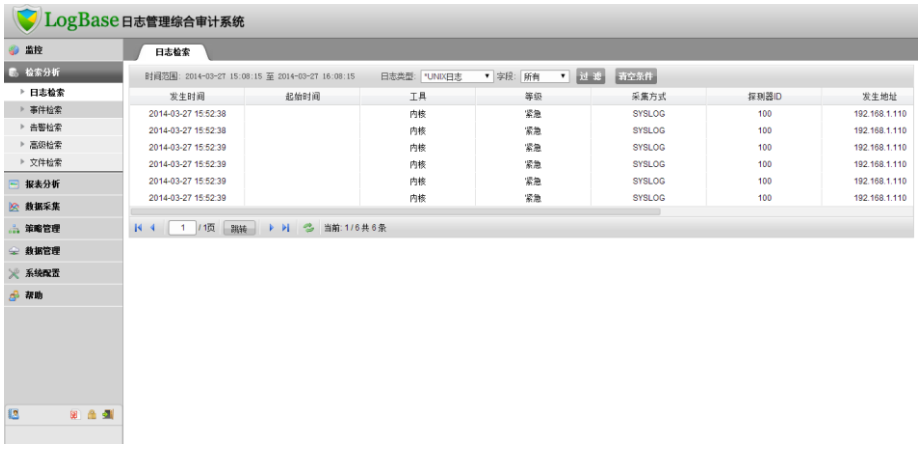
如果需要采集 syslog 服务器日志，则需要在服务器端配置 syslog host，把地址指向思福迪 LogBase 日志审计综合管理系统，在指向完成以后，就可以收取 syslog 服务器日志了。

2.3.Windows 日志

如果需要采集 Windows 日志，则需要在 Windows 服务器端安装思福迪 LogBase 日志审计综合管理系统的 WindowsAgent 来采集 Windows 日志，具体的安装手册，请参考 WindowsAgent 安装手册。

3.数据查询

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，如下图所示：



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，如下图所示：

日志信息

日志检索示例：查询 2014-1-1 至 2014-3-26 日志类型为*UNIX 日志，发生在 192.168.1.110 上的日志。

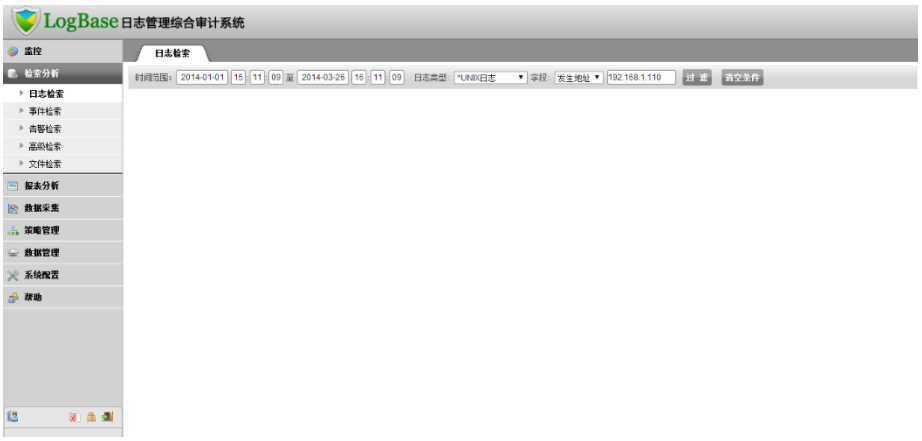
1、先点击“清空条件”

2、选择时间范围：2014-1-1 至 2014-3-26。

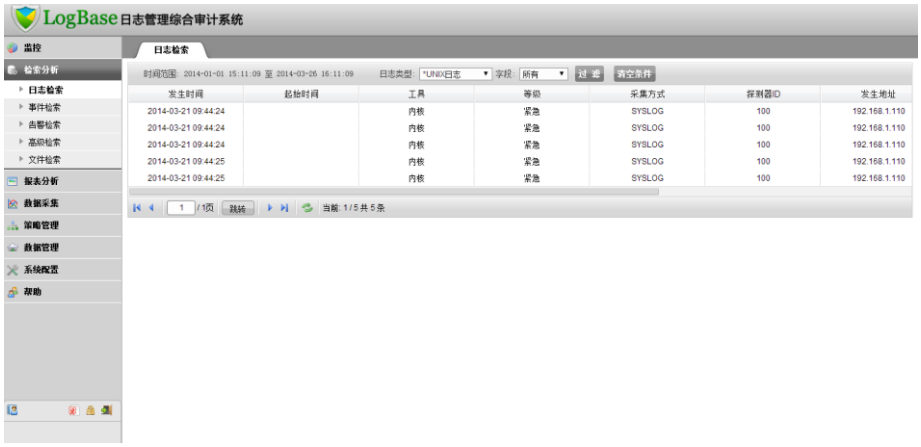
3、日志类型栏选择*UNIX 日志；

4、字段栏中选择发生地址：192.168.1.110，点击过滤；

5、即可在过滤列表中点击查看日志的详细内容。如下面三张图所示。



日志查询条件



日志查询结果

日志详细信息

4.报表制作

4.1.报表管理

选择导航条上【报表分析】—>【报表管理】—>【模板配置】，如下图所示：

4.2 **报表配置**：针对不同需求定制报表模版；

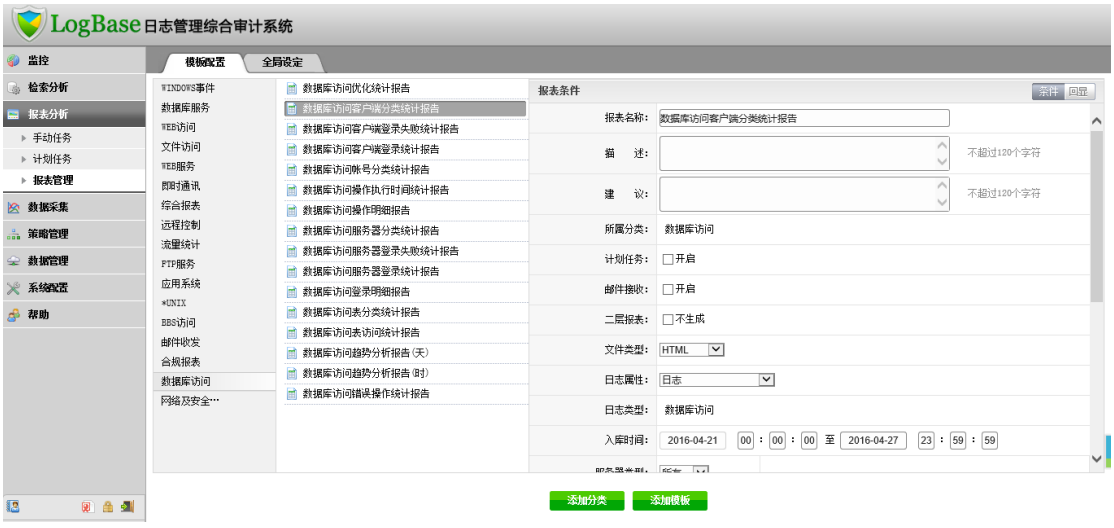
模板配置

4.2.生成报表

示例：生成数据库服务器登录统计报告

1、选择导航条上【报表分析】—【报表管理】—【模板配置】；选择“数据库访问”再选择“数据库访问客户端分类统计报告”

2、报表条件中选择需要的条件，最后执行报表。如下图所示：

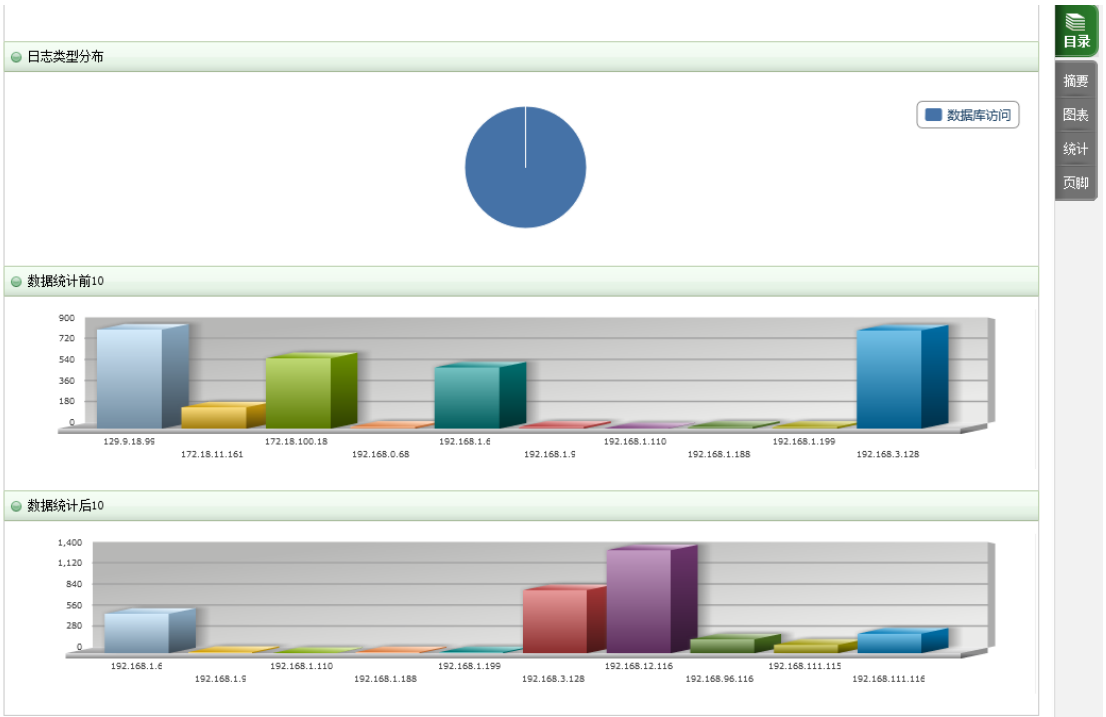


定义报表条件

点击执行报表以后，在【报表分析】—【手动任务】中，能看到刚刚执行的报表，如下图所示。

手动执行报表列表

在第一行，就是刚刚执行成功的报表，点击查看，就可以看到报表所展示的内容，如下图所示。



报表内容