獬豸日志安全审计系统

用户手册-V1.0

北京携推信息技术有限公司

2019 年 12 月

声明

本技术白皮书是对北京携推信息技术有限公司的獬豸日志安全审计系统的描述。与内容相关的权利归北京携推信息技术有限公司所有。手册中的任何内容未经本公司许可，不得转印、复制。本资料将定期更新，如欲索取最新资料，请访问本公司网站：www.xie-tui.com

目　　录

1.系统界面登录

在 IE 浏览器中输入系统访问 IP 地址（默认：172.19.11.26），访问系统的登录界面，如图所示：

图 1-1

注：新用户首次登录日志审计系统，会先展示给用户授权界面，授权成功后，系统方可展示给用户系统登录界面，具体授权相关操作，请用户查看**“9.5 - 授权管理”**中对授权操作的的详细讲解。

默认的系统帐户（用户名）不可以删除，只可以进行默认密码的修改。如下：

登录用户名	默认密码输入	中文名称	用途
useradmin	useradmin@1234	用户管理	可以添加，编辑，删除用户信息，指定用户资产负责人，并进行角

			色设置功能
sysadmin	sysadmin@1234	系统管理	进行日志监控,报警,查询,关联分析,资产管理,报表及系统管理操作
auditadmin	auditadmin@1234	自身审计	对本系统各功能的操作进行记录

默认的系统帐户首次登录，系统要求修改默认密码。如图所示：

图 1-2

重新设置密码后，点击**“修改密码”**按钮，可以成功登录日志审计系统。

注：帐户或密码输入错误或新密码输入不一致，会回退到登录界面。

2.用户管理

2.1. 创建用户

使用 useradmin 用户登录系统，useradmin 拥有创建、编辑和禁用和启用系统用户的权限。如图所示：

图 2-1

- 点击添加新用户按钮或链接，弹出添加用户对话框，如图 2-2 所示：

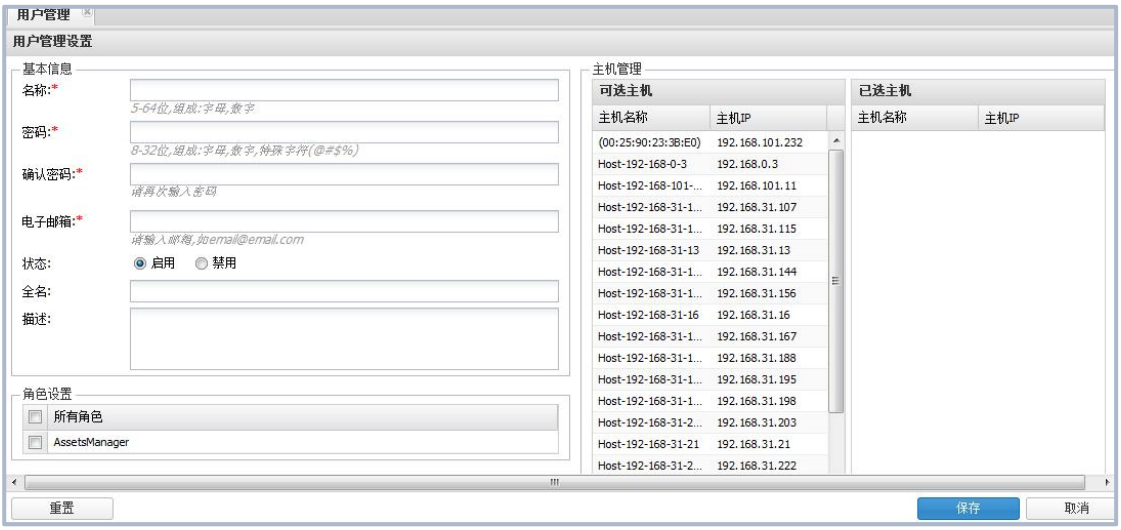


图 2-2

(1) 名称：用户登录账号，此项不得为空；

- 注：登录账号 5-64 位组成：字母、数字。

(2) 密码：用户登录密码；确认输入的密码必须一致；

- 注：必须 8-32 位组成：字母、数字、特殊字符（@#￥%）

(3) 电子邮箱：系统用户的电子邮箱地址；

- 注：邮箱格式必须,如 email@email.com

(4) 状态：初次创建默认为“启用”；如果想要停用当前帐户，选择“禁用”后，点击“保存”按钮。

(5) 用户对应角色 ： 给予系统用户访问系统各界面的权限，此项需要以 Sysadmin 登录，进入系统管理->角色管理后创建角色赋予权限才可以在创建用户时显示出来。

- 注：用户帐号及该帐号的权限在建立后是不能更改的

(6) 全名：可以对相应帐户名称进行描述，并将帐户以中文名显示。

- 注：此全名最长度限制 64 位字符，只能做为界面显示的名称，不能为登录名称。

(7) 描述：可以对相应帐户进行详细描述；

(8) 主机管理：此项包括可选主机和已选主机两个功能栏，用户可选中可选主机栏中的资产 IP,通过拖拽可添加到已选主机栏中，为该用户分配资产，所属该资产的响应行发送会直接发送到该负责人邮箱

(9) 点击“保存”按钮，新添加的用户保存成功，并在界面显示。

2.2. 编辑用户

选择“用户管理”列表中的用户名，点击右边**“编辑”**按钮，进入“用户管理”编辑界面。如图所示：

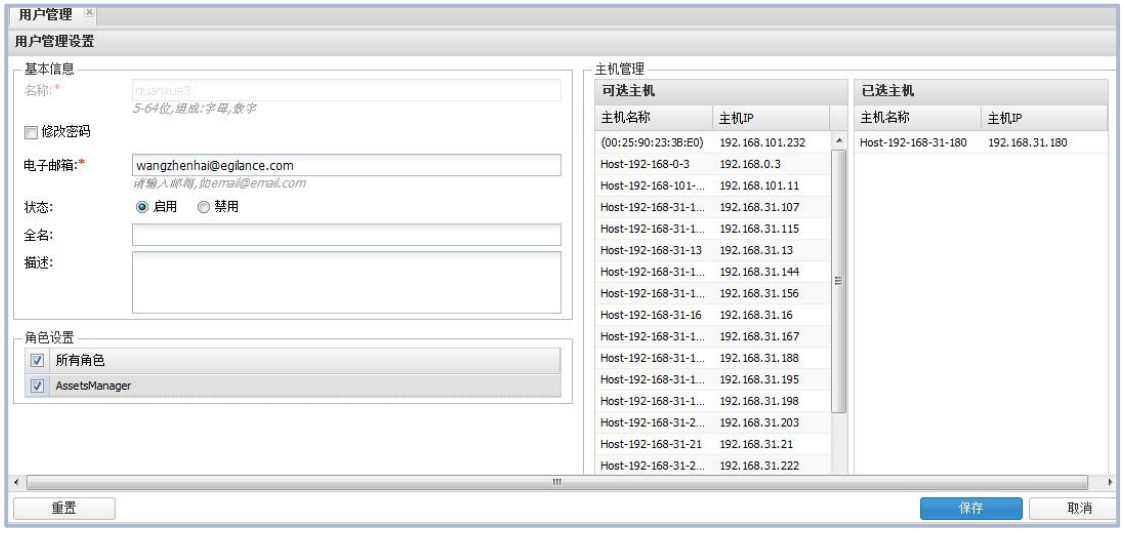


图 2-3

此界面可修改该用户的密码，名称，邮箱，状态，全名，对应角色，描述信息。**(注：用户名称不可更改)**

2.3. 用户的禁用与启用：

新添加的用户帐户是启用状态是，点击**“立刻禁用”**，弹出提示框，如图所示：

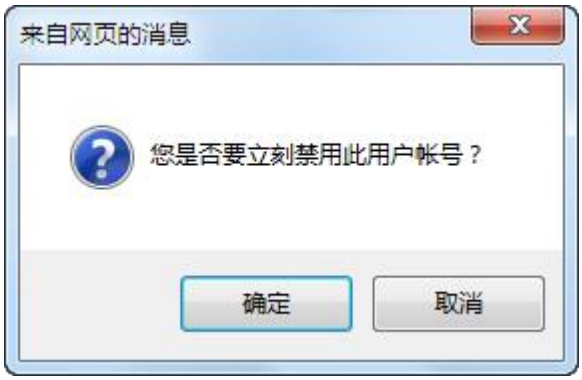


图 2-4

点击**“确定”**按钮，选择的帐户状态修改为禁用，不可在登录系统。

帐户状态已修改为禁用状态时，点击操作列“重新启用”，系统弹出提示框，如图所示：

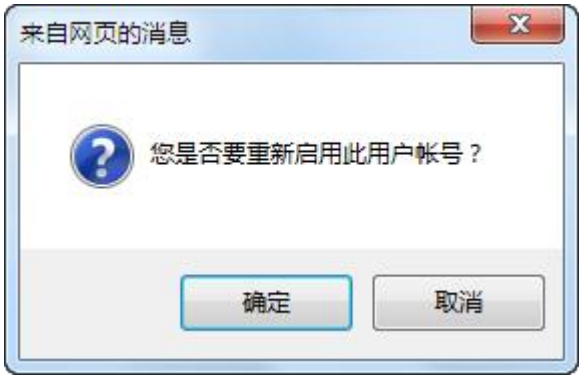


图 2-5

点击**“确定”**按钮，选择的帐户状态修改为启用，该帐户可继续登录系统。

2.4. 配置列

鼠标放在配置展示列尾部出现小图标，点击小图标会弹出如下配置列展示。用户可根据自身需要勾选或取消各个列名，最终在主界面展示出已勾选的各列名。

添加的用户可以点击正序或倒序展示主界面。如图所示：

图 2-6

3.首页

成功登录日志审计系统后，系统默认为用户展示首页，此页只为用户展示最近 24 小时的数据，包括：事件总数，资产分布，报警总数，事件类型，磁盘占用，内存占用，CPU 使用率。如图所示：

图 3-1

界面最顶端为用户统计最近 24 小时的事件总数，报警总数（高、中、低不同颜色分布记录）

事件总数趋势（第一幅图）：此图为用户展示最近 24 中每个时间段内发生的事件总数，图形横坐标展示 24 小时，纵坐标展示事件总数（随着事件的不断增多，纵坐标最大值不断变化）。光标搁置在坐标点处，会弹出 Tip 信息框，为用户展示该点的时间数据。如图所示：

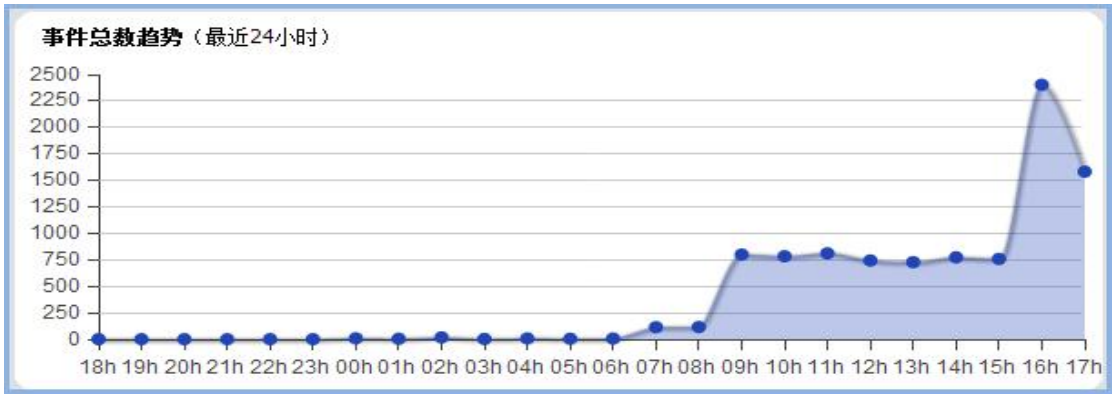


图 3-2

资产分布趋势（第二幅图）:此图为用户展示最近 24 小时每个资产 IP 数据总数（Top10），以柱状显示，所有展示的资产 IP 都需要在主机界面中保函（可添加），展示类型包括：日志报警总数（默认展示），日志事件总数。图形横坐标展示资产 IP，纵坐标展示事件总数（随着事件的不断增多，纵坐标最大值不断变化）。光标搁置柱状图形处，会弹出 Tip 信息框，为用户展示该柱状图所属的资产 IP 的时间数据。如图所示：

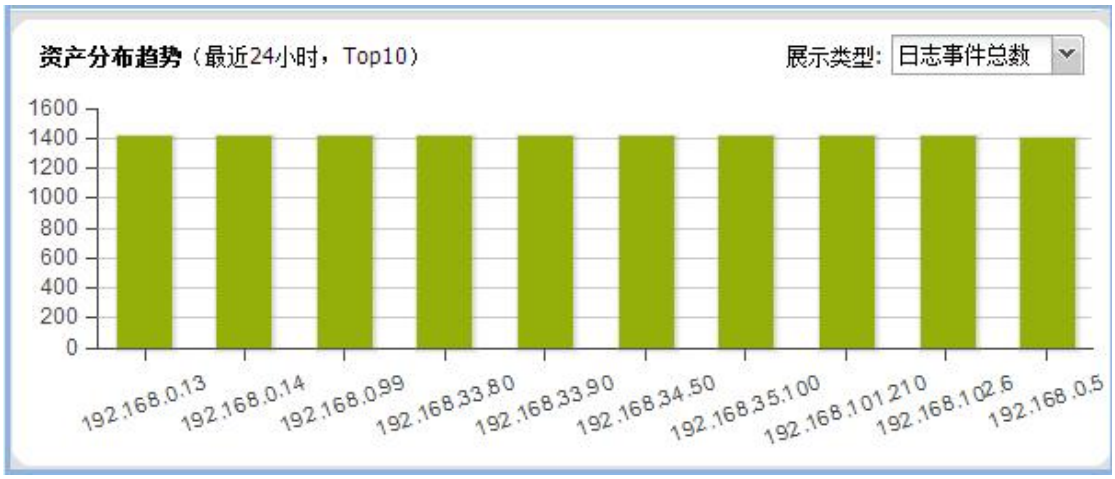


图 3-3

报警总数趋势（第三幅图）：此图为用户展示最近 24 中每个时间段内发生的事件报警总数，图形横坐标展示 24 小时，纵坐标展示事件报警总数（随着事件的不断增多，纵坐标最大值不断变化）。光标搁置在坐标点处，会弹出 Tip 信息框，为用户展示该点的时间数据。如图所示：

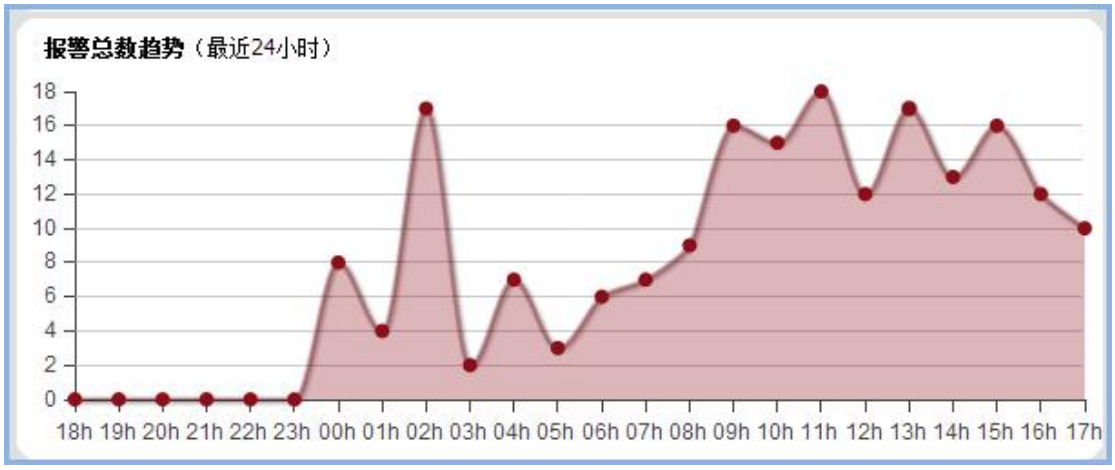


图 3-4

事件类型分布（第四幅图）：此图为用户展示最近 24 小时中所有数据保函的不同事件类型的总数（Top10），并以不同的颜色区分，颜色为不固定展示，随机分配事件类型颜色，图形右侧标注属于该颜色的事件类型。鼠标点击事件类型名称，该事件类型名称被置灰，在圆形中属于该事件类型的颜色消失，再次点击该事件类型名称，圆形中属于该事件类型的颜色恢复。光标搁置在圆形图的某个颜色处，会有动态效果并弹出 Tip 信息，为用户展示属于该颜色的事件类型的事件名称，事件个数和百分比。

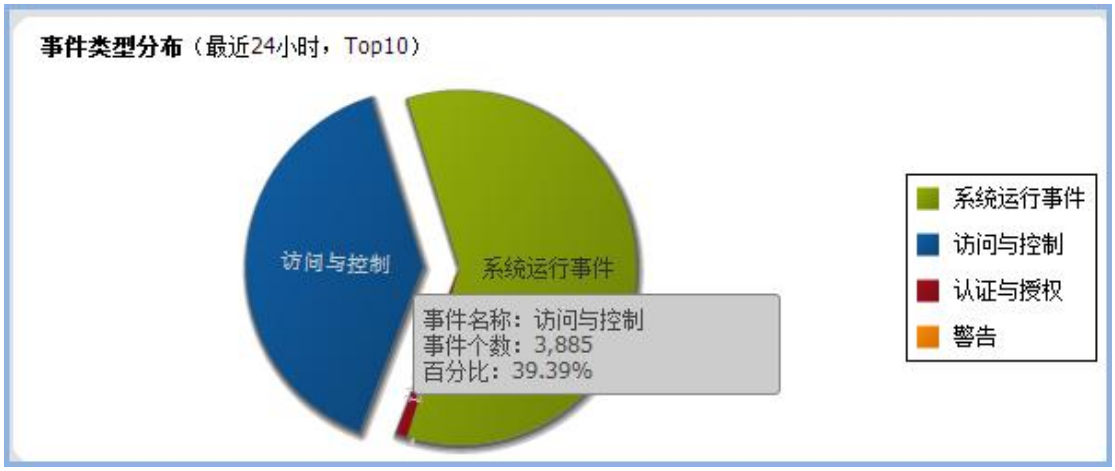


图 3-5

4. 事件监控

事件监控界面用来实时展示审计日志及事件信息。

4.1. 事件监控主页面

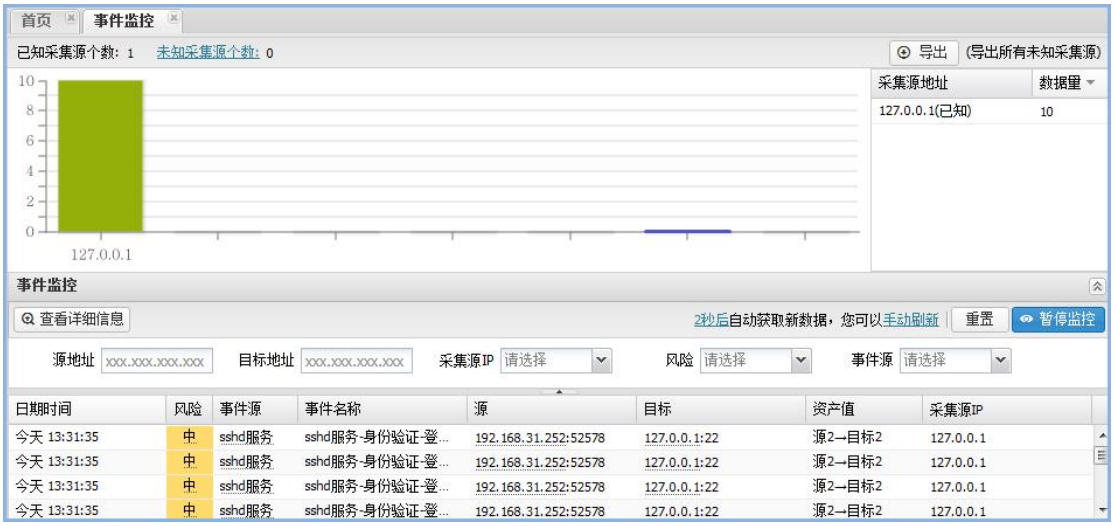


图 4-1

4.2. 事件监控界面功能

事件监控可以看到采集源的数据量分布图（Top7）和各个采集源的数据总数以及支持导出未知采集源。

已知采集源个数：显示当天已知采集源的个数。

未知采集源个数：显示当天未知采集源的个数。点击可以配置未知采集源的采集信息。

导出：点击该按钮，可以把所有的未知采集源导出到自定义位置

(unknownSource-xxxx.xls)。

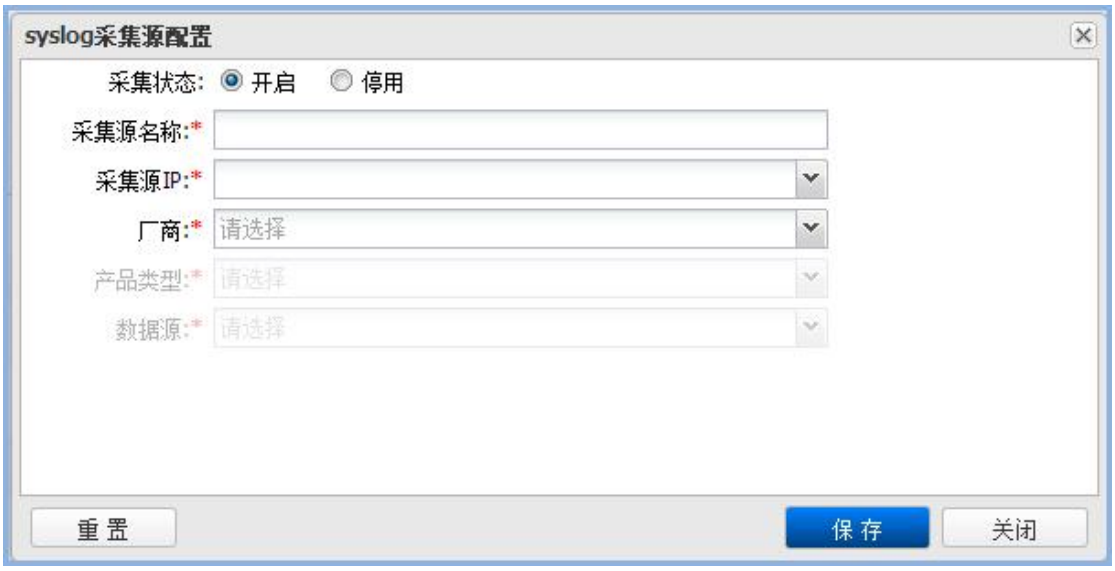


图 4-2

4.2.1 查看详细信息

选择某一条事件，点击查看详细信息 查看详细信息，会展示该事件的详细内容，包括：

- **基本信息**（事件名称，日期时间，源地址，目标地址，网络协议，事件类型，事件子类型，事件 ID），
- **资产信息**（资产值，优先级，可信度，风险），
- **采集信息**（产品类型，采集器，数据源，网卡/接口），
- **其他信息**（用户名，文件名），
- **原始内容**
- **扩展数据**（扩展字段 1—扩展字段 9）。

（**注**：该功能等同于鼠标双击单条事件）

图 4-3

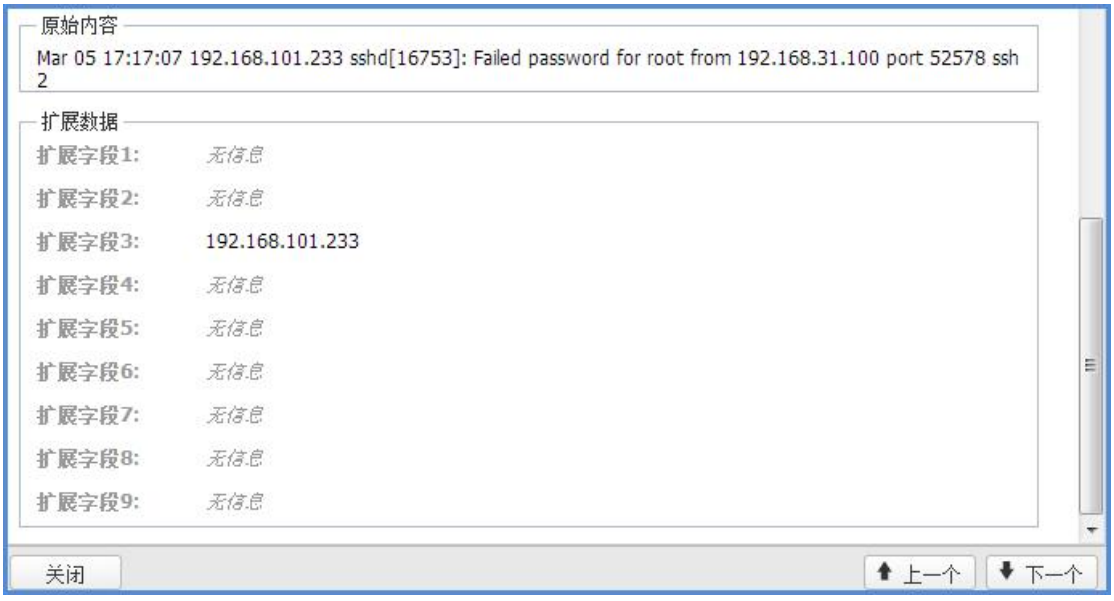


图 4-4

4.2.2 事件详细信息页面功能按钮

图 4-5

- **关闭**：关闭事件详细信息页面。
- **上一个**：显示上一个事件的详细信息。
- **下一个**：显示下一个事件的详细信息。

4.3. 监控条件筛选

图 4-6

4.3.1. 监控条件

用户可以根据源地址，目标地址，风险，数据源对监控页面展示进行过滤。

1. **源地址**：数据产生的源 IP 地址。(可以手动按格式输入，也可以点击页面对应的源 IP 做为条件)

2. **目标地址**：监控目标地址的 IP 地址。(可以手动按格式输入，也可以点击页面对应的目标 IP 做为条件)

3. **风险**：事件类型的风险级别。(可以手动按格式输入，也可以点击页面对应的风险值做为条件)

4. **数据源**：数据来源。(可在数据源下拉菜单选择数据源条件)

用户可以根据自己的需要选择一个或多个条件来对监控信息进行筛选。

4.4. 监控按钮

- **暂停按钮**： 

可以暂停监控页面的自动刷新。
- **启动按钮**： 

对已经停止自动刷新的监控页面恢复监控的功能。
- **重置按钮**： 

清空源地址，目标地址，风险，数据源的内容。
- **刷新时间**（图 3-6，图 3-7）：

图 4-7　　图 4-8

1. 用户可以等待刷新时间自动刷新，也可以点击手动刷新即刷新监控页面。(图 3-6)
2. 用户可以点击时间来更改自动刷新时长。(系统默认 10 秒)

5.报警审计

报警审计界面用来展示各种 syslog 事件所关联出来的报警信息，和其他硬件报警等信息(普通用户登录日志审计系统，该用户只能查看用户管理员指定给该用户的所有资产的报警信息。该用户不负责的资产报警信息查询不到)如图所示：

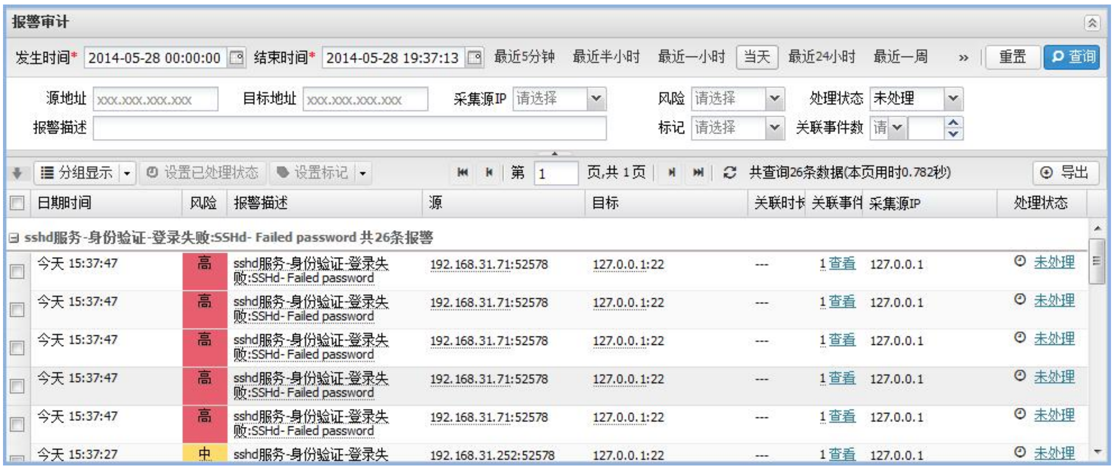


图 5-1

5.1. 查询报警信息

查询条件设置，如图所示：

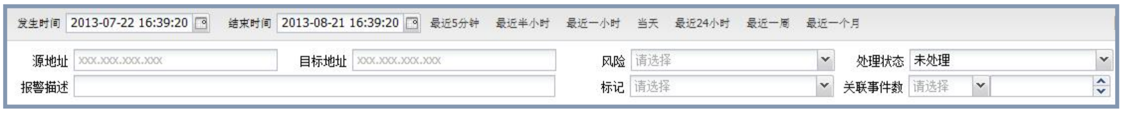


图 5-2

- **时间条件**：支持手动调整或输入，同时也支持快速输入时间条件，例如，点击“最近 5 分钟”后，当前时间即显示为“开始时间”：当前时间前 5 分钟，“结束时间”：当前时间。
- **源地址**：报警信息的源 IP，支持点击报警信息中“源”的内容，快速输入源地址。
- **目标地址**：报警信息的目的 IP，支持点击报警信息中“目标”的内容，快速输入源地址。
- **风险**：分为“高、中、低、无”4 个级别。

- **处理状态**：分为“所有、未处理、已处理”3 种状态。
- **报警描述**：可手动输入报警描述的内容，同时也支持点击报警信息中“报警描述”的内容，快速输入报警描述的内容。
- **标记**：分为紧急、非常重要、还在分析、没有发现异常。
- **关联事件数**：支持按关联事件数查询。

5.1.1. 查询报警信息

根据实际情况设置查询条件后，点击“查询”按钮。界面即展示所有符合要求的报警，如图所示：

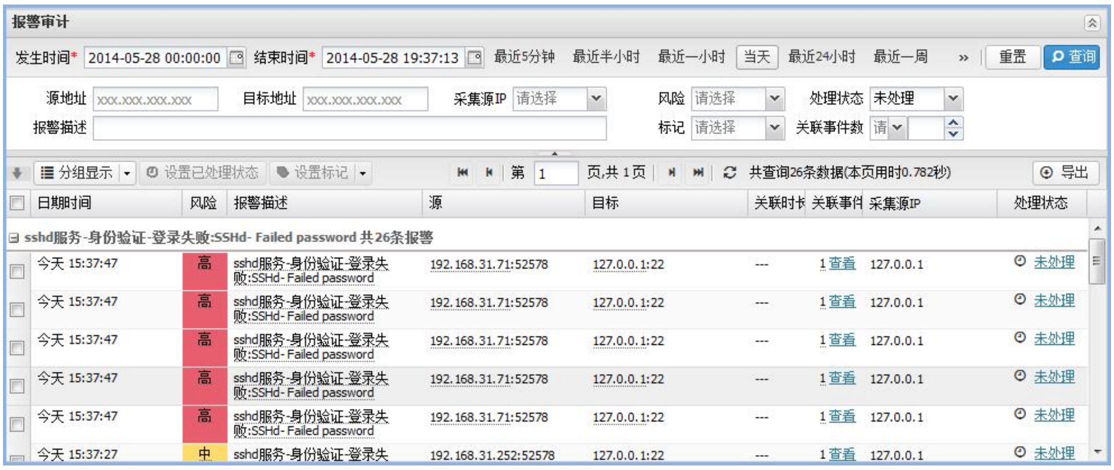


图 5-3

点击“按日期分组显示”按钮，可以对当前界面中的数据以日期进行分组展示，如图所示：

图 5-4

5.1.2. 查询报警关联事件

查询报警关联事件有两种方式：

1. 左键双击报警信息。
2. 点击报警信息中“关联事件个数”列中的“查看”。

报警关联事件界面，如图所示：

图 5-5

查看报警关联事件的详细信息有两种方式：

1. 左键双击报警关联事件。
2. 选中报警关联事件后，点击“查看详细信息”按钮。

报警关联事件的详细信息，如图所示：

图 5-6

5.1.3 报警导出

报警导出条件：查询结果展示后导出或设定条件后直接导出，导出内容：原日志内容，导出格式：Ecxle 文档的 cvs 格式。点击“导出”按钮，系统会弹出**“打开，保存”**提示窗口，如图所示：

图 5-7

点击“**保存**”按钮，系统会接着弹出“**另存为**”提示窗口。如图所示:

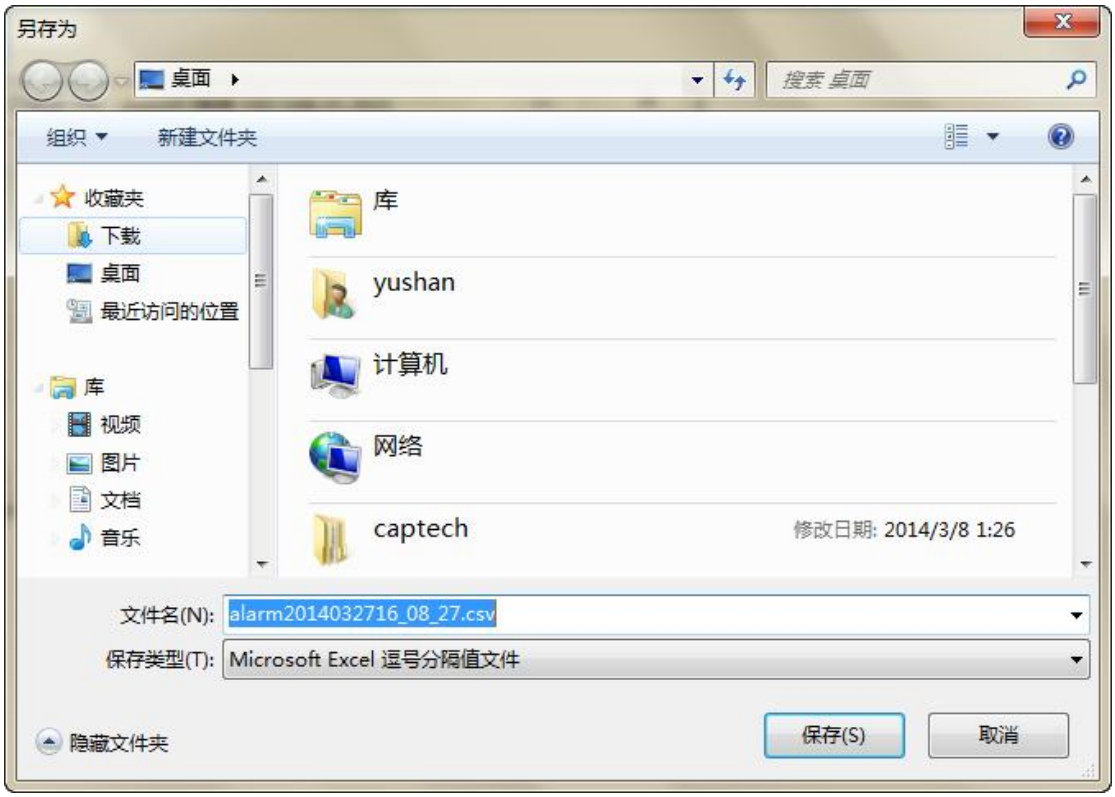


图 5-8

您可以输入命名保存文件，点击“**保存**”按钮即可成功导出日志信息的详细

内容，通过 EXCLE 文档格式查看，导出的日志日期时间倒序显示。

导出功能最多可支持 1000 条信息的导出，如果你导出的日志信息条数大于 1000 条，点击“导出”按钮后，系统会弹出提示窗口。如图所示：

图 5-9

点击**“确定”**按钮。系统会默认的导出最新的 1000 条数据信息供用户查看，点击**“取消”**按钮。则放弃此次的日志导出。

5.1.4 报警信息分组显示

日志报警界面点击**“分组显示”**按钮，会弹出下拉框，分组条件包括：日期、报警描述、源 IP、目的 IP、采集源 IP。其中默认展示“报警描述”。如图所示：

图 5-10

5.2. 处理报警信息

处理报警信息包括”设置标记”和”设置处理状态”两种。

5.2.1. 设置和取消标记

5.2.1.1. 设置标记

勾选想要进行标记的报警信息，点击“设置标记”下拉列表，如图所示：

图 5-11

选择所要标记的级别即可，且同一报警信息可以设置多个标记，如图所示：

图 5-12

5.2.1.2. 取消标记

取消标记有两种方式：

1. 点击标记上的关闭即可，如图所示：

图 5-13

2. 打开“设置标记”下拉列表，重复点击对应的标记，即可取消对应的标记图标。

5.2.2. 设置处理状态

设置处理状态是将处理过的报警信息的“处理状态”由默认的“未处理”设置为“已处理”，设置后不可回退到“未处理”状态。

设置处理状态有两种方式：

1. 选中报警信息后，点击“设置已处理状态”按钮并确认即可。

2. 直接点击报警信息中“处理状态”列中的“未处理”并确认即可。

设置完成后，报警信息的“处理状态”列显示为“已处理”，如图所示：

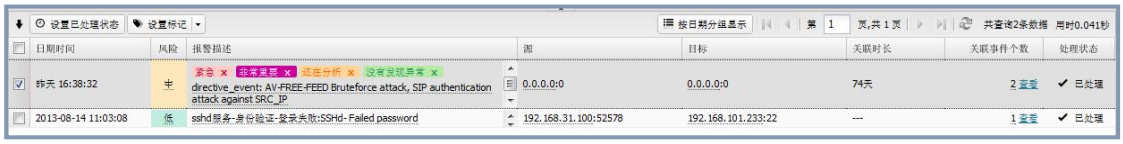


图 5-14

6. 事件查询

事件查询界面主要是将通过多种查询条件的单一查询和组合查询后的结果显示在查询界面，并以列表形式展示出日期时间，风险，事件名称，源（IP、端

口)，目标（IP,端口)，资产值，事件 ID，事件类型，事件子类型，数据源，产品类型，用户名，文件名，采集器，网卡/接口，协议，优先级可信度，原始内容，及扩展字段等配置列(普通用户登录日志审计系统,该用户只能查看用户管理员指定给该用户的所有资产的日志信息。该用户不负责的资产日志信息查询不到)。如图所示：

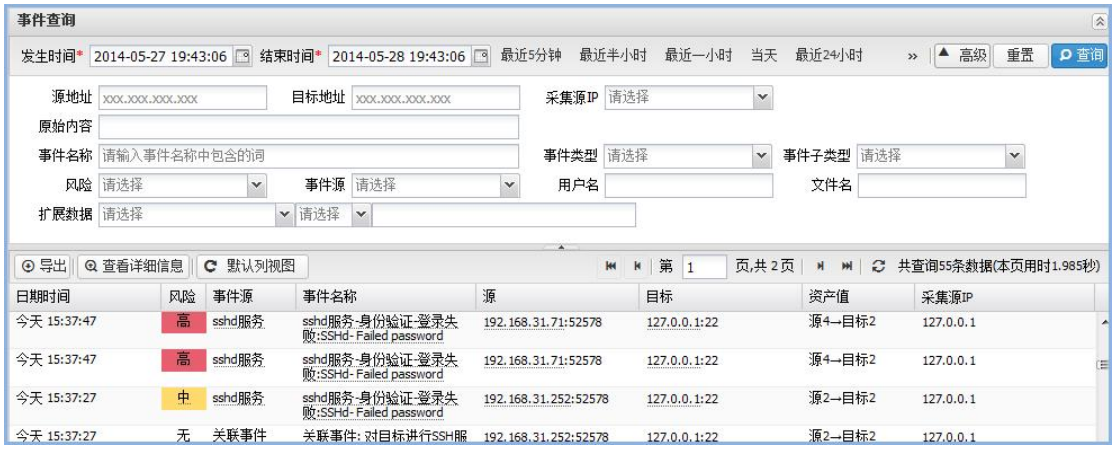


图 6-1

6.1. 查询条件

系统支持事件查询条件：时间查询（时间是查询的必要条件，<默认当天>）和其它可选性条件查询（其中包括：A:普通查询：源地址，目标地址，采集源 IP，原始内容。B 高级查询：事件名称，事件类型，事件子类型，风险，数据源，用户名，文件名，扩展数据）进行查询系统日志信息。如图所示：

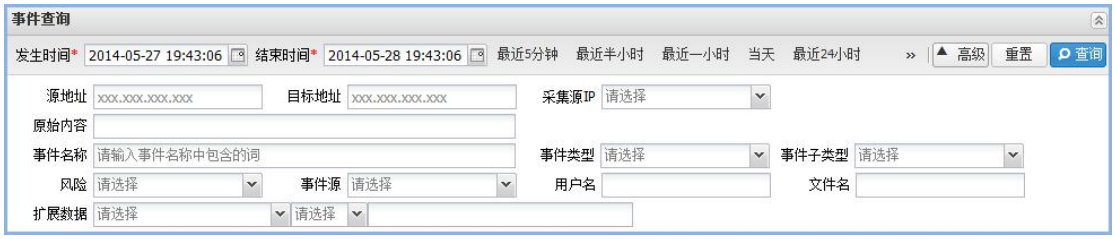


图 6-2

点击“**高级**”按钮，用户可进行普通查询和高级查询之间的切换。

点击“**重置**”按钮，其他可选性条件清空，时间查询不受重置功能影响

注：点击 按钮，可以将查询条件收起和展开。

6.1.1. 时间查询

用户可根据需要选择日志发生时间和结束时间也可手动输入，时间控件随用户对时间的选取需要而即时改变，点击时间控件图标选择所需时间，其中时间的年月日均可通过控件选择，时间的时分秒均可选择也支持手动输入。时间支持快速查询时间，分别有：最近 5 分钟，最近半小时，最近一小时，当天，最近 24 小时，最近一周，最近一个月。如图所示：

图 6-3

用户选择所需时间后点击“**查询**”按钮，即可查询出相应的日志信息内容并在界面显示。

6.1.2. 其它条件查询

可选性条件查询可单一条件查询并且可以选择使用普通查询还是高级查询，也可以组合条件查询，查询时必须伴有正确的时间查询条件，可选性条件查询支

持自动输入（即查询出条件单机所想输入的查询条件内容，即可自动显示在查询条件输入框中）。如图所示：

图 6-4

其中输入已有条件后点击**“查询”**按钮，即可查询出符合条件的日志信息内容并在界面显示。

6.2. 查询结果

输入查询条件后，点击**“查询”**按钮，界面显示出符合条件的所有日志信息，日志日期时间倒序展示。如果原始内容过多。用户可以将鼠标搁置原始内容信息处，系统会以 TIPS 形式供用户查看此条全部的信息内容。您也可以打开详细信息框查看详细的信息内容。如图所示：

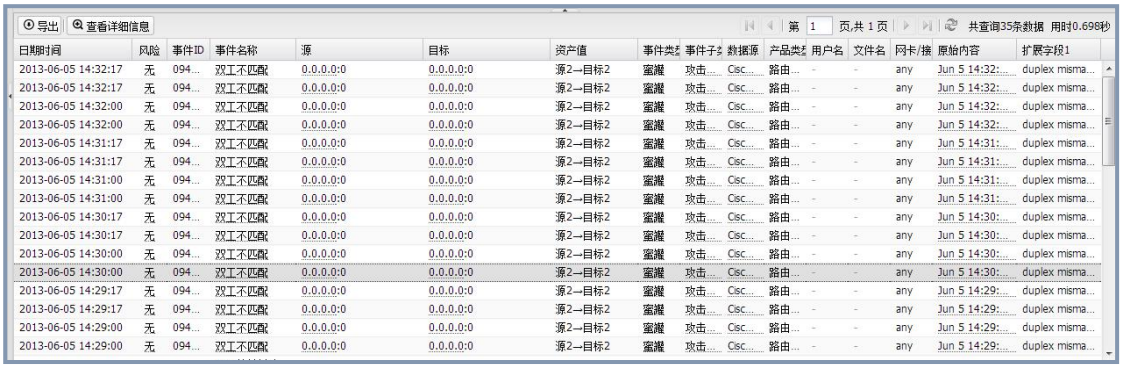


图 6-5

每页默认展示 50 条信息。超出 50 条，用户可点击翻页按钮，查看信息内容。查询结果中右侧上端会显示本次查询数据总数及本次查询耗时 xx/秒。(信息结果最多展示 200000 条数据)。如图所示:

图 6-6

6.2.1. 查看详细信息

点击**“详细信息”**按钮，弹出详细信息框，展示所有字段，可以查看每条信息的详细信息内容（您也可以鼠标左键双击主界面查询结果中的信息），如图所示:

图 6-7

6.2.2. 配置列的选择

查询结果在主界面显示默认配置列：日期时间，风险，事件名称，源，目标，资产值六项配置列，用户可以自主筛选配置列展示项，点击 

图中箭头处（鼠标搁置每项配置列最右端处即可出现该箭头），会弹出所有配置选项。如图所示：

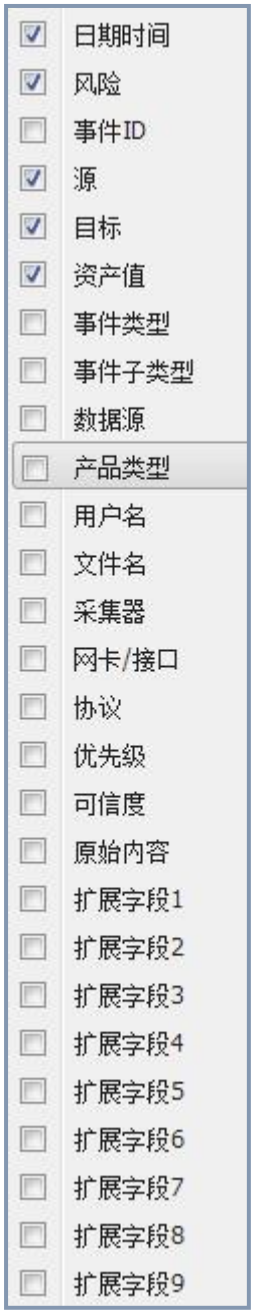


图 6-8

勾选的每项配置列名称，即可在查询结果主界面展示出已勾选的配置列。

6.3. 事件导出

事件条件：查询结果展示后导出或设定条件后直接导出，导出内容：原日志

内容，导出格式：Ecxle 文档的 cvs 格式。点击“导出”按钮，系统会弹出**“打开，保存”**提示窗口，如图所示：

图 6-9

点击**“保存”**按钮，系统会接着弹出**“另存为”**提示窗口。如图所示：

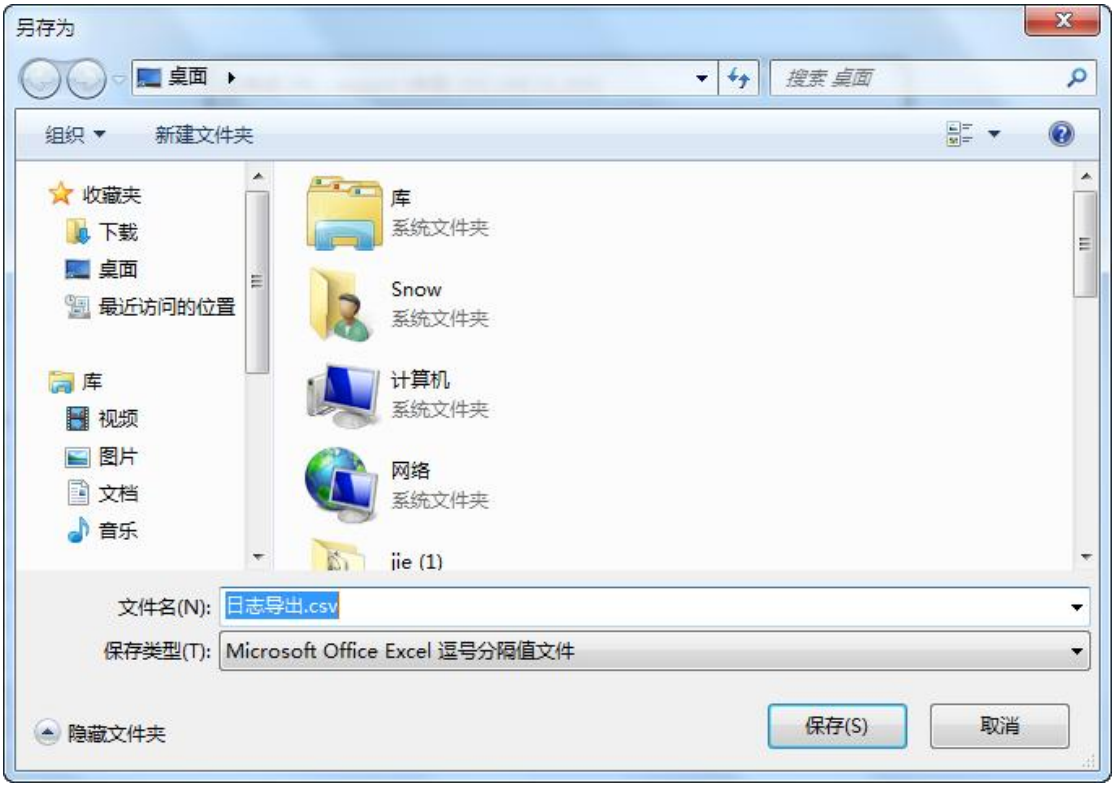


图 6-10

您可以输入命名保存文件，点击**“保存”**按钮即可成功导出日志信息的详细内容，通过 EXCLE 文档格式查看，导出的日志日期时间倒序显示。

导出功能最多可支持 1000 条信息的导出，如果你导出的日志信息条数大于 1000 条，点击“导出”按钮后，系统会弹出提示窗口。如图所示：

图 6-11

点击**“确定”**按钮。系统会默认的导出最新的 1000 条数据信息供用户查看，点击**“取消”**按钮。则放弃此次的事件。

7.关联分析规则

7.1. 交叉关联规则

7.1.1.交叉关联规则的界面展示

日志审计系统首界面菜单栏点击**“关联分析规则”——“交叉关联规则”**页签，如图所示：

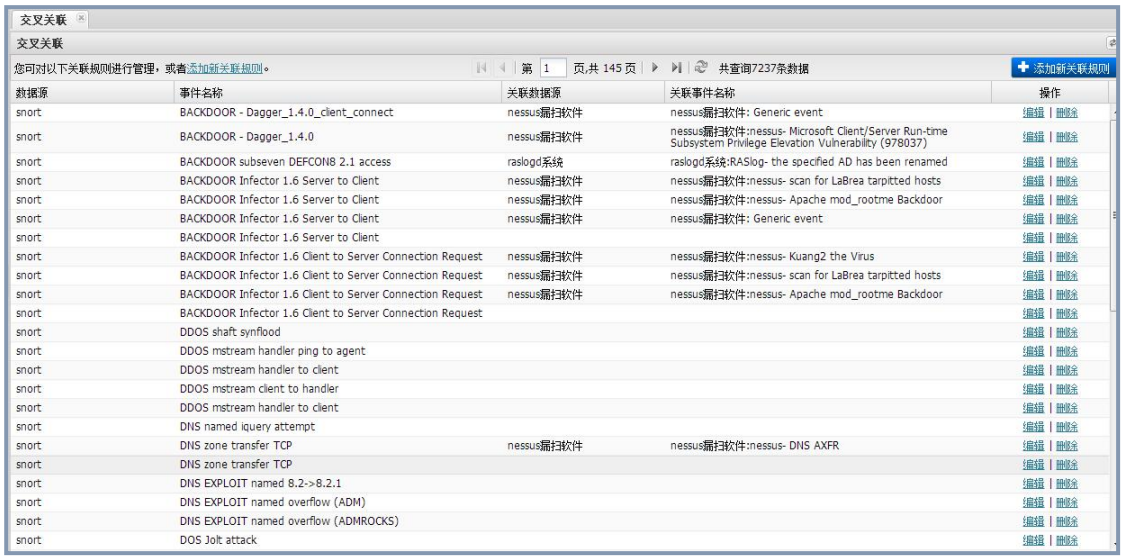


图 7-1

交叉关联规则每页展示 50 条关联规则，大于 50 条规则时，可以点击翻页按钮查看每条规则。

7.1.2. 交叉关联规则的添加

点击 

，用户可以手动添加新的交叉关联规则，点击下拉按钮选择数据源，事件名称，关联数据源，关联事件名称，如图所示：

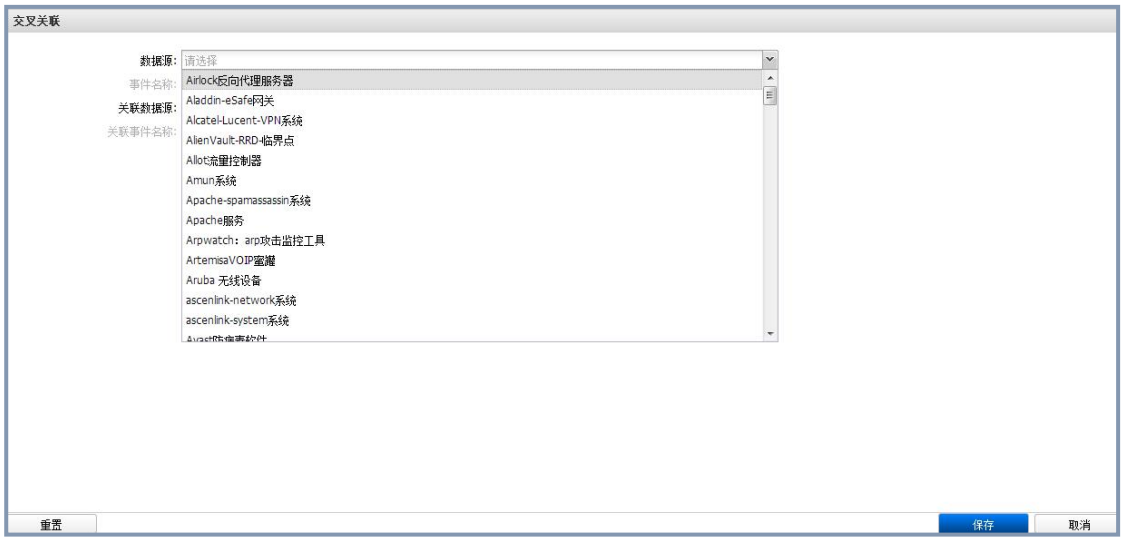


图 7-2

规则中的四项元素选择但未保存时，点击**“重置”**按钮，规则中的四项元素被清空，您需重新选择关联。

选择要关联的规则中的四项元素，点击**“保存”**按钮，成功添加新关联规则（新添加的交叉关联规则在交叉关联最后一页最后一条显示）。

选择要关联的规则中的四项元素中任意一项，点击**“取消”**按钮，此时系统弹出提示信息，如图所示：

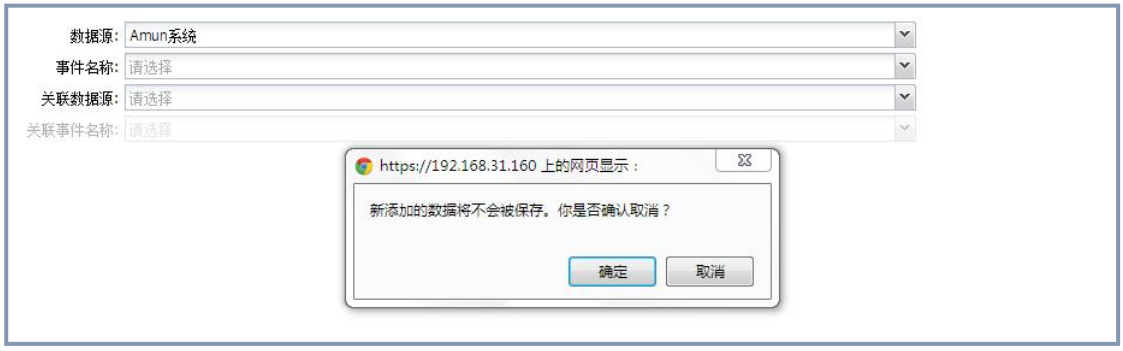


图 7-3

点击**“确定”**按钮，退出添加关联规则界面，页面跳转到交叉关联规则主界面，点击**“取消”**按钮，提示框关闭，您可继续操作您要添加的新关联规则。

添加新的关联规则后，点击**“应用”**按钮，弹出温馨提示框。如图所示：

图 7-4

7.1.3. 交叉关联规则的编辑

交叉关联规则主界面点击“编辑”按钮，如图所示：

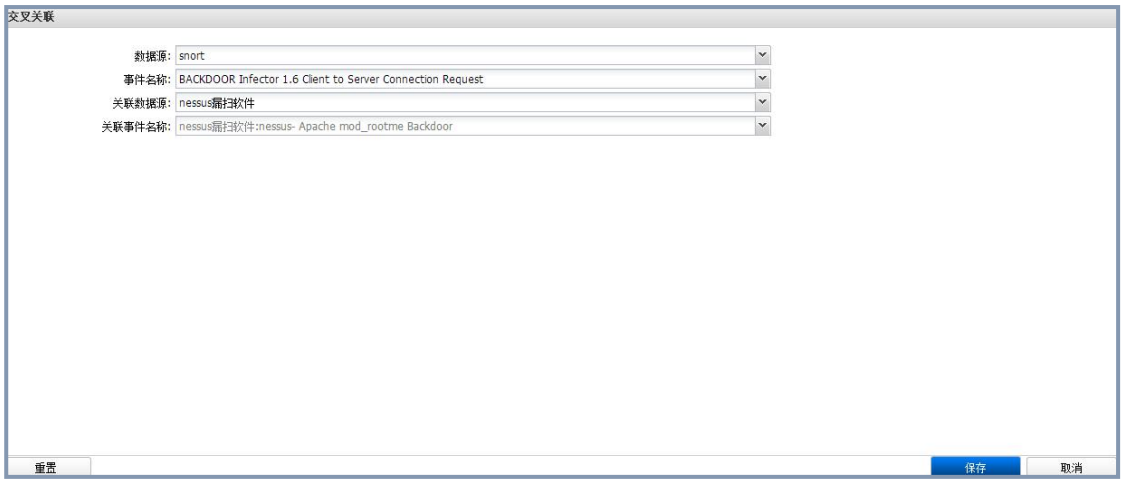


图 7-5

若对四项元素进行修改，点击**“重置”**按钮，恢复原有规则，点击**“保存”**按钮，保存修改后的规则，点击**“取消”**按钮，弹出提示框，如图所示：

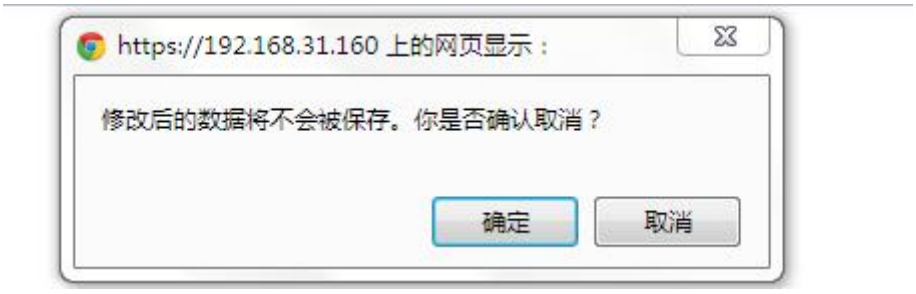


图 7-6

若点击**“确定”**按钮，系统界面显示交叉关联主界面，点击**“取消”**按钮，

恢复交叉关联规则编辑界面

7.1.4. 交叉关联规则的删除

交叉关联主界面点击“删除”按钮，如图所示：

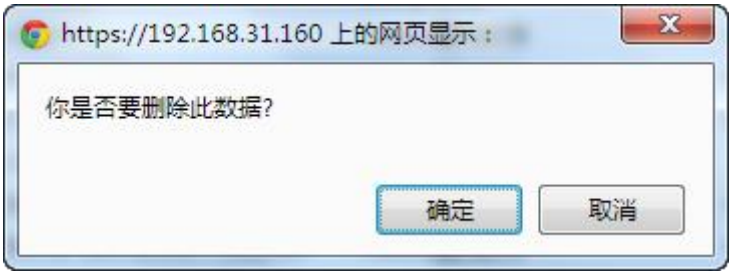


图 7-7

点击“确定”按钮，该规则被删除，显示交叉关联主界面

7.2 逻辑关联规则

- 逻辑关联规则为 esm 产品中最核心关联功能，为用户提供灵活、强大的关联规则，可以从源目的 ip、端口、事件类型等多维护进行关联，以发现隐藏较深的安全问题。逻辑关联模块内置一些常用的关联分析规则，用户也可以根据自己的需要新增一些关联分析规则，下面简单介绍一下该模块的各个功能的使用及用户自定义关联规则的配置过程。

- 在系统功能菜单点击关联分析规则→逻辑关联规则，可以看到逻辑关联规则的主界面（如图）

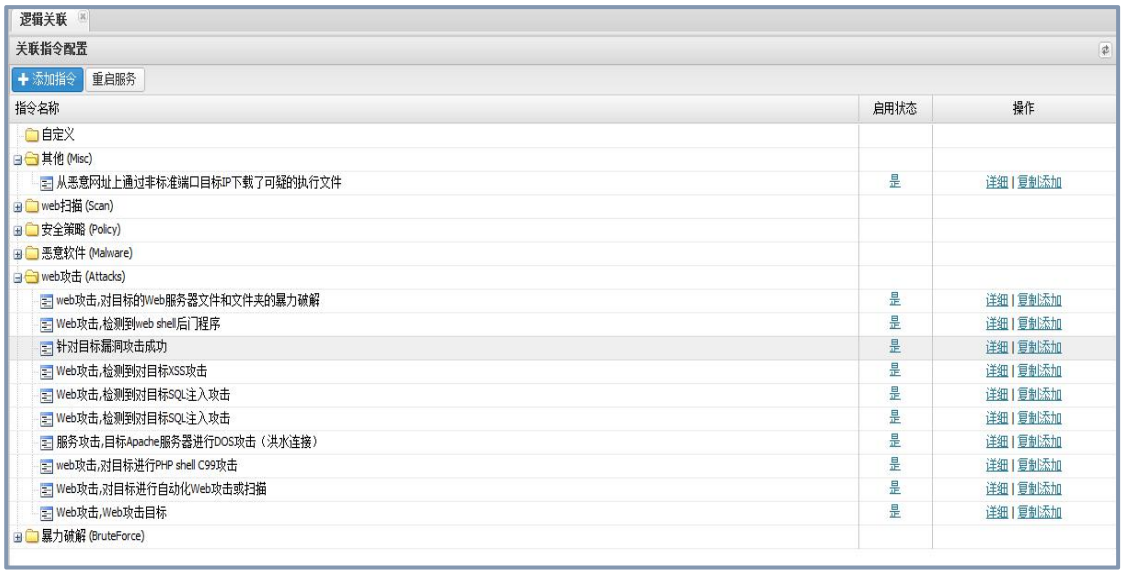


图 7-8

界面（关联指令配置）主要包含：两个功能按钮（添加指令和重启服务），关联规则的启用状态和支持的操作。

功能按钮的使用介绍：

添加指令按钮：即用户可以添加自定义关联规则的按钮，点击“添加指令”，进入自定义规则的编辑界面（如图）：

图 7-9

1. 定义关联规则的名称（必填）

2. 设定关联规则的优先级（优先级范围：1--5）

定义完成后，点击“下一步”按钮，界面跳转到关联规则具体关联事件界面

(如图)

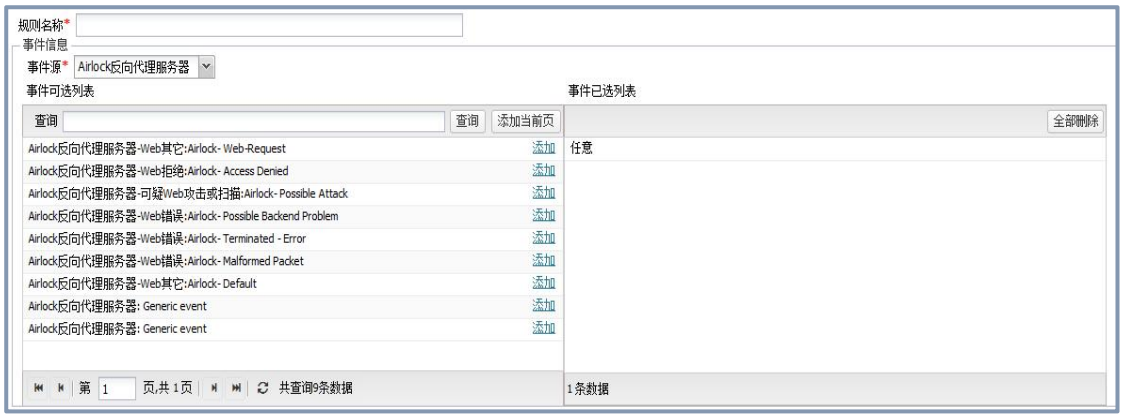


图 7-10

3. 在这个界面，用户可以自定义规则名称（必填），选择事件源（支持首字母筛选，查询功能），添加一个或多个关联事件，也可以点击“添加当前页”按钮，添加某事件源的所有关联事件。

4. 定义源地址和目的地址（如图）

图 7-11

点击“添加”（如图）

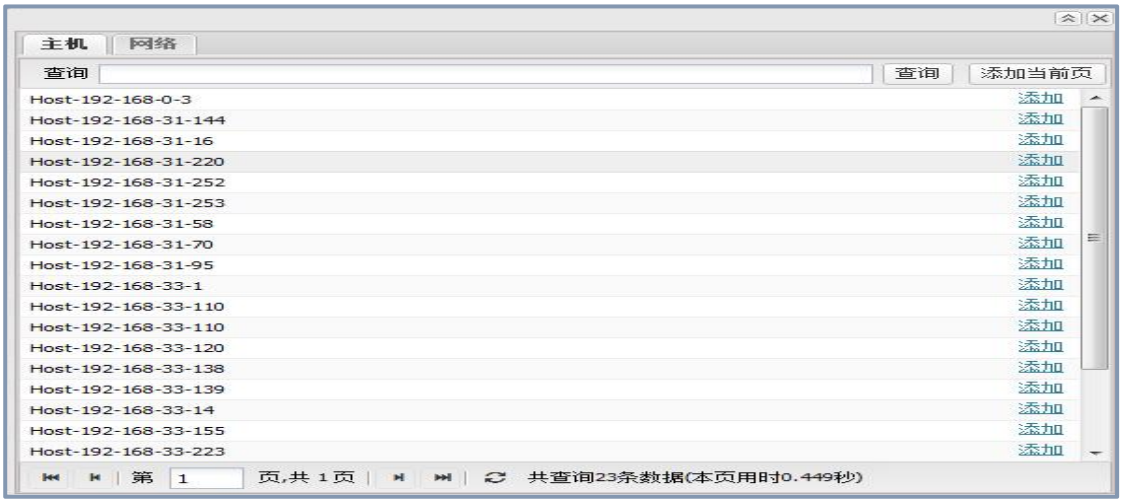


图 7-12

在这个界面，可以选择单个主机或多个主机（支持查询和添加当前页的功能，点击对应的按钮即可），也可以定义单个网络或多个网络内的主机（切换到网络界面下添加即可），还可以自定义具体的端口。（注：源地址和目的地址添加过程相同）

5. 定义规则的可靠度，协议和其他选填项内容（如图）

图 7-13

这个界面定义规则的可靠度（绝对值和相对值的范围 1--10），协议（TCP，

UDP，ICMP）三个选项不可以同时取消，选填项部分（可以不添加)。

以上配置完成后，点击**“保存”**按钮，新定义关联的规则添加完成。(如图)

图 7-14

可以在此界面重新编辑，查看更多的内容，还可以在此规则下添加一条或多条子规则（添加方式同添加新指令过程）

全部添加完成后，可以在自定义里看到新增的关联规则，并可以对其重新编辑，删除的操作。

注：用户也可以在内置的关联规则中，复制添加一条或多条规则，按照自己的需要进行编辑操作（具体操作同新添加指令的过程)，用户每次添加或进行编辑 (删除) 操作，更改启用状态后，需要重启服务才能生效 (即在主界面点击“重启服务”按钮即可)。

8.资产管理

8.1 主机

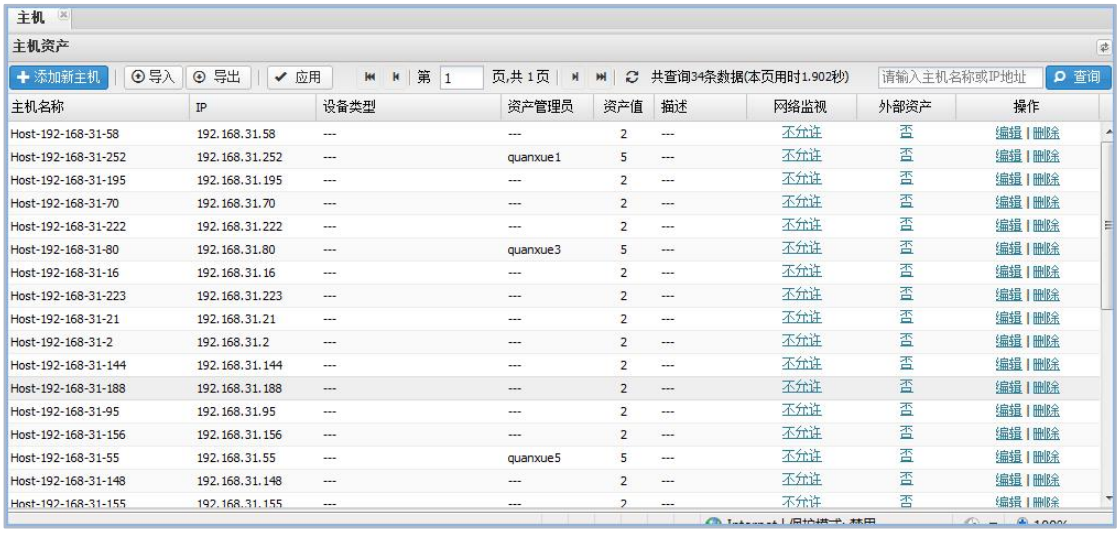


图 8-1

主机资产信息，包括：主机名称，IP，设备类型，资产值，描述，网络监视，内部资产，操作等。

页面展示功能按钮，包括：

"导入"按钮：导入主机资产的配置（.csv 格式）；

"导出"按钮：导出主机资产的配置信息（.csv 格式）；

"应用"按钮：使主机资产配置信息生效。

中间"上一页"和"下一页"刷新等操作。

网络监视的"允许"：允许监视该主机，单击即为不允许（也可进编辑界面高级下操作）；

网络监视的"不允许"：不允许监视该主机，单击即为允许（也可进编辑界面高级下操作)；

操作功能的"编辑"：点击进入编辑页面，可以对该主机的配置信息进行编辑更改；

操作功能的"删除"：即删除该主机资产的信息。

说明：普通用户不可对主机信息进行添加、导入、编辑、删除等操作。

8.1.1 添加新主机

点击"添加新主机"按钮，显示添加新主机的基本信息，如图：

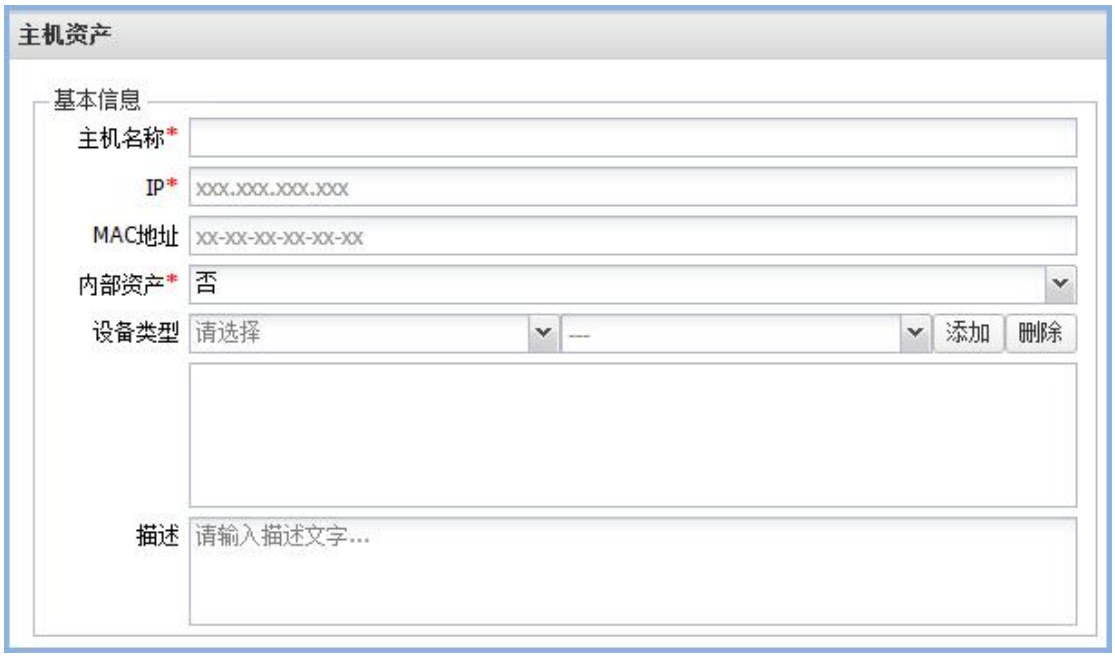


图 8-2

基本信息包括：主机名称，IP，MAC 地址，内部资产，设备类型，描述。(其中主机名称，IP，内部资产为必填项)

主机名称：配置主机的名称（自定义)。

IP：配置主机的 IP 地址（正确的 IP 格式)。

MAC 地址：配置主机的物理地址（选填)。

内部资产：定义是否为内部资产。

设备类型：配置主机的设备类型（提供候选项)。

描述：对配置主机进行描述。

设备详细：(如图)

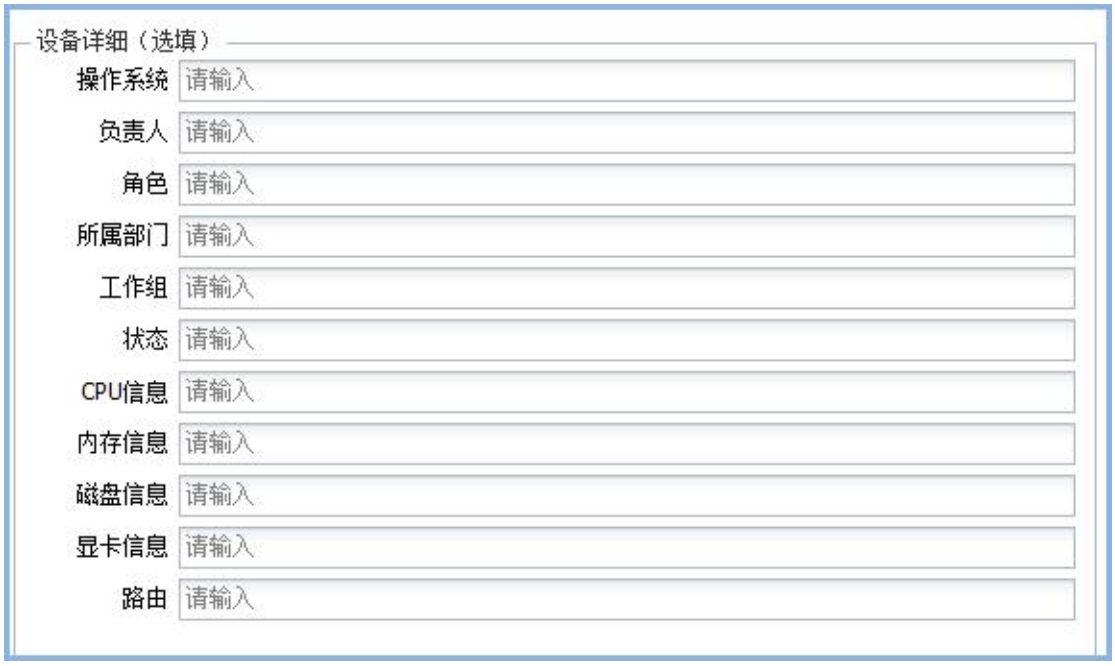


图 8-3

设备详细（选填）包括:操作系统，负责人，角色，所属部门，工作组，状态，CPU 信息，内存信息，磁盘信息，显卡信息，路由。

高级：(如图）包括资产值（必填）和网络监视（是否允许)。

图 8-4

8.2 主机组

主机组界面（如图）：

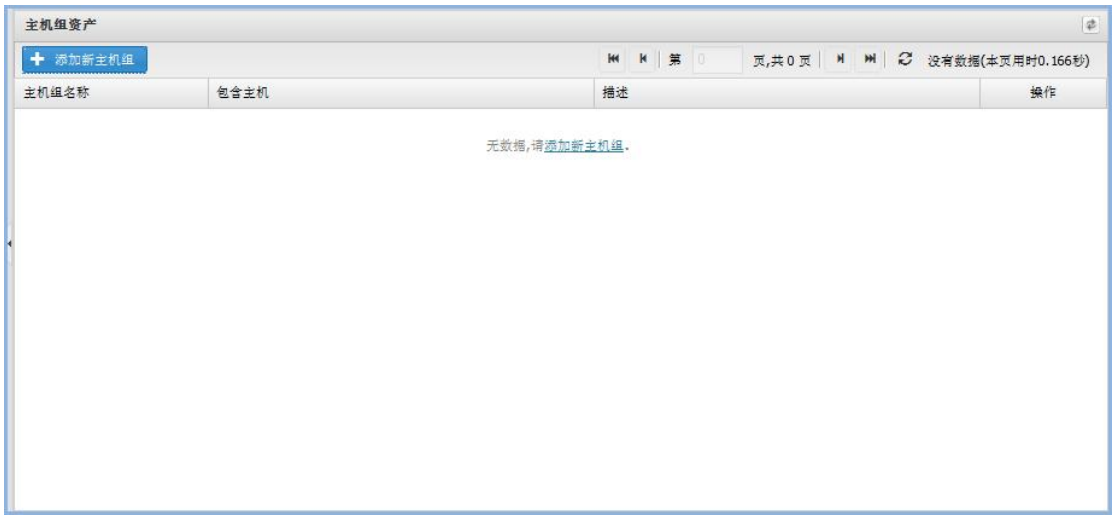


图 8-5

主机组资产信息，包括:主机组名称，包含主机，描述，操作。

页面展示功能按钮，包括：

操作功能的"编辑"：点击进入编辑页面，可以对该主机组的配置信息进行编辑更改；

操作功能的"删除"：即删除该主机组资产的信息。

8.2.1 添加信息主机组

点击"添加新主机组"按钮，页面显示新主机组的基本信息界面：

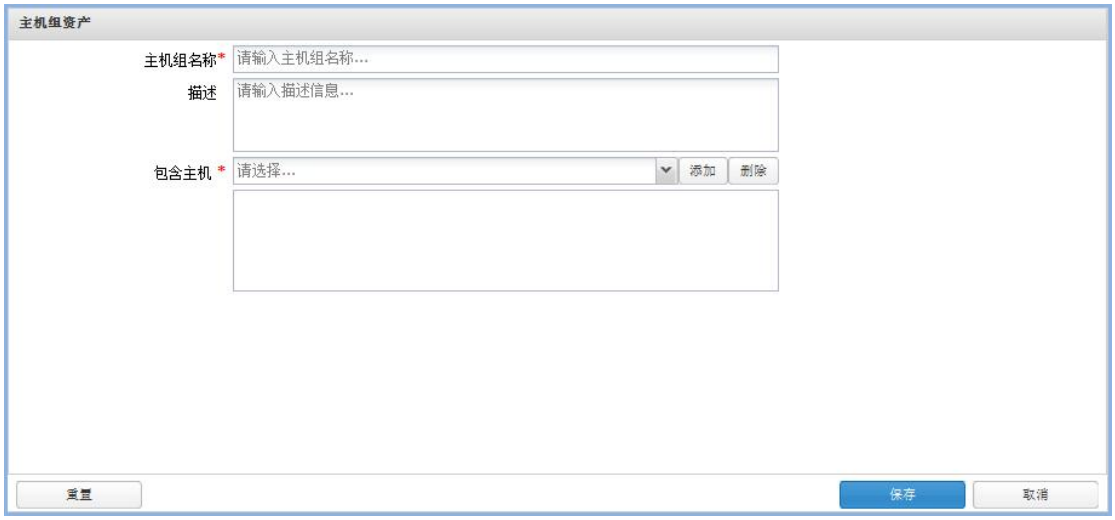


图 8-6

基本信息包括:主机组名称，描述，包含主机。(其中主机组名称和包含主机是必填项)

主机名称：配置主机组的名称（自定义）。

描述：对配置主机组进行描述。

包含主机：对已有主机选择添加。

8.3 网络

网络主界面显示（如图）：

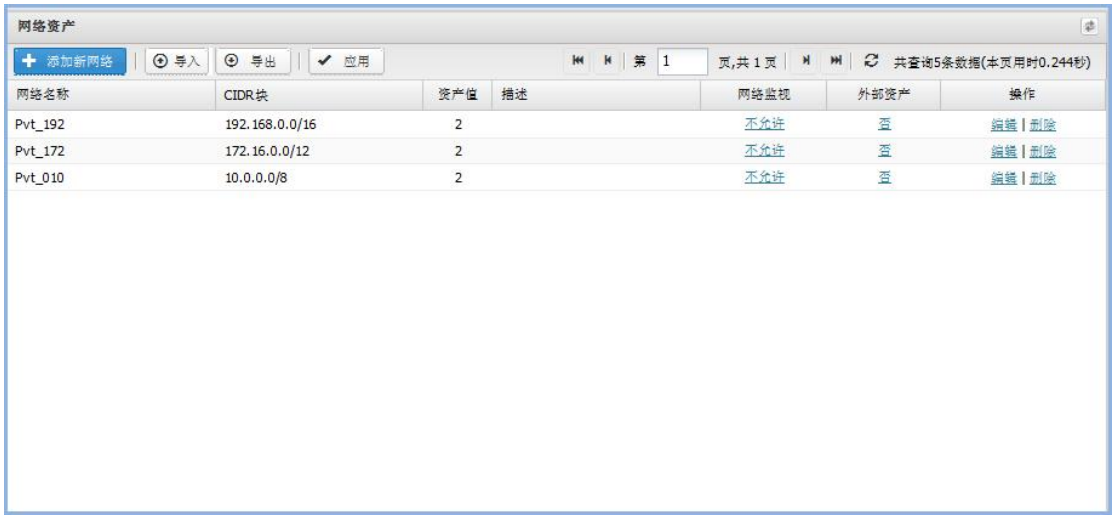


图 8-7

网络资产信息，包括：网络名称，CIDR 块，资产值，描述，网络监视，外部资产，操作等。

页面展示功能按钮，包括：

"导入"按钮：导入网络资产的配置（.csv 格式)；

"导出"按钮：导出网络资产的配置信息（.csv 格式)；

"应用"按钮：使网络资产配置信息生效。

中间"上一页"和"下一页"刷新等操作。

网络监视的"允许"：允许监视该网络，单击即为不允许（也可进编辑界面高级下操作)；

网络监视的"不允许"：不允许监视该网络，单击即为允许（也可进编辑界面高级下操作)；

操作功能的"编辑"：点击进入编辑页面，可以对该网络的配置信息进行编辑更改；

操作功能的"删除"：即删除该网络资产的信息。

8.3.1 添加新网络

点击"添加新网络"按钮，显示网络基本信息编辑界面（如图）：

图 8-8

基本信息包括：网络名称，CIDR 块，外部资产，描述。(网络名称，CIDR 块必填项)

网络名称：配置网络的名称（自定义）。

CIDR 块：配置网络 IP。

外部资产：定义是否为内部资产。

描述：对配置网络进行描述。

高级（如图）：包括资产值（必填）和网络监视（是否允许）。

图 8-9

8.4 网络组

网络组显示界面：(如图)

图 8-10

网络组资产信息包括：名称，包含网络，描述，网络监视，操作等。

页面展示功能按钮包括：中间"上一页"和"下一页"刷新等操作。

操作功能的"编辑"：点击进入编辑页面，可以对该网络组的配置信息进行编辑更改；

操作功能的"删除"：即删除该网络组资产的信息。

8.4.1 添加新网络组

点击"添加新网络组"按钮，显示新网络组的基本信息：(如图)

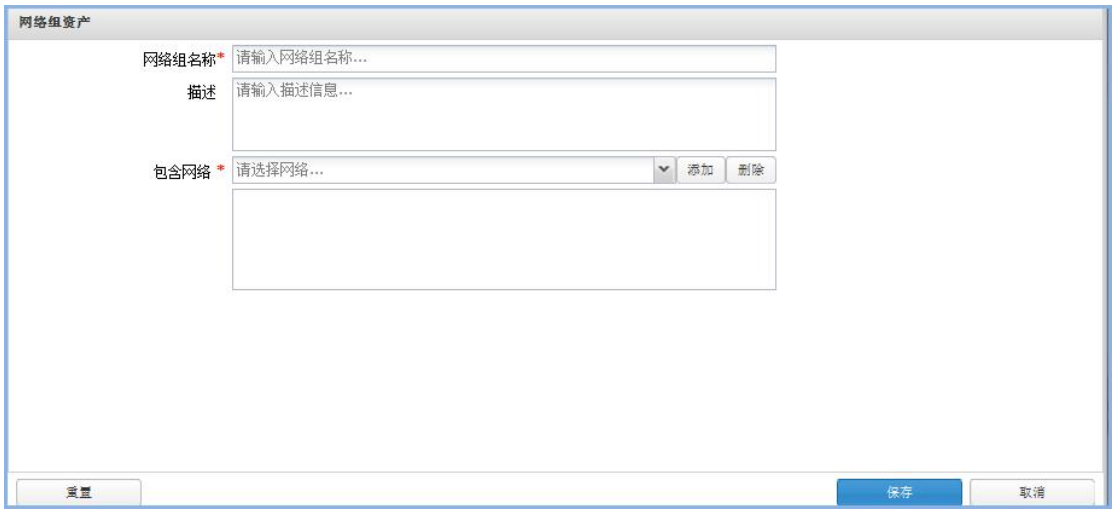


图 8-11

基本信息包括：网络组名称，描述，包含网络。

网络名称：配置网络组的名称（自定义）。

描述：对配置网络进行描述。

包含网络：选择已添加的网络进行添加或删除。

8.5 端口

端口信息界面显示（如图)：

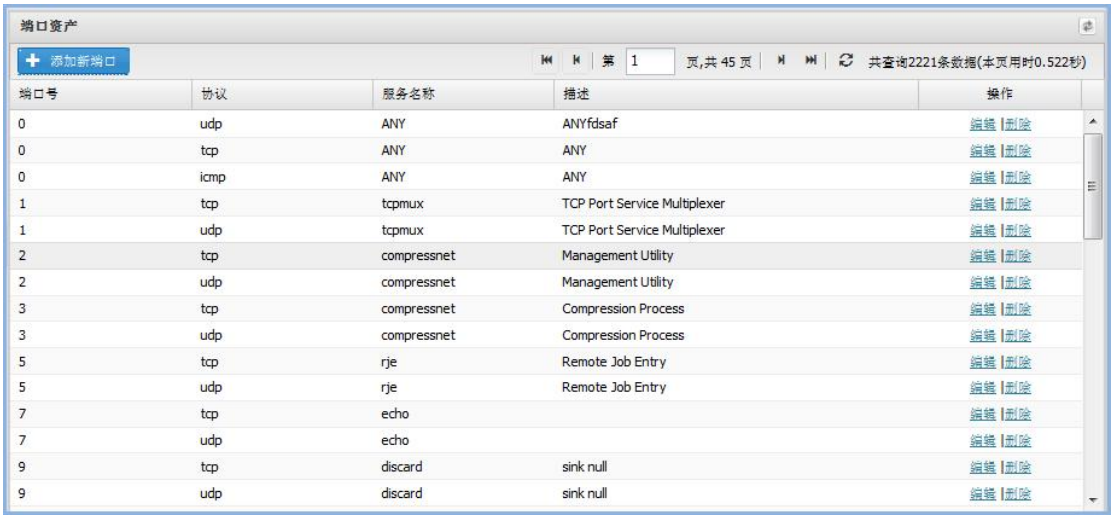


图 8-12

端口资产信息，包括：端口号，协议，服务名称，描述，操作。

中间"上一页"和"下一页"刷新等操作。

操作功能的"编辑"：点击进入编辑页面，可以对该端口的配置信息进行编辑更改；

操作功能的"删除"：即删除该端口资产的信息。

8.5.1 添加新端口

点击"添加新端口"按钮，显示新端口的基本信息（如图）：

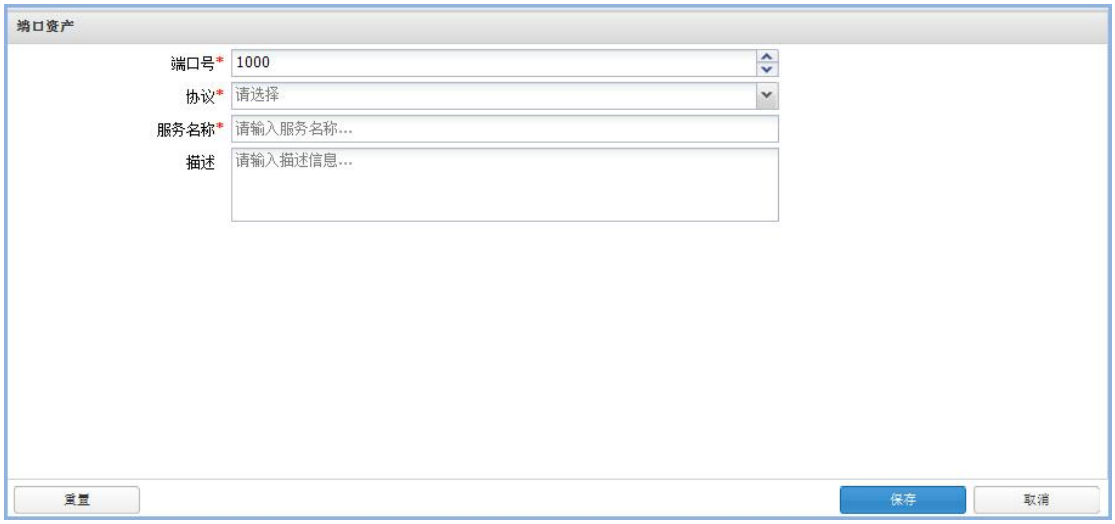


图 8-13

基本信息包括：端口号，协议，服务名称，描述。

端口号：输入端口号（端口号：1-65535)。

协议：下拉选择项，包含'tcp','udp','其它'

服务名称：编辑端口的名称（自定义)。

描述：对新端口信息进行说明。

8.6 端口组

端口组界面显示:(如图)

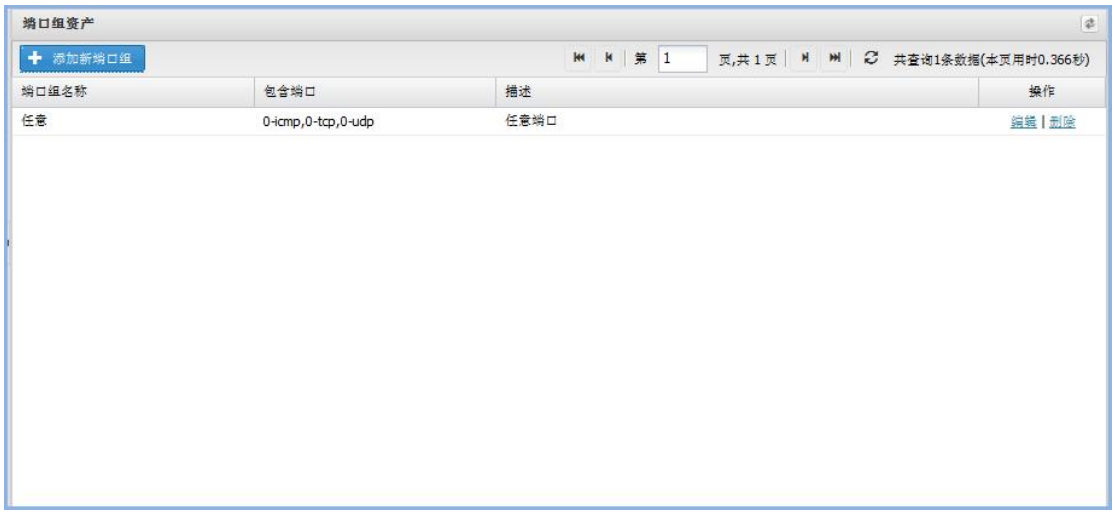


图 8-14

端口资产信息，包括：端口组名称，包含端口，描述，操作。

中间"上一页"和"下一页"刷新等操作。

操作功能的"编辑"：点击进入编辑页面，可以对该端口组的配置信息进行编辑更改；

操作功能的"删除"：即删除该端口组资产的信息。

8.6.1 添加新端口组

点击"添加新端口组"按钮，显示新端口组的基本信息：(如图)

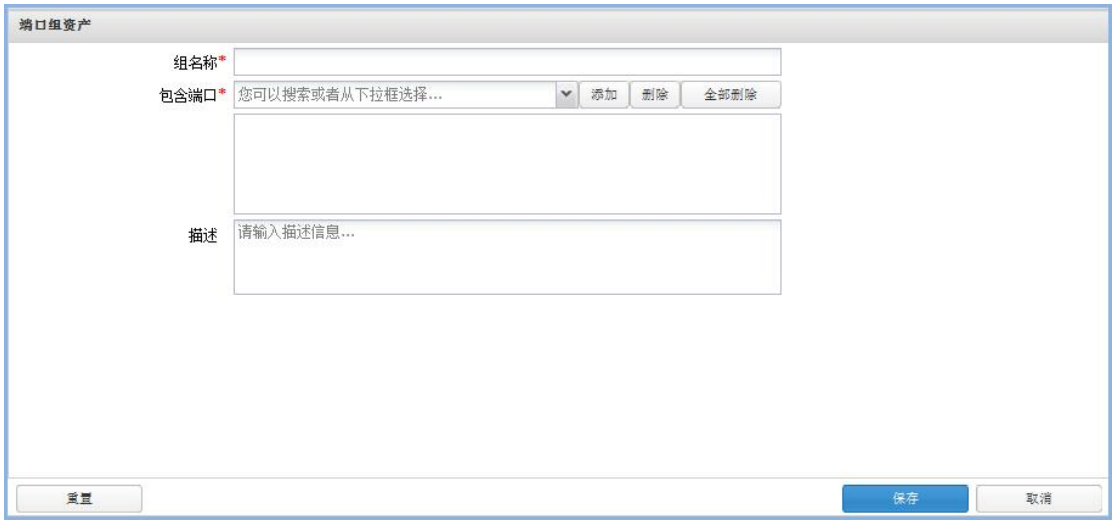


图 8-15

基本信息包括：组名称，包含端口，描述。

组名称：配置端口组的名称（自定义）。

包含端口：配置端口选择，添加，删除，全部删除。

描述：对添加的端口组信息进行说明。

8.7 漏扫报告

漏扫报告界面显示：（如图）

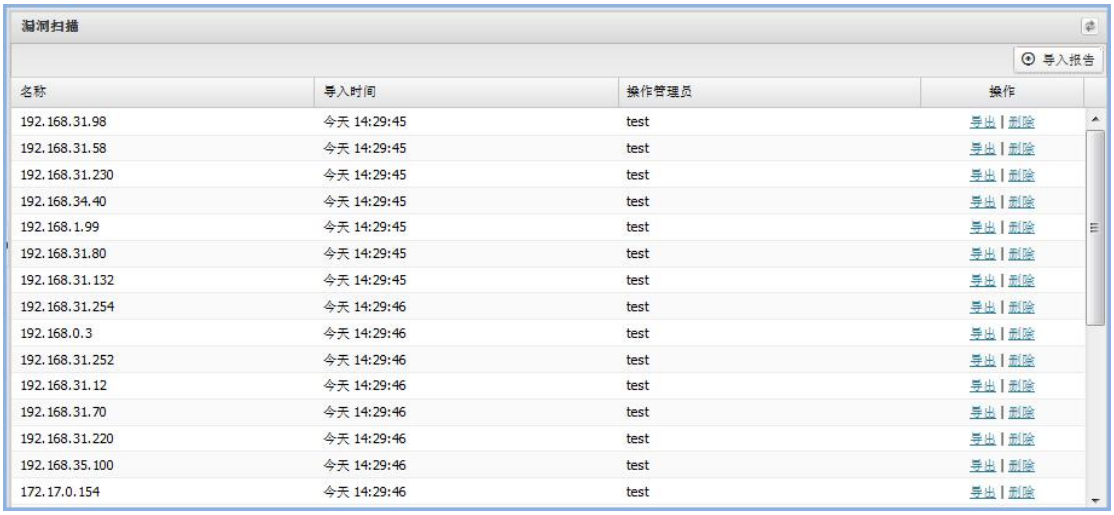


图 8-16

漏扫报告信息包括：名称，导入时间，操作管理员，操作。

点击"导入报告"按钮，选择'扫描设备'、'报告类型'下拉菜单选择名称和格式类型。点击"导入"按钮，选择文件导入即可。

8.7.1 其它操作

操作功能的"导出"：对漏扫报告导出，选择文件存在路径导出就可以了。

操作功能的"删除"：即删除该漏洞扫描的信息。

9.策略

拥有策略管理权限的用户，左侧菜单栏点击策略管理，展开策略管理功能包含项：策略配置、策略组管理、响应行为配置。用户可自己添加策略组供添加策略配置界面调用，系统设有默认策略组，用户添加策略后可分组查

看与管理。当用户配置的策略被命中后，根据用户在响应行为配置界面设置的相关，通过邮件方式或 sysylog 方式通知用户。

9.1 策略配置

用户可通过配置策略从而更改日志信息的优先级达到事件信息进行响应行为的处理效果：

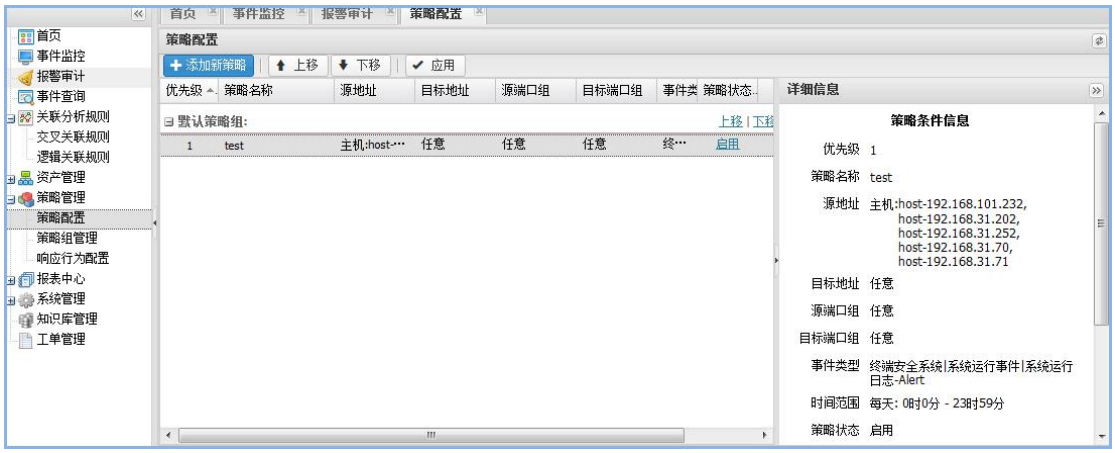


图 9-1

9.1.1添加新策略界面功能

用户在策略配置界面，点击“添加新策略”按钮或点击“添加新策略”链接。即可打开添加新策略界面。滚动条向下拉。可查看完整的添加新策略界面，此界面包含基本信息的输入，条件配置的选择，响应结果的配置。编辑后，点击“重置”按钮，则所有信息被清空为进入界面时的初始状态，点击“保存”按钮，可以保存已经编辑的信息，跳转至响策略配置界面。如果已填相关内容，点击“取消”按钮，界面会弹出温馨提示窗口。如果未填写相关内容，点击“取消”按钮，当前界面关闭，跳转至策略配置界面。如图

所示：

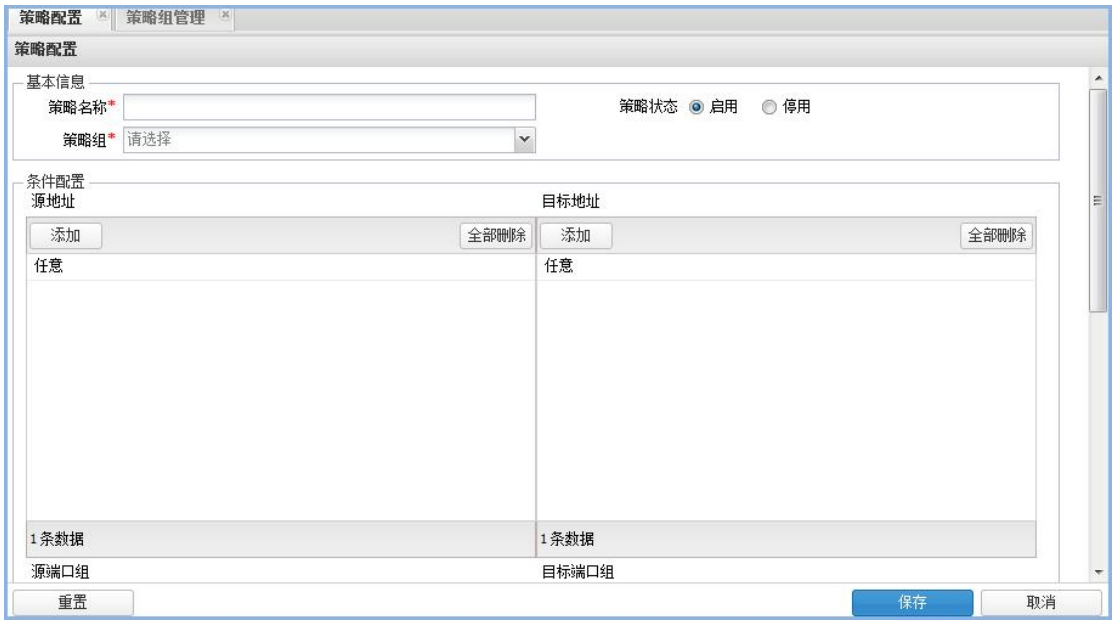


图 9-2

9.1.1.1 基本信息栏

添加新策略基本信息的填写：A:策略名称为必填项，用户需输入最大字符不能超过 64 位，字符类型无限制。B:策略组的选择为必填项，用户需点击策略组下拉框选择策略组名称，如果未配置添加策略组，可选择默认策略组。C:策略状态“启用与停用”必填一项（策略状态默认为“启用”状态），保证该条策略生效的最根本需求是策略状态为“启用”状态。如图所示：

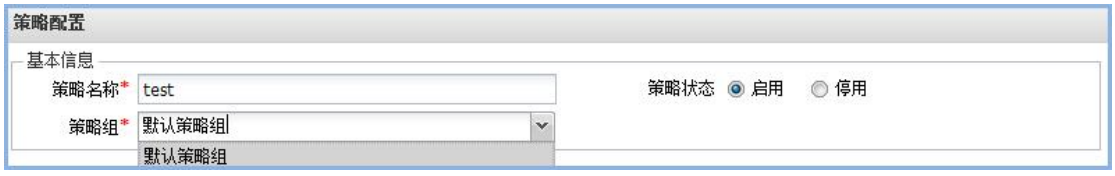


图 9-3

9.1.1.2 条件配置栏

源地址的选择：源地址、目标地址、源端口组、目标端口组四项操作类似。如图所示：

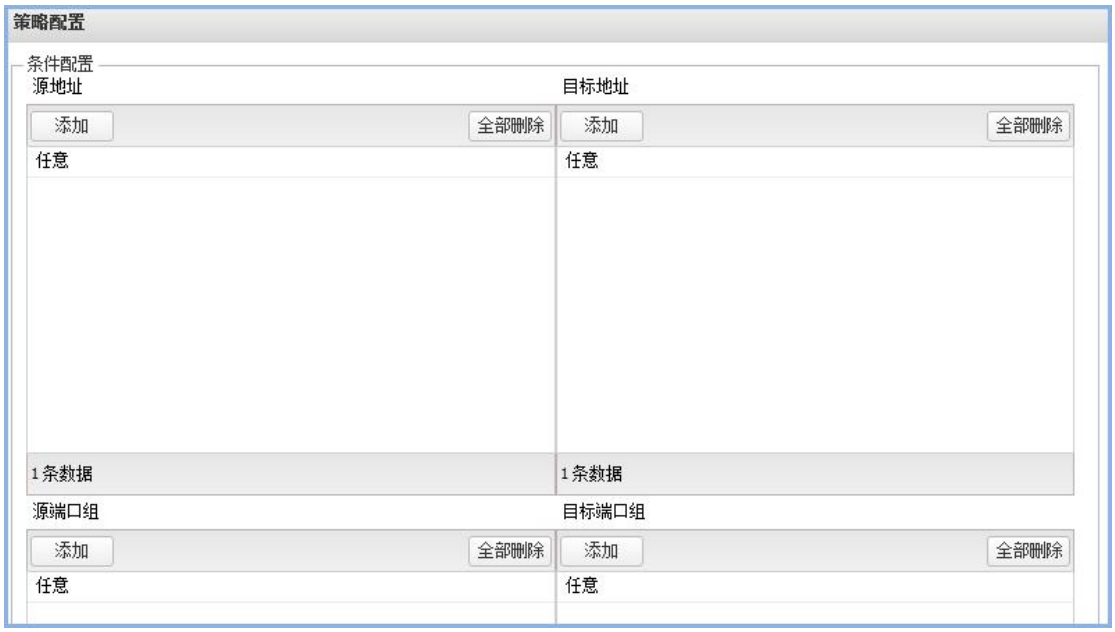


图 9-4

我们现在以源地址为例：用户点击点击新策略按钮或链接，页面跳转到添加新策略界面，输入必填项策略名称，选择策略组，条件配置栏中点击源地址下方“添加”按钮，弹出条件配置编辑窗口，供用户选择策略条件配置，该窗口包括的主要功能选项包括“主机”的添加、“主机组”的添加、“网络”的添加、“网络组”的添加。如图所示：

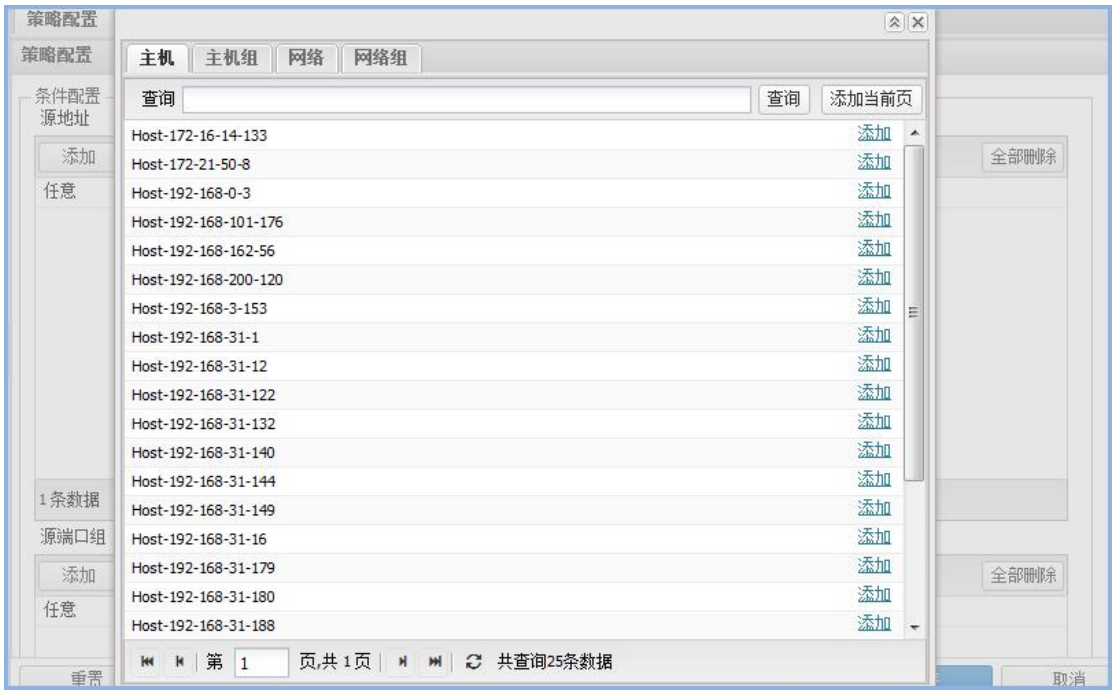


图 9-5

弹出的条件配置编辑窗口，默认会展示主机项的所有包含的主机信息，加载的数据与资产管理项中主机包含的数据一致，成功加载后，用户可点击“添加”按钮，此时添加所在行被显示到添加新策略界面条件配置栏中的源地址项中（数据量多时，该项支持翻页功能，并显示界面加载的总数），该编辑界面提供用户查询功能，当您主机包含项中信息过多时 ，您可以参照以显示的主机信息格式手动输入到查询框中（该输入框支持模糊查询），而后点击“查询”按钮，即可成功在下面空白处显示您所查询的相关主机名称。您也可以点击“添加当前页”按钮，当也显示的所有主机名称都会被成功显示添加新策略界面条件配置栏中的源地址项中。点击“关闭”图标，该窗口被成功关闭。（主机组、网络、网络组操作一致）。删除功能：添加条件后，点击框中每行的“删除”按钮，该条信息行被成功删除，如果您想删除所有添加的信息，可点击“全部删除”按钮，对应栏中的信息被全部删除。

事件类型条件的选择：您可以选择产品类型，事件类型，事件子类型。如图所示：

图 9-6

其中产品类型可以随意选择，与事件类型和事件子类型没有直接的关系。当您选择事件子类型的时候，必须要选择事件类型，否则点击没有任何效果。选定类型后，点击“添加”按钮，所选类型会自动添加到右侧框中显示，点击“删除”按钮。框中信息被成功删除，当框中有多条信息时 ，用户需选择一条一条信息删除，此框不支持全部删除效果。

时间范围的选择：时间分为四类，每天、每周、每月、和自定义，通过对事件的设置，用户可以选择在某个事件段时，日志信息在此时间段才会命中该策略，其他事件发生的日志信息均不会命中该条策略。如图所示：

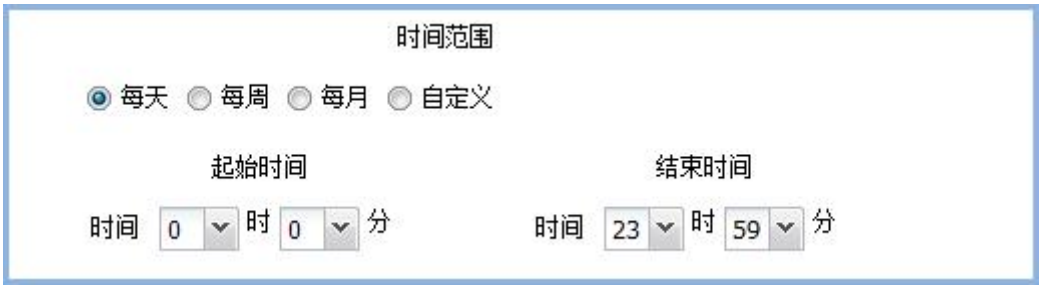


图 9-7

9.1.1.3 响应结果

点击“响应结果”展开按钮，可显示响应结果中用户可配置的包含信息项。用户可以通过对响应结果项的设置，确定一条原始信息命中策略后，优先级是否会被改变，是否报警，是否会走逻辑关联事件，是否会走交叉关联事件并觉得是否存储到数据库中。如图所示：

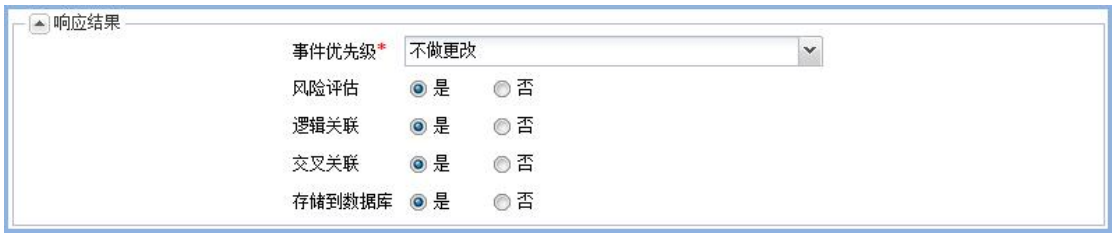


图 9-8

事件优选级：此项为必填项，默认为“不做更改”，点开下拉按钮，下拉框中为用户列出 5 个级别 ，用户可自由选择。

风险评估：如果用户风险评估选择“是”，则会报警，反之选择“否”则不会报警

逻辑关联：如果用户逻辑关联选择“是”，则会产生逻辑关联事件，反之选择“否”则不会产生逻辑关联事件

交叉管理：如果用户逻辑关联选择“是”，则会产生交叉关联事件，反之选择“否”则不会产生交叉关联事件

存储到数据库：如果存储到数据库选择“是”，则产生的事件会被存储到数据库中，反之选择“否”则不会存储到数据库中，信息的详细内容，优先级是否被更改也无法查看。

9.1.2 策略配置界面功能

成功添加新策略保存，自动跳转到策略配置界面，并显示已经添加的策略信息。此界面供用户添加新策略（用户可以在每项策略组直接点击并将策略添加到该策略组中），修改策略状态，编辑策略，删除策略，修改策略优先级，查看策略详细信息。如图所示：

图 9-9

添加新策略：用户点击**“添加新策略”**按钮，或者**“添加新策略”**链接，界面自动跳转到添加新策略界面。

编辑策略：用户点击**“编辑”**按钮，界面自动跳转到编辑界面（添加新策略界面），您可以对该条策略执行编辑操作，修改策略被命中的条件。

删除策略：用户点击“删除”按钮，界面会弹出确认删除提示框，点击**“确定”**按钮，该条策略即被删除，点击**“否”**按钮，或点击关闭图标，弹出窗口关闭。

策略状态：用户在添加新策略界面在不更改默认设置时,策略状态默认为“启动”，在策略配置界面。您可点击策略状态列中的“启动”，则该条策略此时状态被更

改为“停用”状态。相同的，您也可以在此处再次点击，将该条策略更改为“启用”状态。

上移下移按钮：用户点击此按钮，可以调整策略及策略组的优先级。当您点击策略配置界面顶端的上移下移按钮时，此按钮是对同一个策略组中的所有策略单条策略优先级的改变。当您点击展示列下方每项策略组右侧的上移下移按钮时，此按钮是对所有策略组之间优先级别的改变。

应用按钮：用户配置策略成功后，点击应用按钮，使所有策略已生效

详细信息板:一条策略配置成功后保存在策略配置界面，用户可以点击详细信息板展开按钮（图中标红区），弹出详细信息板供用户查看该条策略的所有详细信息内容。再次点击该按钮，详细信息板关闭。

刷新图标：用户可以点击界面右侧上端的刷新图标（图中标蓝区）刷新当前界面。

9.2 策略组管理

策略组管理界面可以给用户提供策略组的管理，系统有为您内置默认策略组，该项可以在您未添加任何策略组时提供给您添加策略时必填项选择策略组时使用。默认策略组不可进行编辑和删除操作。如图所示：

图 9-10

9.2.1 添加新策略组窗口功能

用户点击“添加新策略组”按钮，弹出添加新策略组窗口。如图所示：

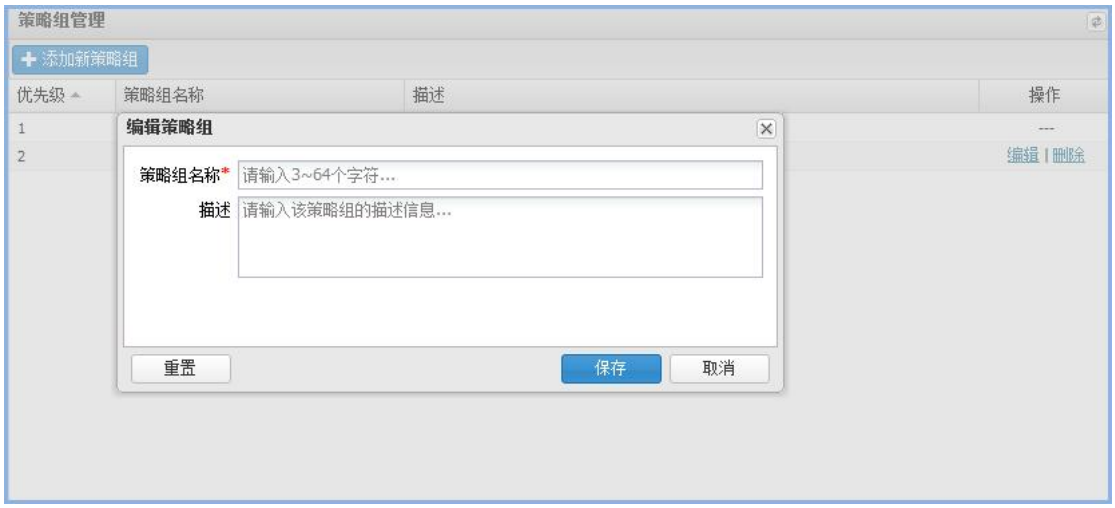


图 9-11

策略组名称：此项为必填项，需要用户输入 3-64 位字符，字符类型无限制。

描述：此项为可选项，是对该策略组的描述信息，您可根据个人需求决定是否填写该项。

重置按钮：当您输入错误信息或想全部删除已填写信息，用户可以点击**“重置”**按钮，即可清空用户所填写的所有信息，您可重新填写其他内容。

保存按钮：用户输入策略名称必填项，点击**“保存”**按钮，当前窗口被关闭，新添加的策略组被保存并在策略组管理界面显示。

取消按钮：当前窗口，用户点击取消按钮，窗口关闭，返回到策略组管理界面。

关闭图标：点击窗口右上方的关闭图标，当前窗口被关闭，返回到策略组管理界面。

9.2.2 策略组管理界面功能

用户在策略组管理界面可以添加新策略组，编辑策略组，删除策略组的操作。如图所示：

图 9-12

添加策略组：用户点击**“添加新策略组”**按钮，弹出添加新策略组窗口

编辑策略组：用户点击**“编辑”**按钮，界面弹出编辑窗口（添加新策略组窗口），您可以对该条策略执行编辑操作，修改策略组名称及描述。

删除策略组：用户点击**“删除”**按钮，界面会弹出确认删除提示框，点击**“确定”**按钮，该条策略即被删除，点击**“否”**按钮，或点击关闭图标，弹出窗口关闭。

刷新图标：用户可以点击界面右侧上端的刷新图标，刷新当前界面。

9.3 响应行为配置

9.3.1 添加新响应行为界面功能

日志信息产生报警事件或命中策略后会通过 syslog 日志和邮件发送两种方式通知用户，下图为响应行为配置界面。如图所示：

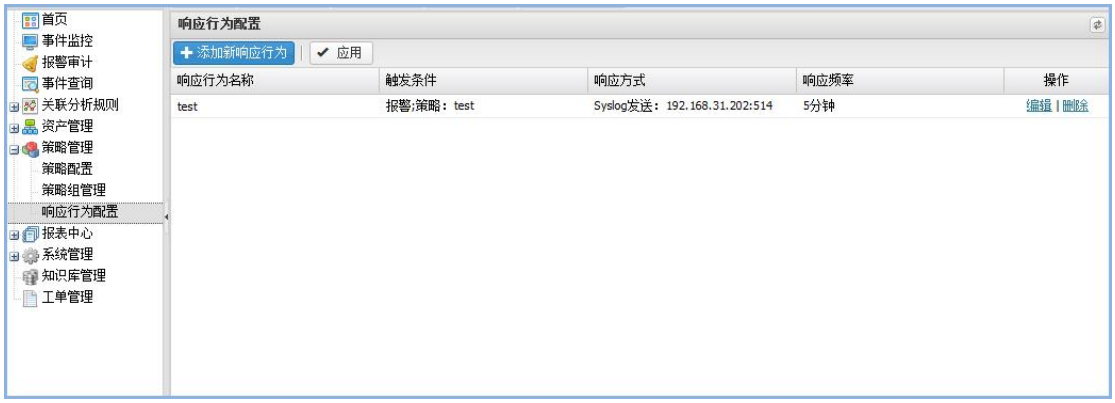


图 9-13

用户在响应行为配置界面，点击“添加新响应行为”按钮或点击“添加新响应行为”链接。即可打开添加新响应行为界面。滚动条向下拉。可查看完整的添加新响应行为界面，此界面包含基本响应行为名称、触发条件、响应方式、响应频率。编辑后，点击“重置”按钮，则所有信息被清空为进入界面时的初始状态，点击“保存”按钮，可以保存已经编辑的信息，跳转至响应行为配置界面。如果已填相关内容，点击“取消”按钮，界面会弹出温馨提示窗口。如果未填写相关内容，点击“取消”按钮，当前界面关闭，跳转至响应行为配置界面。如图所示：

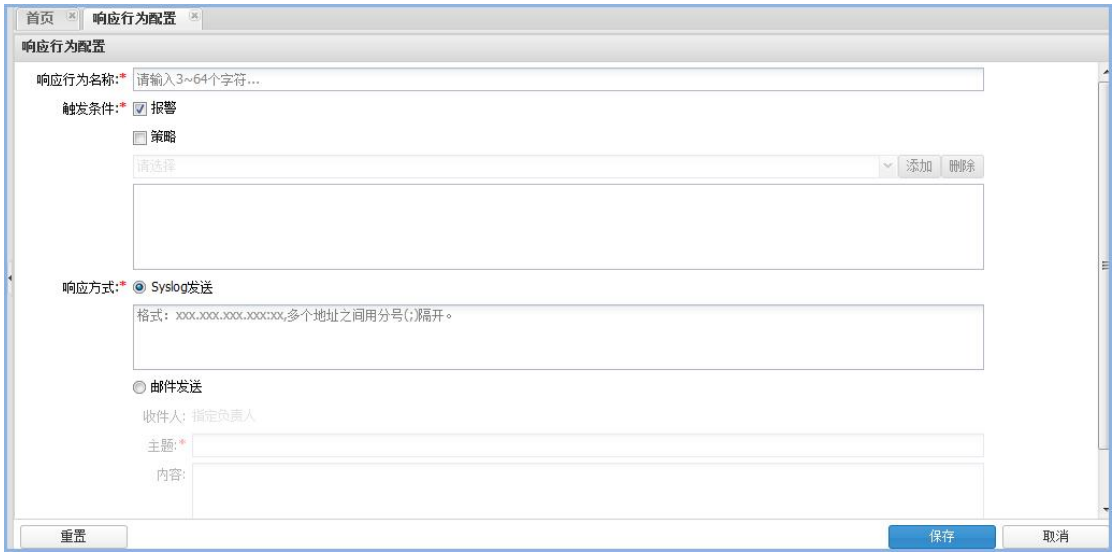


图 9-14

响应行为名称：此项为必填项，用户需输入 3-64 位字符，字符类型不限制。

触发条件：此项为必填项，默认勾选报警、策略默认不勾选，置灰状态显示。用户可选择性勾选“报警”和“策略”，也可同时勾选两项。当用户勾选“策略”时，可点击下拉框选择策略名称并点击**“添加”**按钮，若您想删除已添加的策略，您可在框中选中想要删除的策略名称，点击**“删除”**按钮，选中的策略被删除。此处删除功能不支持全部删除。如图所示：

图 9-15

响应方式：此项为必填项，默认勾选“syslog 发送”，“邮件发送”默认不勾选，置灰状态显示，用户可选择性勾选“syslog 发送”和“邮件发送”，也可同时勾

选两项。如图所示：

图-16

A：“syslog 发送”：输入格式：xxx.xxx.xxx.xxx:xxx,多个地址之间用（;）号隔开。

B:“邮件发送”：收件人为指定负责人，有属于该负责人的资产时 ，产生报警或者命中策略后。会直接发送到该资产指定的相应负责人邮箱。

注：规定时间内：（报警信息响应时间系统默认设置为：高危级别报警 24 小时、中危级别报警 48 小时）未被及时响应的报警信息会进行二次外发，自动发送至日志审计系统的系统管理员邮箱（sysadmin 中编辑添加邮箱）。系统管理员会在相应的时间收到属于所有负责人资产和无责任人的所有未处理的报警信息。

响应频率：默认显示“5 分钟”，点击下拉按钮，时间可选。

9.3.2 响应行为配置界面功能

响应行为配置界面为用户提供添加新响应行为在界面中展示，并可执行编辑、删除、应用操作。如图所示：

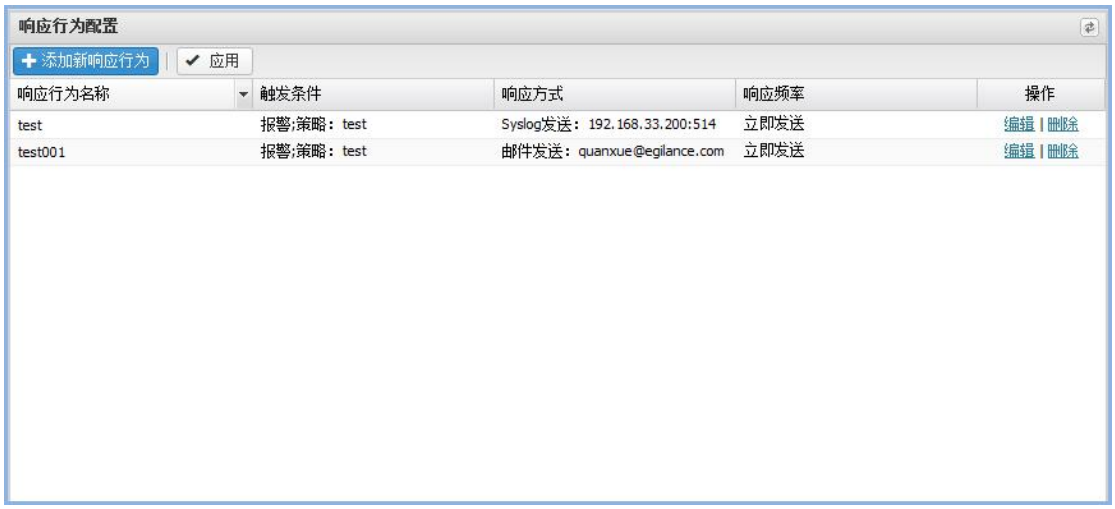


图 9-17

编辑：用户点击“编辑”按钮，界面跳转到响应行为的编辑界面（同添加新响应行为界面），用户可更改响应的内容。

删除：用户选择一条响应行为，点击“删除”按钮，选择的响应行为被成功删除。

应用：用户响应行为添加成功后，点击“应用”按钮，使所有的响应行为生效。

刷新图标：用户可以点击界面右侧上端的刷新图标，刷新当前界面。

10. 报表中心

系统为用户提供报表模版，使用各种方式统计审计数据，方便用户查看。

10.1 报表预览管理

以拥有 “报表预览管理” 功能权限的用户登录系统，鼠标点击 “报表中心->报表预览管理”，进入报表预览管理界面，如图所示：

图 10-1

根据用户实际需要，系统内置 8 类不同的报表模板，分别是资产信息分析、资产运行概况分析、事件类型分析（事件大类）、报警分析、脆弱性分析，等级保护，采集源分析，具体事件分析。

用户可以根据系统内置的报表模板预览报表、下载报表、设为常用报表等。

10.1.1 预览报表

报表分类中选中某个报表模版，输入需要的参数条件，点击 预览报表 按钮，界面会加载出该报表信息，如图所示：

图 10-2

预览完成后，点击“刷新”按钮，报表分类中多出一类“最近预览”，查看此分类下的报表，可以看到最近预览过的所有报表。

注：各种报表模板的参数主要有以下几种

- 起始时间：报表统计数据的开始时间，默认为昨天的 00:00:00；
- 结束时间：报表统计数据的结束时间，默认为昨天的 23:59:59；
- 资产：报表统计的指定资产 ip 地址；
- 事件类型：报表统计的指定事件类型

报表分类中，点击“全部展开”，各文件夹下所有报表模版展开显示，点击“全部折叠”，各报表模版恢复收起状态。

10.1.2 下载报表

报表加载完成后，可以点击 DOCX XLSX PPTX PDF 按钮，进行下载报表，如图 8-3 所示：

图 10-3

输入报表名称（注：为空时，将默认为原始报表名称），点击“确定”按钮，界面提示“要打开或保存来自 x.x.x.x 的 xx.docx 吗”,选择“另存为”，弹出另存为窗口，如图 8-4 所示：

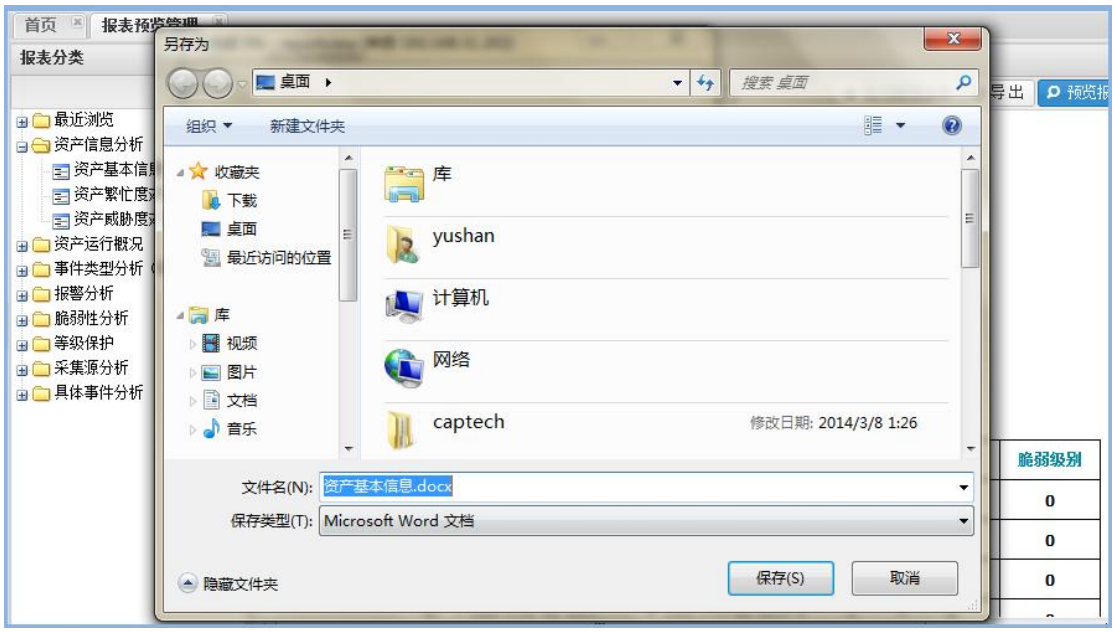


图 10-4

指定存储路径，点击“保存”按钮，下载完成。

注：下载报表支持的文本格式有 docx、xlsx、pptx 及 pdf。

10.1.3 设为常用报表

报表加载完成后，可以点击 设为常用报表 按钮，将此报表设为常用报表，如图 8-5 所示：

图 10-5

点击“确定”按钮，点击“刷新”按钮，报表分类中多出一类“常用报表”，查看此分类下的报表，可以看到该报表，设为常用报表成功。

图 10-6

10.2 报表模板管理

报表模板管理向用户提供定期自动发送报表邮件的功能

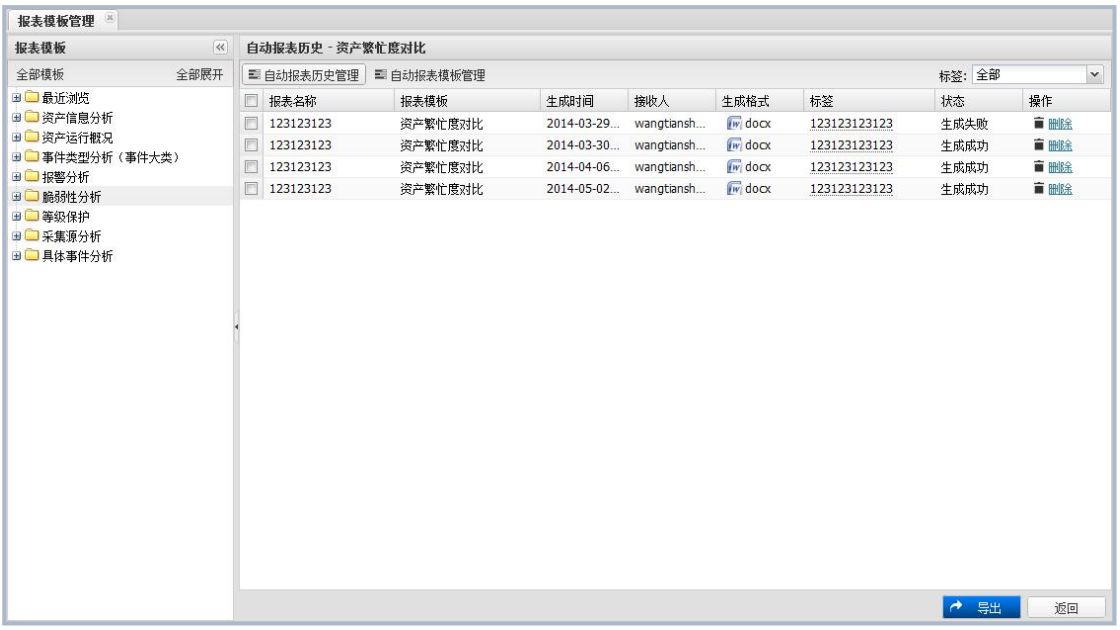
其中左侧展示的是系统中所有的报表模板，可以点击全部展开、全部折叠来查看报表模板

右侧分为自动报表历史管理与自动报表模板管理两项：

10.2.1 自动报表历史管理

点击自动报表历史管理标签打开对应界面

自动报表历史管理可以查看设备自动生成的全部自动报表，点击左侧全部模板可以查看所有模板生成的历史报表，选取自动报表模板只展示由当前报表模板生成的对应历史报表，如图所示：



图：10-7

用户可以对已经生成的报表进行导出或删除操作

10.2.2 自动报表模板管理

点击自动报表模板管理标签打开对应界面

自动报表模板管理可以设置使用指定报表模板进行定时报表任务，并且可以针对已经生成的报表任务进行管理。如图所示：

图 10-8

在左侧选取对应的报表模板后点击右下方添加报表按钮即可添加自动报表任务（注意不是所有报表模板都支持自动报表任务功能）如图所示：

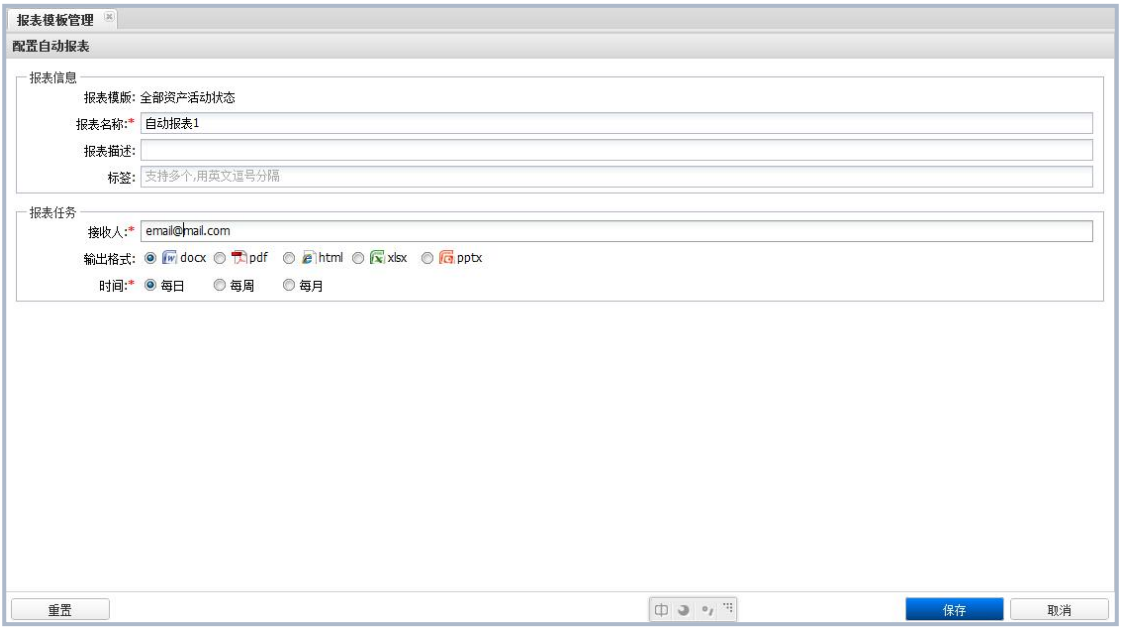


图 10-9

其中报表名称为必填项，且唯一，报表描述可以选填针对此报表自动任务的描述，标签支持在针对自动报表历史管理界面与自动报表模板管理界面内展示项

的筛选

在接收人项中填写报表邮件对应接收人的邮箱，可支持多个，在配置此项功能前需要保证在系统管理->工作参数->SMTP 邮件服务器中的配置正确可用。

输出格式为报表的文件格式，系统将会把报表文件作为附件的形式发送到对用收件箱

时间项为报表发送周期，

1 每日：

报表数据的统计范围为 1 天内的所有数据，该报表会在第二天 0 时（当天 24 时）进行统计并发送到指定邮箱

2 每周：

报表数据的统计范围为周日到周六，共七天的数据，该报表会在第二周的周日 0 时（当周的周六 24 时）进行统计并发送到指定邮箱

3 每月：

报表数据的统计范围为本月一日到下月一日的数据，该报表会在第二月的二日 0 时（第二月的一日 24 时）进行统计并发送到指定邮箱

配置完毕后点击保存即可使配置生效，点击重置按钮会清空已经填写的信息

针对已经配置完毕的自动报表任务还可对其进行编辑和删除操作，编辑后保存该自动任务会重新生效

11. 系统管理

11.1 工作参数

工作参数配置包括 SNMP 服务器，DNS 服务器，时间设置，用户安全性配置，磁盘预警，数据处理的配置。

11.1.1 SMTP 服务器

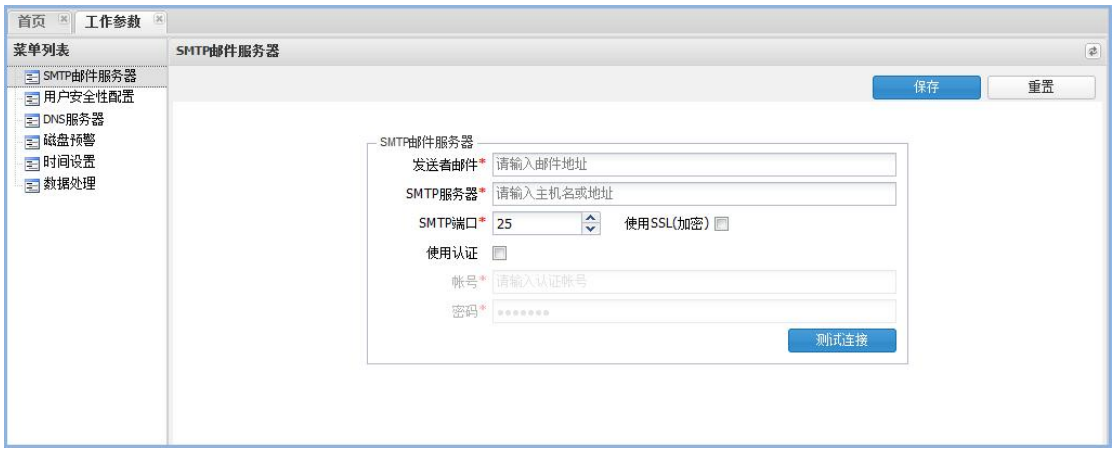


图 11-1

SMTP 服务器的基本信息包括发送者邮件（必填），SMTP 服务器，SMTP 端口（是否认证）。

发送者昵称：发送者的名称；**发送者邮件**：邮件地址（正确的邮件格式）；**SMTP 服务器**：即邮件服务器（IP 地址或域名格式）；**SMTP 端口**：邮件传输端口；**认证信息**：发送者的信息认证。

11.1.2 DNS 服务器

图 11-2

DNS 服务器：包括主服务器，和两个备用服务器（正确服务器的格式）。

11.1.3 时间设置

图 11-3

时间设置：可以手动设置时间，也可以同步 NTP 服务器时间（NTP 服务器或主机 IP 地址）。

11.1.4 用户安全性配置

图 11-4

用户安全性配置：连续登录失败次数（默认为 5），系统锁定时间（默认为 5），帐号密码长度（最小 8 位，最大 32 位），页面超时时间（默认 10 分钟）。

连续登录失败：连续登录失败达到设定次数，对系统进行锁定。

系统锁定时间：系统锁定，用户将不能登录系统（超出锁定时间才可以）。

帐号密码长度：用于限制新建用户密码长度和更改用户密码长度。

页面超时：设定时间内，对系统无操作，系统将自动退到登录界面。

11.1.5 磁盘预警

图 11-5

磁盘预警：对磁盘的使用率一种限制，包括预警阀值，邮件告警，保护阀值，处理方式。

预警阀值：设置磁盘的预警阀值（50%<预警阀值<89%）

保护阀值：设置磁盘的保护阀值（51%<保护阀值<98%）

邮件告警：磁盘到达预警阀值会自动发送邮件提醒（SNMP 服务器测试通过的邮件服务器地址）。

处理方式：覆盖或停止记录。覆盖：在磁盘容量达到预警阀值以后，系统自动覆盖磁盘中最早一天的数据记录，可能导致部分日期的数据记录丢失。停止记录： 在磁盘容量达到预警阀值以后，系统自动停止工作并且不再向磁盘写入新的数据。

11.1.6 数据处理

图 11-6

数据处理：设置数据保留天数（默认 30 天）。超出保存天数的数据会自动删除。

11.2 采集配置

采集配置：定义日志采集的来源和采集的事件类型。

全局配置：包括采集服务的开启和关闭，和相关软件的下载（主要对 windows 日志采集的采集的 agent 插件）。(注：每次更改采集服务的开启和关闭，需要应用成功后，才能生效)

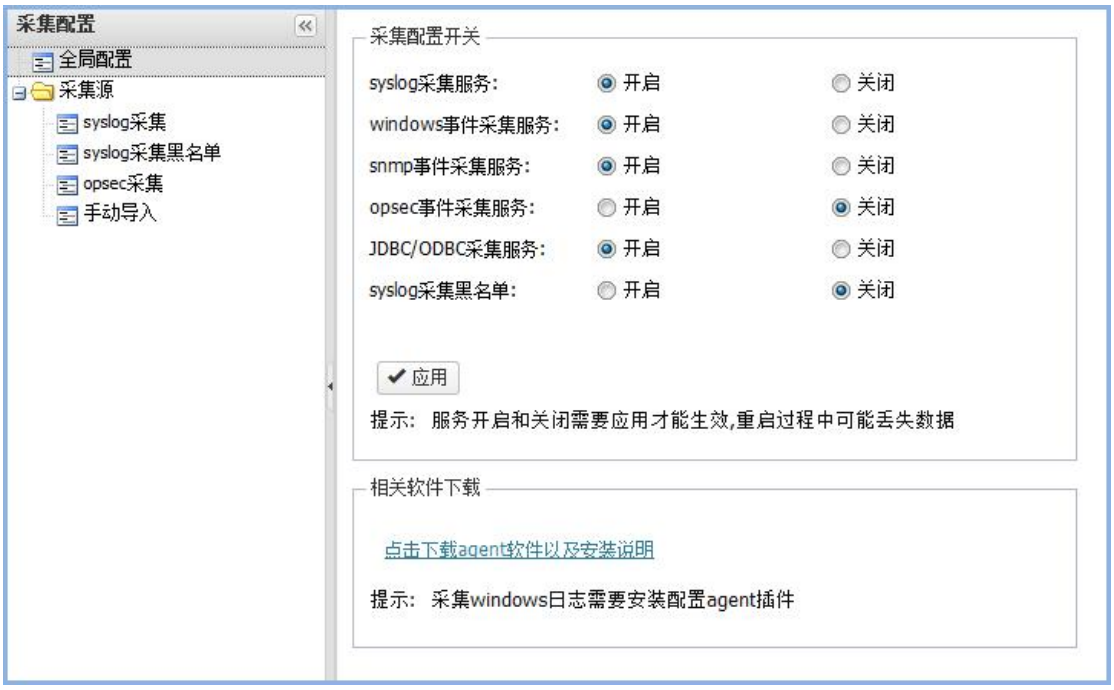


图 11-7

采集源：包括 syslog 采集源、syslog 采集黑名单和 opsec 采集源的配置

1. syslog 采集源的配置

图 11-8

Syslog 采集界面支持新增采集源配置，导入和导出。(每次添加新的采集源，需要应用成功后才能生效)

（1） 添加新采集源

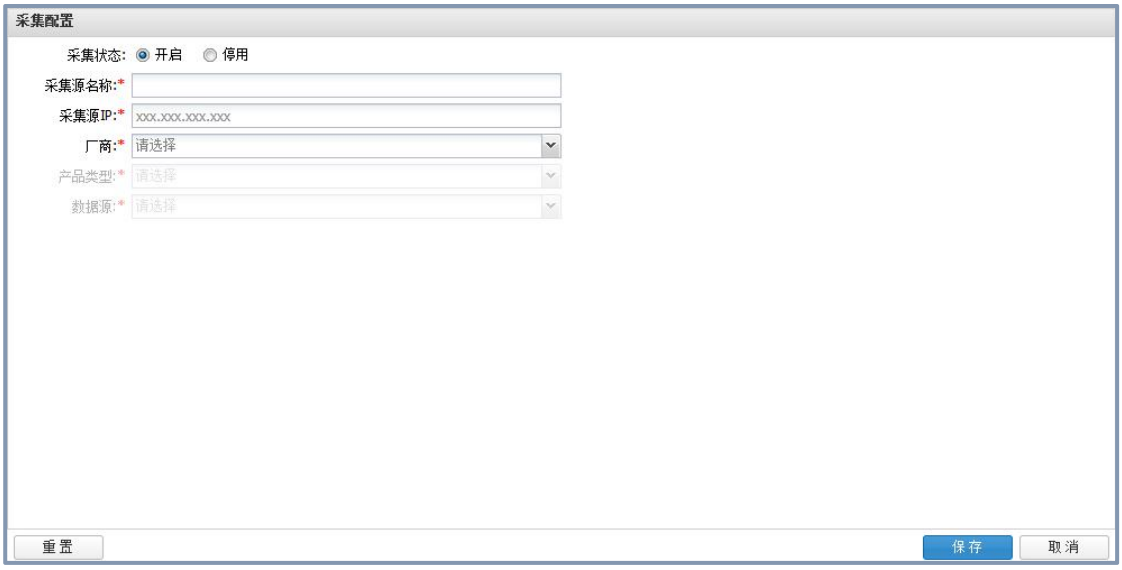


图 11-9

采集状态：开启、停用两种方式

采集源名称：用户自定义采集源的名称（必填）

采集源 IP：必填项可依据匹配上述采集信息选择 IP 地址，如格式：192.168.101.1（必填）

厂商：必填项点击下拉文本框，可依据匹配上述采集信息选择厂商名，如图

所示：(图 9.2.1.2)

图 11-10

产品类型：点击下拉文本框，可依据厂商（例如 Cisco）匹配上述采集信息选择产品类型，如图所示：

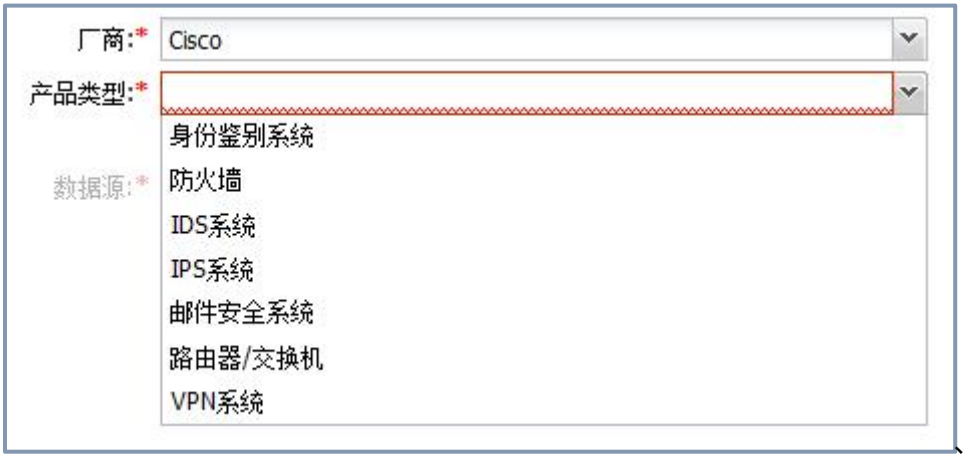


图 11-11

数据源：点击下提文本框，可依据匹配上述采集信息（例如厂商：Cisco，产品

类型：路由器/交换机）选择数据源，如图所示

图 11-12

（2）编辑采集配置

系统管理员在界面中选择要修改的采集配置，点击**“编辑”**按钮，可以在弹出框中更改采集状态，修改采集名称以及采集源配置。如图：

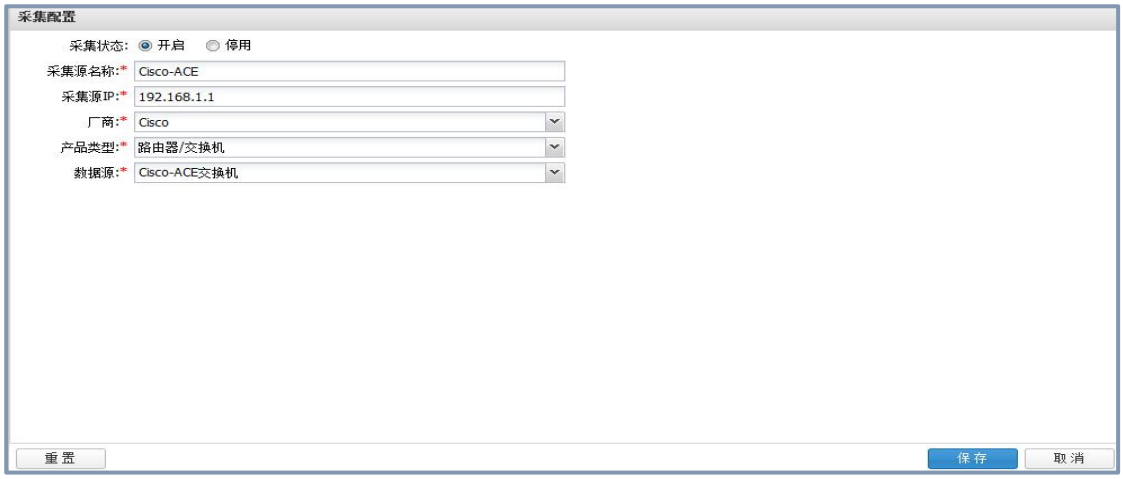


图 11-13

注：可以对采集状态、采集源名称、采集源 IP、厂商、产品类型、数据源进行修改，点击保存。如果对此信息不修改点击**“取消”**按钮。

系统管理员选中要删除的采集配置，点击**“删除”**按钮，如果确认要删除，则点击**“确定”**；否则，则点击**“取消”**即可。如图所示

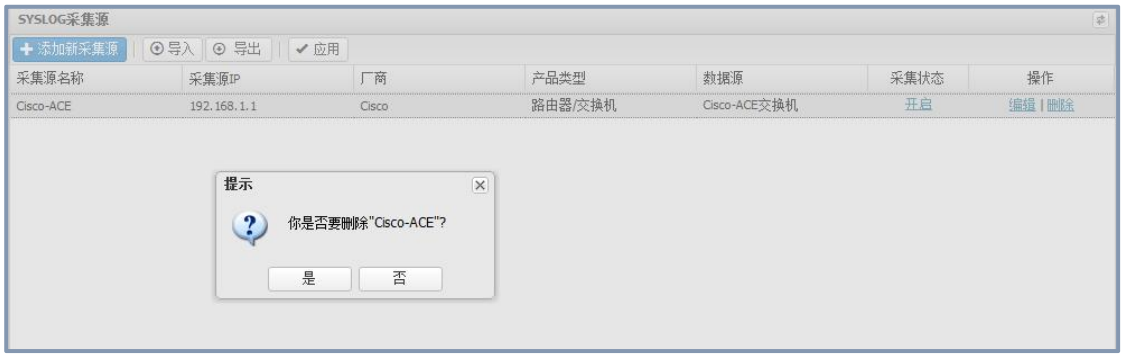


图 11-14

syslog 采集黑名单：

点击“添加采集黑名单”按钮，输入采集源 IP，点击保存。点击应用（注：采集黑名单配置完成后，需要注意全局配置采集黑名单服务开启状态）才能生效。

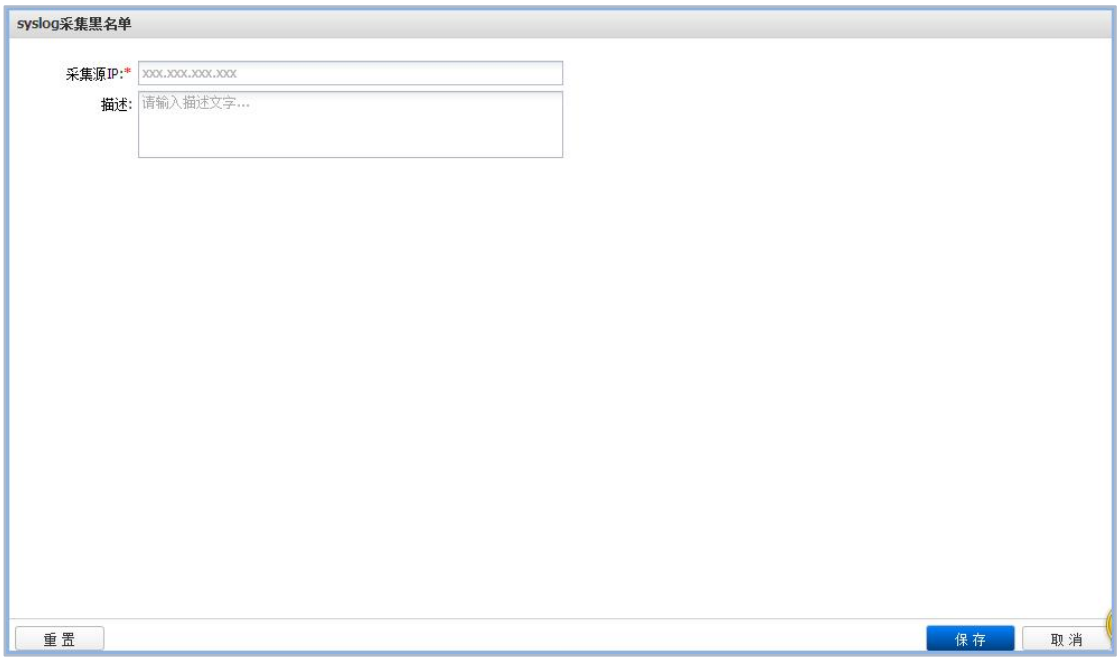


图 11-15

采集黑名单操作：

可以对采集黑名单进行编辑或删除操作（应用后生效）。

OPSEC 采集配置：

Opsec 采集配置和 syslog 采集配置略有不同。如图

图 11-16

点击“添加新采集源”，进到采集配置界面，如图

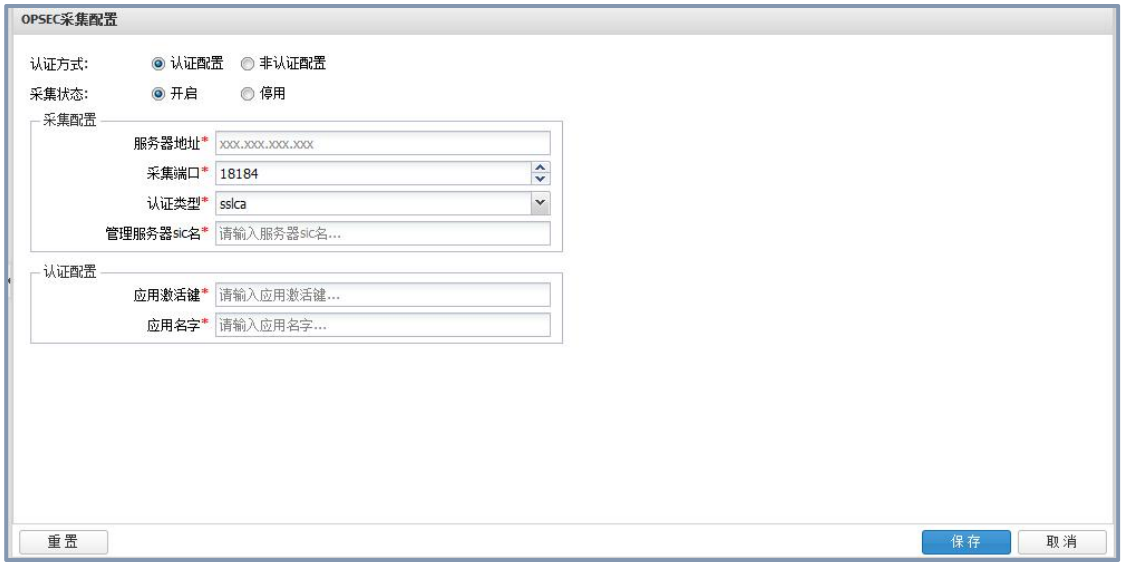


图 11-17

注：opsec 采集源的配置包括认证配置和非认证的配置两种模式（要求服务器端的配置也是不一样的）。

1. 认证模式配置：

需要配置服务器地址，采集端口，认证类型，管理服务器 sic 名称，应用名字，和激活键。配置完成后，点击“保存”按钮，提示认证成功后才能

获取设备日志。

2. 非认证模式配置：

图 11-18

非认证模式配置较简单，只需要配置服务器地址，采集端口和选择认证类型。配置完成后，点击“保存”按钮，保存成功就可以了。

Opsec 采集源配置完成后的界面显示，如图

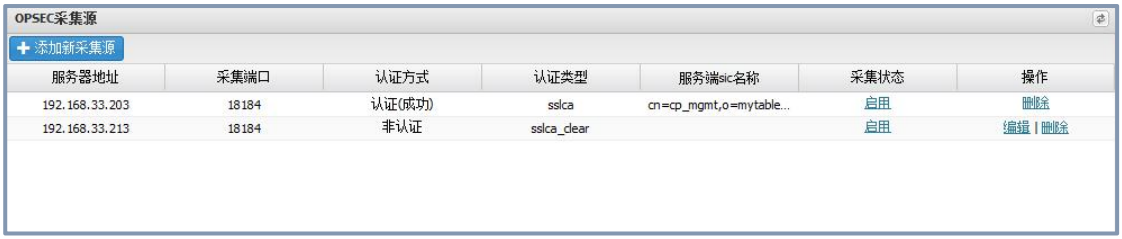


图 11-19

说明：认证模式配置成功后不可以再次编辑；同一服务器地址，认证模式和非认证模式只可以配置一次。

手动导入

图 11-20

说明：日志类型可以按默认和自定义两种类型导入相应的日志。

A：按默认类型导入，点击导入，选择日志格式（*.log），确认导入。

B：自定义类型导入，匹配相应的厂商、产品类型、数据源，选择日志格式（*.log），确认导入。

11.3 数据备份

数据备份向用户提供备份历史数据以及对已备份数据进行还原的功能，支持备份的数据包括：报警事件、审计事件、配置相关三种，用户可以设置自动备份或手动备份，以天为单位对以上三种数据进行选择性备份，并且支持对备份数据的还原，其界面如图所示：

图 11-21

11.3.1 备份配置

用户可在备份配置界面设置 安全磁盘空间、自动备份设置、FTP 文件备份配置的参数。点击备份配置按钮即可打开备份配置界面，配置完成后点击保存即可保存当前设置并即时生效，点击取消将放弃已输入的配置并返回数据备份界面。其界面如图所示：

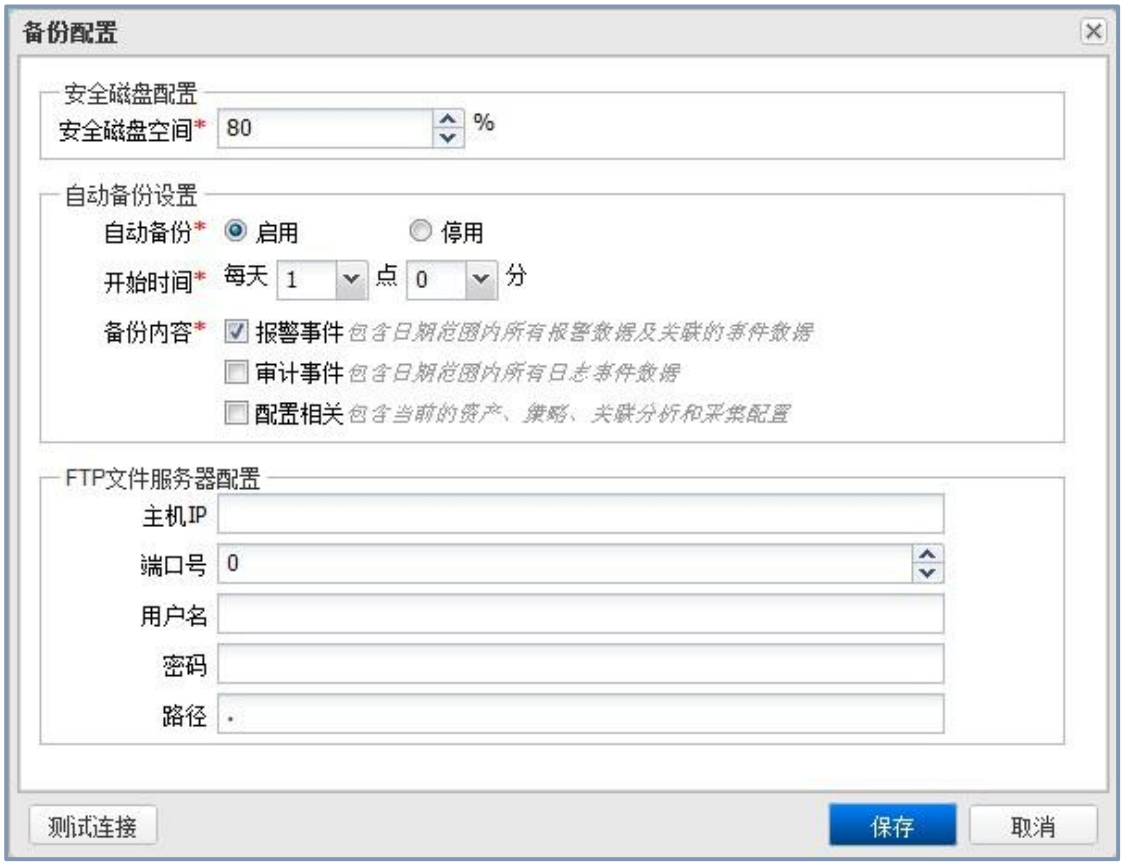


图 11-22

11.3.1.1 安全磁盘配置

用户可设置安全磁盘空间的值，当设备磁盘空间占用率超过设置的值，系统将不会再允许转储以及还原的功能的执行，直到设备磁盘占用率低于设置的值。该设置适用于自动备份与手动备份。

安全磁盘空间默认值为 80%，其设置有效值的上限为 80%。

如果磁盘空间超过设置的值导致备份失败系统会向系统管理->工作参数->磁盘预警中邮件告警的邮箱发送备份失败的通知邮件

进行设置之后点击保存生效。

11.3.1.2 自动备份设置

自动设置提供每天定时自动备份前一天数据的功能，自动备份设置的参数包括自动备份功能的启用与停用，和每日定时备份的时间（精确到分钟）以及需要备份的数据内容的类型进行设置之后点击保存生效。

11.3.1.3 FTP 文件服务器配置

系统支持将备份的内容上传到用户提供的 ftp 服务器，用户需要设置 FTP 服务器的 IP 地址以及 ftp 服务的工作端口（通常情况下 ftp 工作端口为 21），除此之外还需要用户提供一套拥有该 FTP 服务上传、下载权限的账号，以及存放备份文件的路径。

当设置完 FTP 服务器参数后，可以使用系统提供的测试连接功能对目标 FTP 服务器进行连接测试，点击测试连接按钮即可，如图所示：

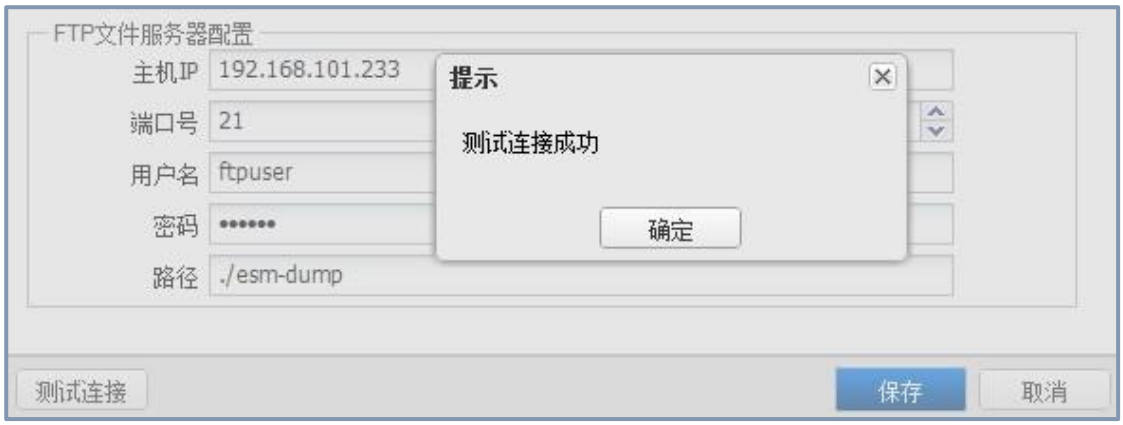


图 11-23

注意！如果设置了正确的 ftp 服务器，已经备份的文件将不会在设备本地磁盘内保存，此时如果修改 FTP 服务器配置可能会造成系统无法找到对应的备份文件导致还原失败

11.3.2 手动备份

除设置自动备份每天自动备份前一天的数据之外，用户还可以通过手动备份备份当天之前（不含当天）任意一天或一段时间内的数据，点击手动备份按钮将打开手动备份界面，如图所示：

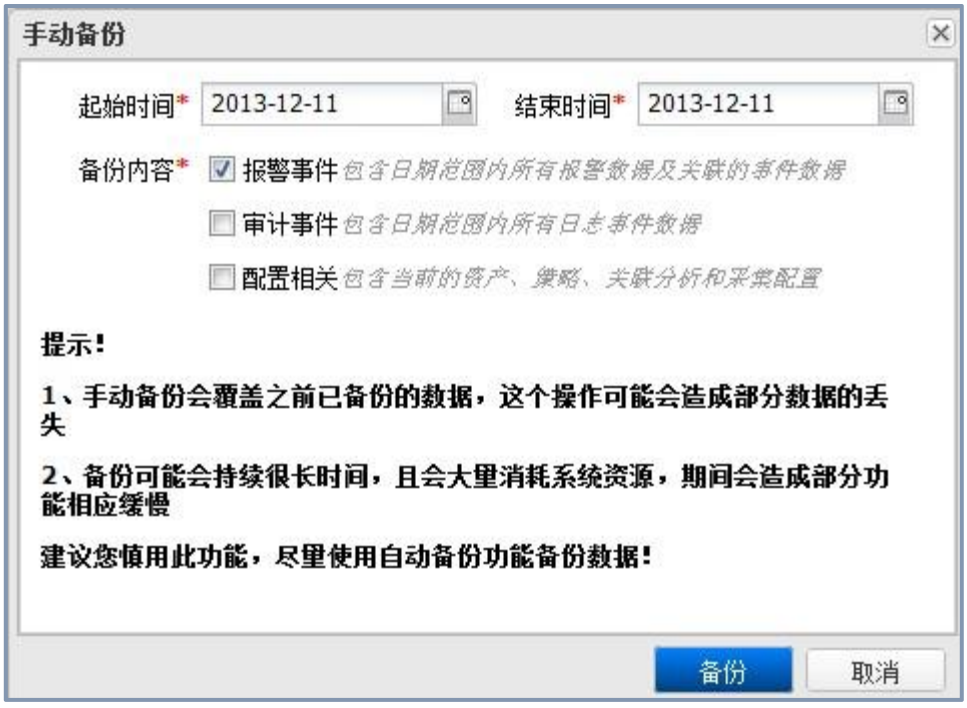


图 11-24

用户可以自定义日期间隔以及备份内容对历史数据进行备份，如果对已经存在备份数据进行再次备份，新的备份数据将会覆盖原备份数据。

注意!备份与还原任务可以同时执行，但不能在同一时间内执行多个备份以及还原操作。

11.3.3 对备份内容的操作

当执行备份任务时系统会在下方备份内容列表类展示备份的进度，相同在还原任务执行时也会展示还原的进度，用户可以对正在备份以及还原的任务执行取消备份操作。如图所示：

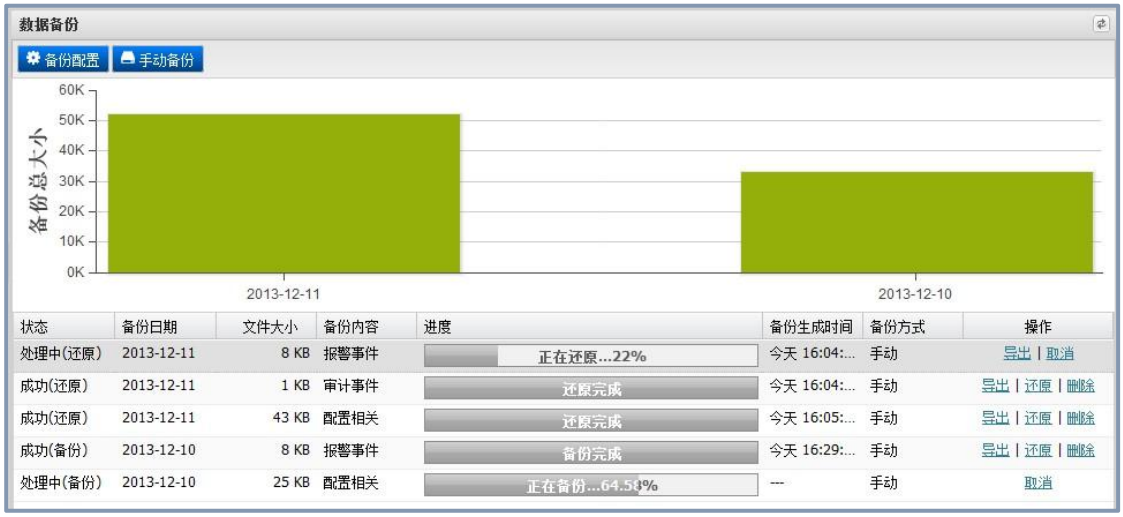


图 11-25

除了在下方展示已经或正在执行的转储数据以外，系统还会在上方备份总大小图表内使用柱状图展示每天备份文件的大小。

已经完成的备份任务支持导出、还原以及删除等操作。

用户可以对已经备份的数据进行还原，还原后的报警、审计事件可以在相关查询界面进行查询，还原配置相关的数据会替换已有的配置信息并且立刻生效，配置相关的数据包括资产管理以及策略管理内所有的配置，请谨慎使用配置相关数据的还原功能。

将过早的备份数据导出后删除可以节省系统或 FTP 服务器的硬盘空间。

11.4 补丁管理

点击**“系统管理->补丁管理”**进入补丁管理界面，如图

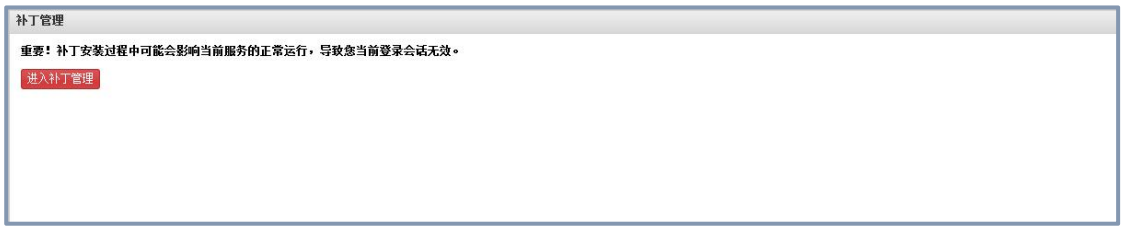


图 11-26

点击“进入补丁管理”按钮，会跳转到另一个界面进行补丁安装，如图

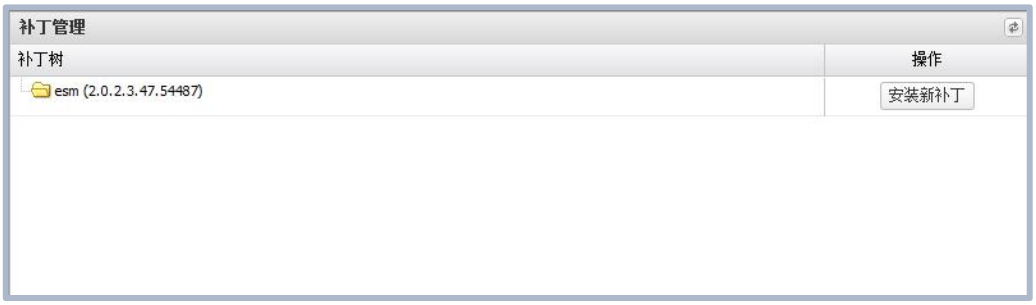


图 11-27

点击“安装新补丁”按钮，选择补丁文件存放的路径，点击“安装”按钮，确认进行补丁安装。补丁安装完成后的界面显示，如图

图 11-28

说明：补丁安装成功后，是不可以卸载的。

11.5 角色管理

sysadmin 登录，进入系统角色界面，如图所示：（图 9.4.1）

图 11-29

用户管理中包括角色管理和对用户的权限分配。系统管理员可以给新建的角色分配不同的权限

11.5.1 添加角色

系统管理员可以通过点击“**添加**”按钮添加角色，在弹出框中选择要授予角色的权限，点击保存后角色添加成功，弹出框如图所示：（图 9.4.2）

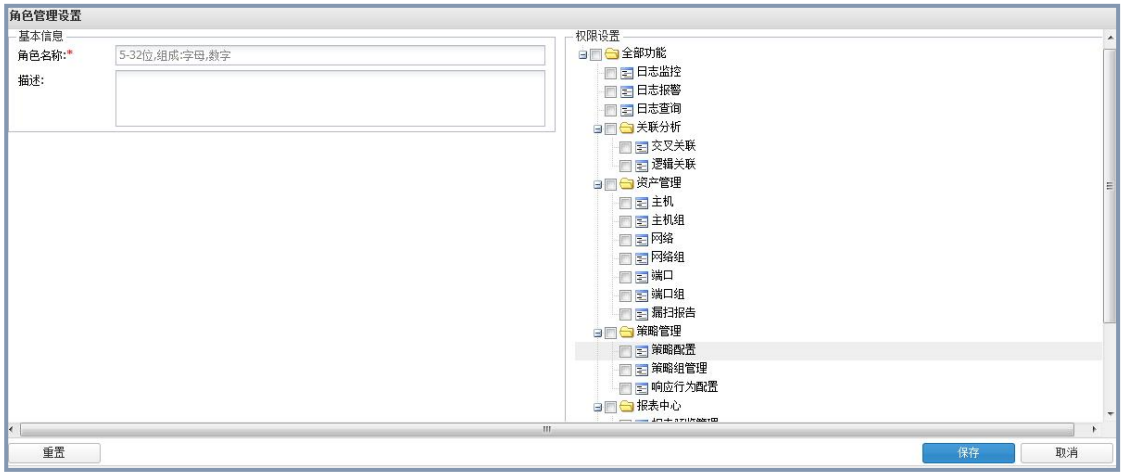


图 11-30

1、 **角色名称**：必填项，5-32 位，组成：字母，数字等。

2、 **描述**：可以对相应帐户进行详细描述。

3、 **用户权限**：分为全部功能：（1）日志监控、日志报警、日志查询（2）关联分析：交叉关联、逻辑关联（3）资产管理：主机、主机组、网络、网络组、端口、端口组以及漏扫报告（4）策略管理：策略配置、策略组配置、响应行为配置 （5）报表中心：报表预览管理 （6）:工作参数、采集配置、数据备份、补丁管理。选择分配某一个、多个或全部的权限。

4、 点击“**保存**”，系统用户即可添加成功。点击“取消”该用户不存在切换角色管理界面。

11.5.2 角色权限

用户管理中包括角色管理和对用户的权限分配。系统管理员可以给新建的角色分配不同的权限。

11.5.3 编辑角色权限

系统管理员在界面中选择要修改的角色，点击“编辑”按钮，系统管理员可以在弹出框中修改角色名称以及角色权限。如图所示：(图 9.4.3)

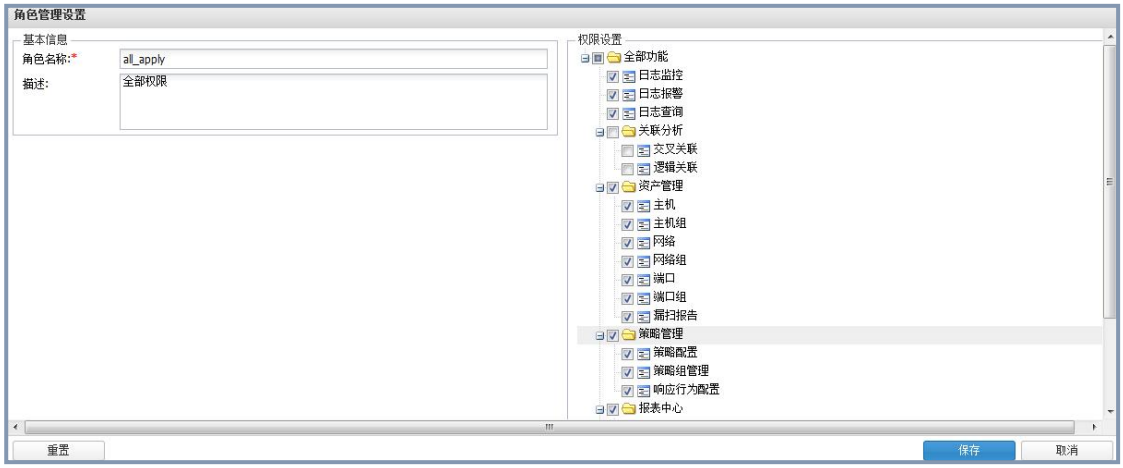


图 11-31

注：可以对角色名称、描述、权限分配进行修改，如图修改角色权限取消选择“关联分析”后，点击保存。如果对此角色不修改点击“取消”按钮。

11.5.4 重置角色权限

系统管理员选中要重置角色的权限，点击“重置”按钮，权限分配将恢复保存前的状态。如添加角色勾选某一个或全部权限选项，点击“重置”按钮。

11.5.5 删除角色

系统管理员选中要删除的角色，点击“删除”按钮，如果确认要删除，则点击“确定”；否则，则点击“取消”即可。如图所示：

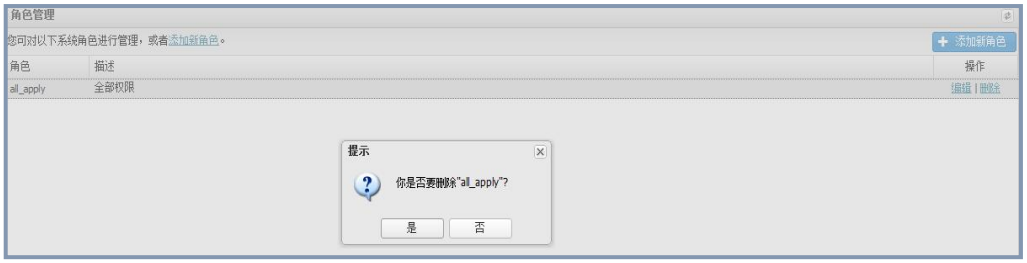


图 11-32

11.6 授权管理

授权管理：显示授权文件的基本信息，支持重新授权和授权文件备份。

如图：

图 11-33

点击“授权”按钮，选择授权文件重新授权。

点击“备份授权文件”按钮，选择授权文件存放路径，备份完成。

12 知识库管理

知识库管理针对泛化不同类型日志对应的泛化插件进行查看以及管理，可以在界面内设置需要加载的相关泛化插件，并且可以对泛化插件库进行升级，使其支持更多类型的数据源。如图所示：

图 12-1

点击每列对应的标题可以对该列进行排序

勾选每项插件对应的复选框可以设置该插件是否加载（注意！加载插件数量过多会导致系统处理性能降低。）设置完加载插件后点击应用按钮即可是当前设置生效，应用后需要等待系统设置生效。 如图所示：

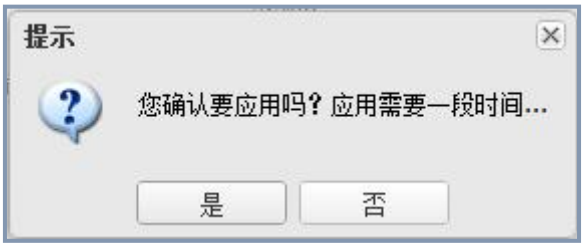


图 12-2

点击“**导入**”按钮可以将知识库对应升级包(esm-kbupgrade*.bin，其中*代表知识库版本号)导入进行安装升级，安装后点击右侧查看历史可以查看所有已安装升级包的历史版本，已经安装的升级包不允许再次安装，如图所示：

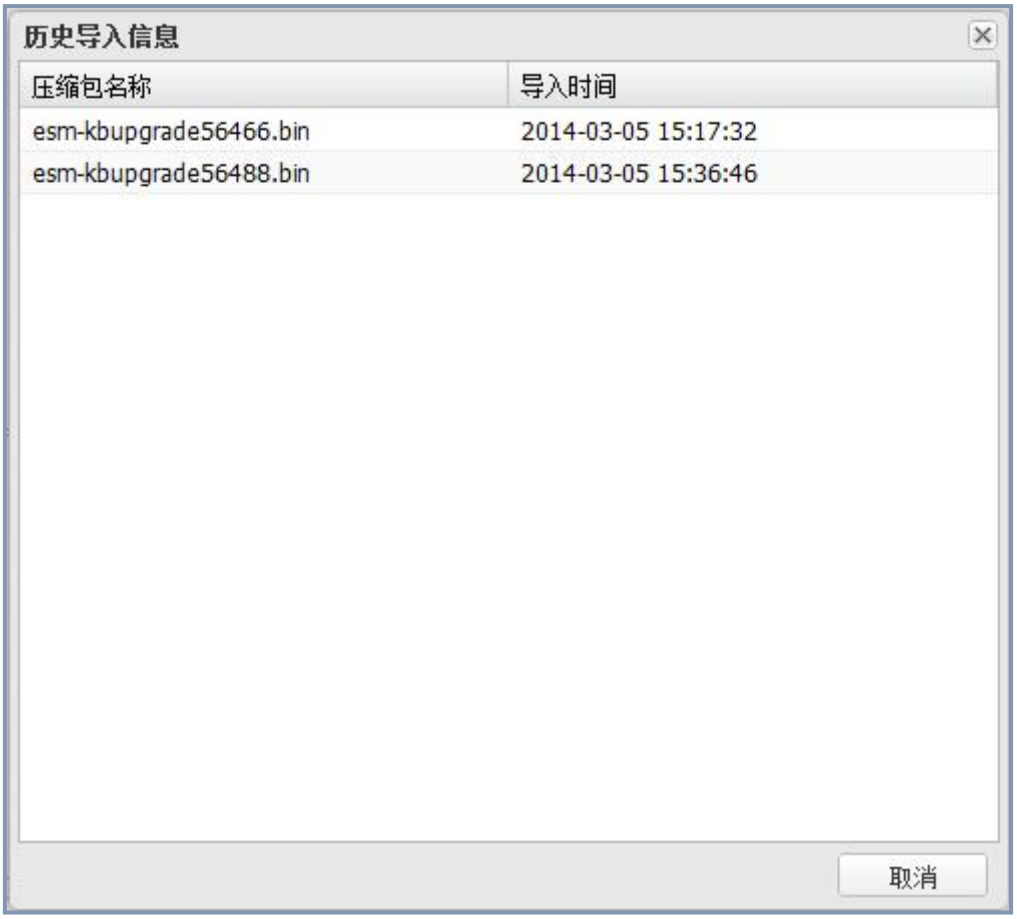


图 12-3

13 工单管理

工单管理针对对象： 报警

工单的处理流程：根据报警详细内容触发生成工单---》工单接收人处理---》关闭工单--》关闭报警，新编辑过的工单会置顶显示

13.1 报警审计界面——工单的添加

用户需根据报警详细内容触发生成工单，双击打开某一条报警信息，点击右侧顶部**“添加工单”**按钮，弹出工单添加界面，如图所示：

图 13-1

包含元素：

标题：用于说明该工单的工作内容，默认为报警事件名称。

接收人：工单发送目标，系统内注册的管理员。用户只能看到自己被分配的工单，并且只有处理和关闭功能，不可编辑

优先级：工单处理优先级 1-10 1-3：低 4-6：中 7-10：高

工单类型：异常事件、系统/应用报错事件、企业网攻击事件、病毒传播事件、通用事件、策略违规事件、安全漏洞事件（ossim 中的 具体带定）

源 IP：默认为报警事件源 IP

目的 IP：默认为报警事件目的 IP

源端口：默认为报警事件源端口

目的端口：默认为报警事件目的端口

工单描述：对该工单的描述

注：创建者：发起工单的管理员，可以编辑，处理，关闭工单的操作。创建时间：工单生成时间

用户需要输入工单信息中包含的必填项，输入框后面有下拉框的可在框中选择，其中 IP 与资产负责人是对应关系，更改 IP，负责人会随着更改。点击**“重置”**按钮，可对用户添加的信息清空，点击**“保存”**按钮，弹出提示框，工单信息添加成功。点击**“取消”**按钮，该条工单信息被取消。

13.2 工单管理界面——工单查询

工单的查询条件有三个：工单类型、优先级、处理状态。输入查询条件后，点击**“重置”**按钮，输入的查询条件被清空，通过三个条件的筛选，点击**“查询”**按钮，可查询出对应条件的工单信息。如图所示：

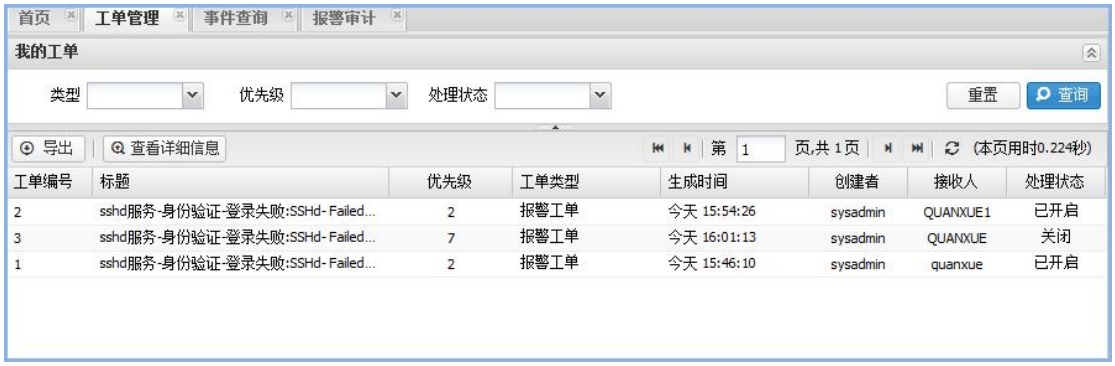


图 13-2

点击**“查看详细信息”**按钮，可查看该条工单的详细信息

点击**“导出”**按钮，工单被导出

点击**“关闭”**按钮，选中的工单被导出

13.3 工单管理界面——工单编辑

点击工单**“编辑”**按钮，打开工单编辑界面，包含元素意义与工单添加界面一致。如图所示：

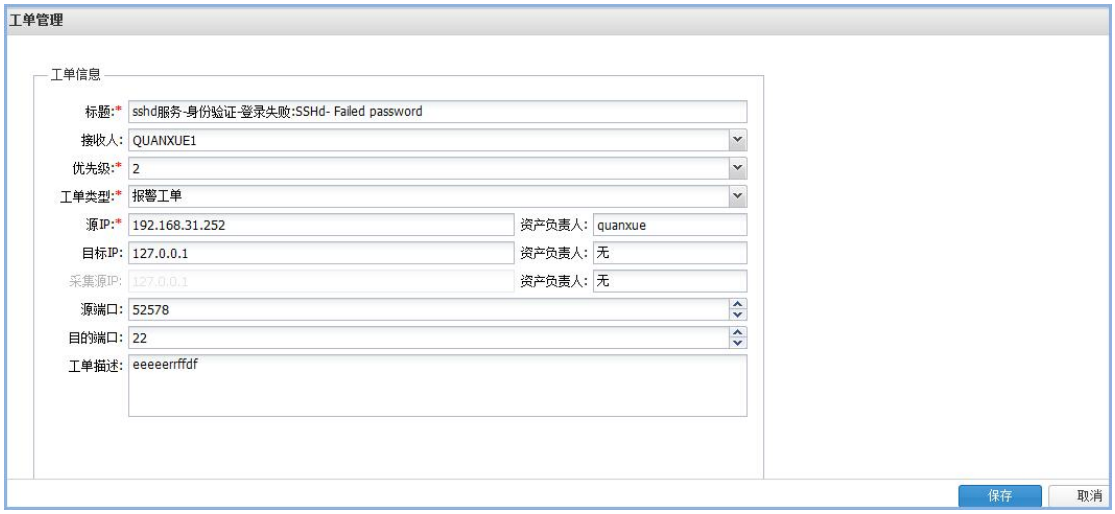


图 13-3

13.4 工单管理界面——工单处理

点击工单“**处理**”按钮，打开工单处理界面，如图所示：

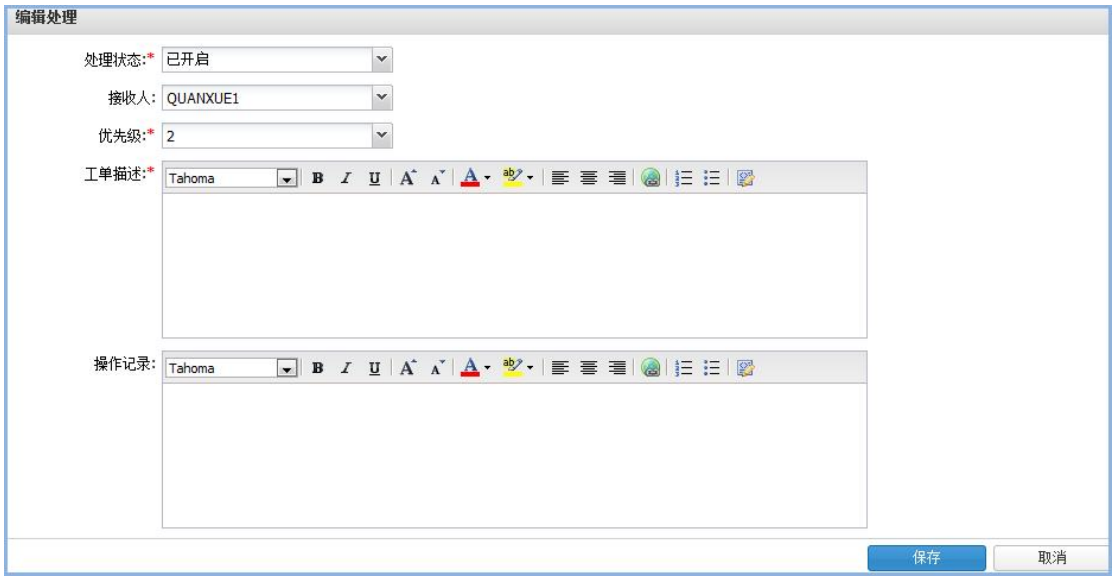


图 13-4

包含元素与编辑界面一致，其中处理状态：已开启、已接收、正在分析、正在处理、正在测试、关闭。点击保存后，选择工单，点击查看详细信息按钮。会显示该条工单信息的处理历史，包含元素：

操作人：XXX

操作时间：XX-XX-XX

优先级：工单处理优先级 1-10　1-3：低 4-6：中 7-10：高 ，与工单绑定

处理状态：　与工单绑定

转发至：　目的负责人，与工单绑定

操作记录描述：记录对该工单的分析及说明

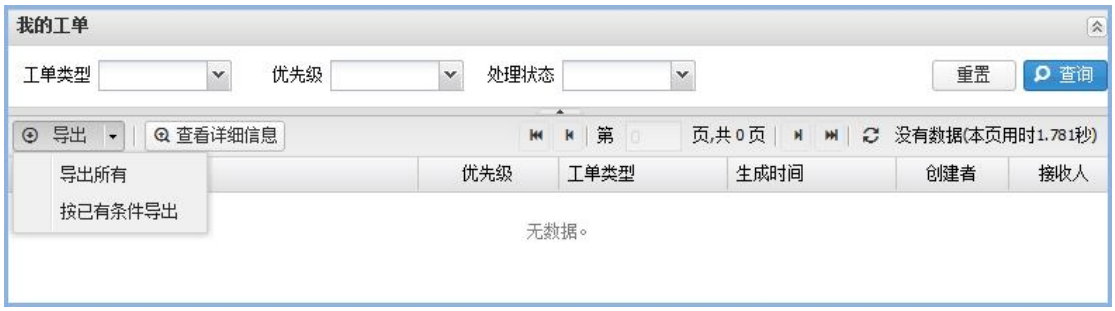
操作记录执行内容：记录操作、处理工作流程

附件：上传必要的证据，记录等，可下载

删除：该条处理操作被删除

13.5 工单管理界面——工单导出和关闭

工单管理界面点击“导出下拉”按钮，如图所示：



图：13-5

内容包含 1：导出所有，2：按已选条件导出，导出内容以 Excel 形式展示，用户选择导出所有，界面会弹出提示框并会导出全部工单信息。如图所示：

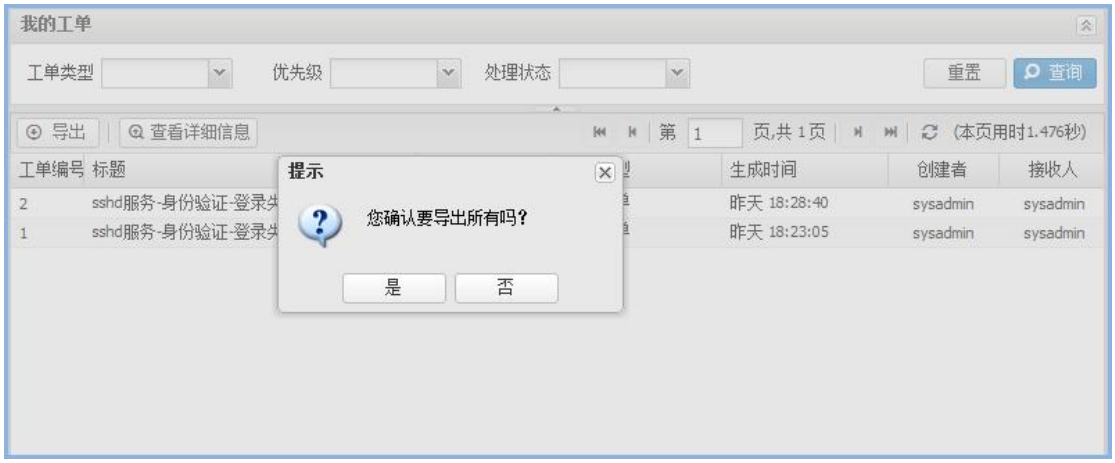


图 13-5

用户选择按现有条件导出，界面会弹出提示框并会导出已选工单信息内容。如图所示：

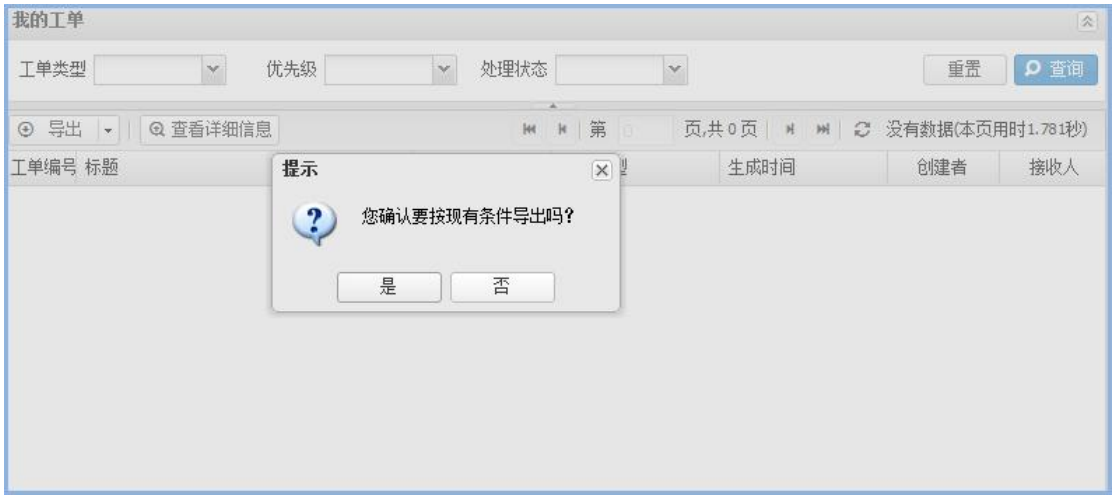


图 13-6

工单管理界面点击“关闭”按钮，选中的工单被关闭，该条工单只能被查看详细信息功能。

14　我的参数

以系统管理员 sysadmin/useradmin/auditadmin 登录系统后，点击用户名右侧顶端“我的参数  ”图标，系统会弹出我的参数信息框，个人参数包括用户名全名、电子邮箱、密码三项。如图所示：

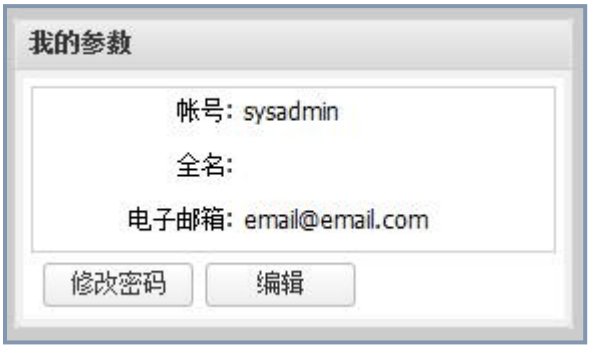


图 14-1

14.1 帐号编辑

我的参数弹出框，点击**“编辑”**按钮，**“全名”“电子邮箱”**显示可输入状态，输入自定义全名及电子邮箱。

全名：输入系统用户的名称，默认的全名是 sysadmin/useradmin/auditadmin。注：与登录时的用户名不同。当输入“全名”后，点击保存，待弹出保存成功提示后，再次登录系统即生效，保存了的名称将显示在门户菜单中。点击取消，则取消当前操作。电子邮箱：输入电子邮箱地址，点击保存，待弹出保存成功提示后，保存成功。点击取消，则取消当前操作如图所示：

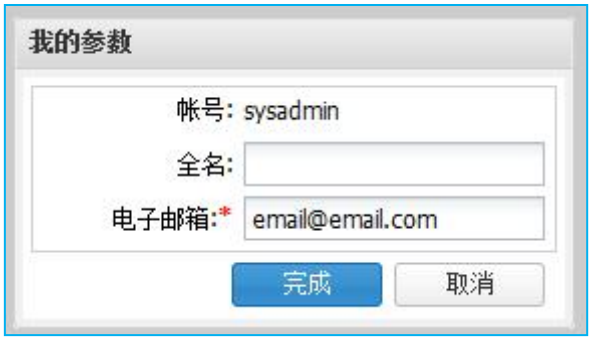


图 14-2

14.2 修改密码

我的参数弹出框，点击**“修改密码”**按钮。密码修改： 若要修改密码，密码长度 8-32 位，并且密码必须包含字母、数字和特殊字符。例如：abc@1234。输入新密码后，点击**“保存”**按钮，待弹出保存成功提示后，保存成功。点击取消，则取消当前操作。如图所示：

图 14-3

输入当前密码和两次新密码一致，点击**“完成”**按钮即可。

14.3 退出系统

如果您想退出日志审计系统，用户参数弹出框点击**“注销”**按钮，系统会给您弹出退出提示框。如图：

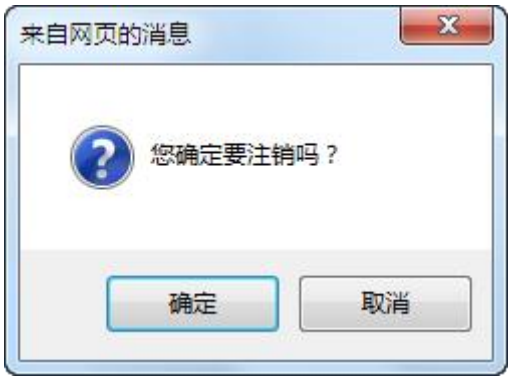


图 14-4

点击**“确定”**则退出日志审计系统，点击**“取消”**按钮，则注销操作被取消。

15 自身审计系统

使用 auditadmin 密码:auditadmin@1234 登录自身审计系统。“自身审计系统”主要记录了用户在系统下的所有操作行为的时间、类型、级别、内容及用户的结果，包括以下几种（如图 11-1 所示）：

图 15-1

15.1 日志类型

15.1.1 系统日志查询

条件类别分别为：级别、状态、日志类型、用户名、内容五种。

级别：点击**“下拉”**按钮，选择查询条件级别，如图所示：

图 15-2

状态：点击**“下拉”**按钮，选择查询条件状态，如图所示：

图 15-3

日志类型：点击**“下拉”**按钮，选择查询条件日志类型，如图所示：

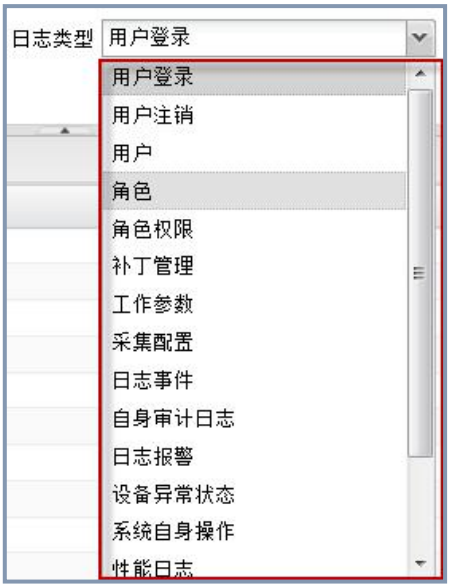


图 15-4

用户名：直接在文本框输入关键字做为添加查询条件的用户名，如图所示：

图 15-5

内容：直接在文本框输入包含的关键字做为添加查询条件内容，如图所示：

图 15-6

同一查询条件可复选，也可将不同查询条件进行组合，如图所示：

图 15-7

点击  按钮，可以快速将所有查询条件清空。

15.1.2 查询时间段设置

点击 可以选择日期，点击 时间: 15 13 0 可以选择时间刻度。

用户可以根据实际情况选择开始时间和结束时间，默认时间间隔为 30 分钟。

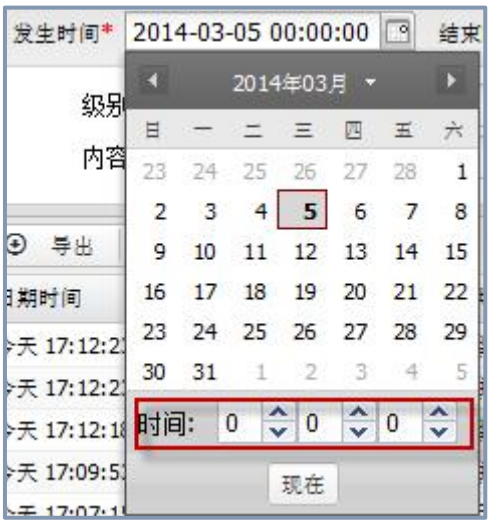


图 15-8

15.1.3 快速选项

快速选项即查询时间的快速设置，此选项优先于开始时间和结束时间设置。

快速选项中包括：最近五分钟、最近半小时、当天、最近 24 小时、最近一周、最近一个月等 6 种选项可供选择。

15.1.4 查询指定日志

查询条件设置完成后，点击右上角的**“查询”**按钮即可查询日志审计信息，如图所示：

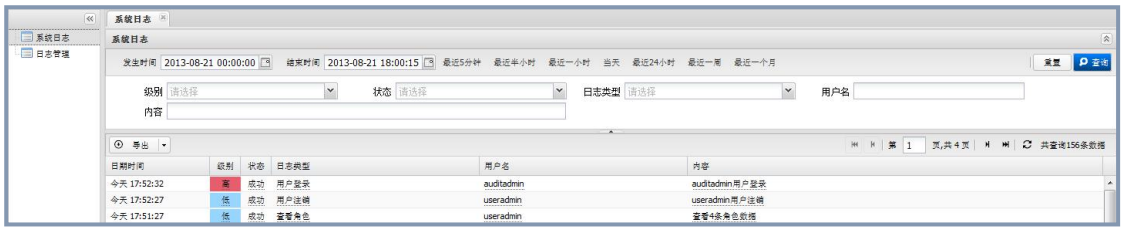


图 15-9

15.2 导出日志

首先查询所要导出的系统日志，然后点击界面左下角的**“导出”**按钮，系统会弹出导出设置对话框，如图所示：

图 15-10

注：此功能是将当前所查询到的所有系统日志导出。

导出格式分为三种：

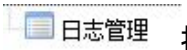
1、 word 格式

2、 html 格式

3、 csv 格式

选中想要导出的文件格式，点击**“导出”、“保存”**即可。

15.3 删除系统日志

如果想要删除系统日志，在主菜单点击 

按钮，切换日志管理界面，再点击 

按钮，系统会弹出确认提示窗口，如图所示：

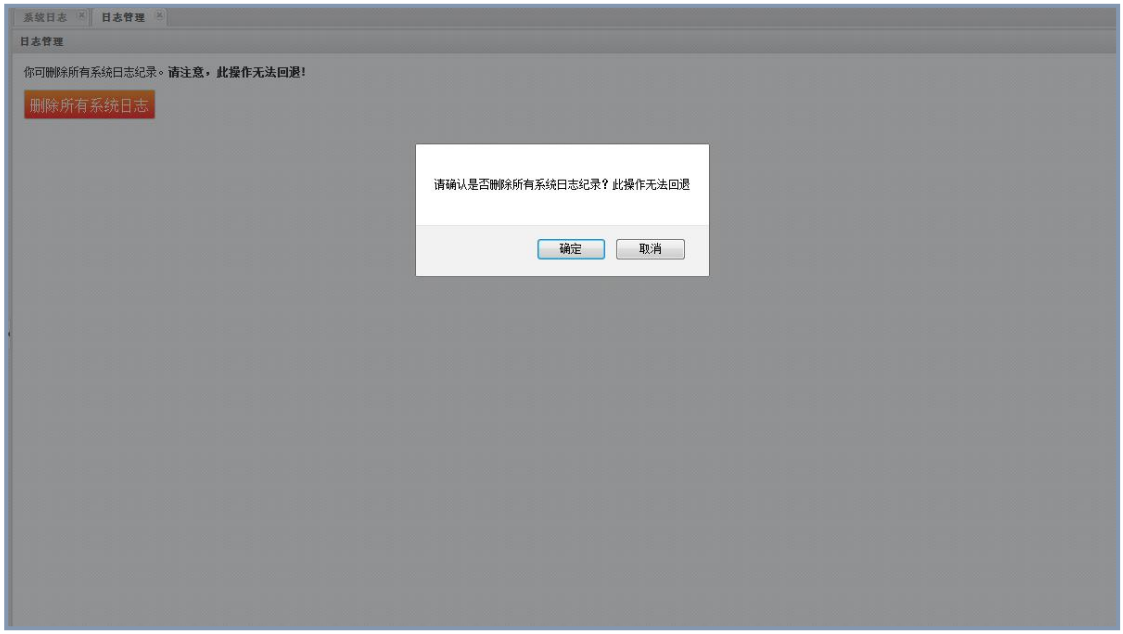


图 15-11

如果真要删除，则点击**“确定”**；否则，则点击**“取消”**即可。

注：此功能是删除所有的系统日志，删除后不可恢复，请慎重做此操作。