

东软 NetEye 统一身份管理系统 （NABH）

BS 审计使用手册

Neusoft

沈阳东软系统集成工程有限公司

2014 年 8 月

版权声明

本手册中涉及的任何文字叙述、文档格式、插图、照片、方法、过程等所有内容的版权属于沈阳东软系统集成工程有限公司所有。未经沈阳东软系统集成工程有限公司许可，不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。本手册中的信息受中国知识产权法和国际公约保护。

版权所有，翻版必究©

目 录

1	前言	1
1.1	文档目的	1
1.2	读者对象	1
1.3	使用环境	1
1.4	工作要求	1
2	审计管理模块	3
2.1	系统监控	3
2.1.1	网络信息	4
2.1.2	活动会话	4
2.1.3	设备状态	5
2.2	会话审计	6
2.2.1	会话查询	6
2.3	会话统计	18
2.4	告警审计	22
2.4.1	告警查询	22
2.4.2	告警查询配置	24
2.5	事件审计	25
2.5.1	事件查询	25
2.5.2	事件查询配置	26
2.6	报表审计	27
2.6.1	日常报表	28
2.6.2	创建会话报表	29
2.6.3	创建运维操作报表	31
2.6.4	创建帐户分配报表	32
2.6.5	创建事件报表	34
2.6.6	创建告警报表	35
2.6.7	创建审计员操作报表	36
2.6.8	创建全局统计报表	37

2.6.9	创建会话统计报表.....	39
2.6.10	设备日常维护统计报表.....	41
2.7	审计配置.....	43
2.7.1	条件管理.....	43
2.7.2	定时报表.....	46

1 前言

1.1 文档目的

本文档为沈阳东软系统集成工程有限公司的东软 NetEye 统一身份管理系统的 B/S 审计使用手册。通过阅读本文档，读者能够正确地使用东软 NetEye 统一身份管理系统的审计功能，运用审计功能来强化现有的安全管理制度，规范安全管理流程，达到运维安全审计的目的。

1.2 读者对象

本文档适用于 3.7（E、P、S）版本。

1.3 使用环境

NABH 的审计员使用 WEB 登录方式作为用户界面。可以使用 Microsoft Internet Explore 或以其为内核的其他浏览器，因部分控件的兼容问题，如果您使用的是 IE 8 浏览器，请在兼容模式下进行运行。

1.4 工作要求

因审计中涉及到日志回放功能，需要做以下设置：

1. 网络环境：防火墙上需开放 NABH 到客户端的全部端口，如有 NAT 地址转换，会话回放则不能使用。
2. 是否开启 **Windows 防火墙**，如开启，可将 1816 端口开放，或关闭防火墙，S 版回放的服务使用了此端口；
2. 检查 IE 菜单栏-》工具-》管理加载项中，将“**SecureClient Control**”控件启用，如果是 IE7，
- 8，检查是否在可信任站点运行，注：可信任站点安全级别支持默认中级。 见附图。



2 审计管理模块

审计管理模块包括系统监控、会话审计、告警审计、事件审计、报表审计、审计配置六个功能模块。



2.1 系统监控

系统监控主要监控系统的基本信息，包括网络信息、活动会话和设备状态。



2.1.1 网络信息

网络信息页面如上图所示：

IP 信息：显示 IP 数据包的各种信息；

TCP 信息：显示 TCP 数据包的各种信息；

UDP 信息：显示 UDP 数据包的各种信息。

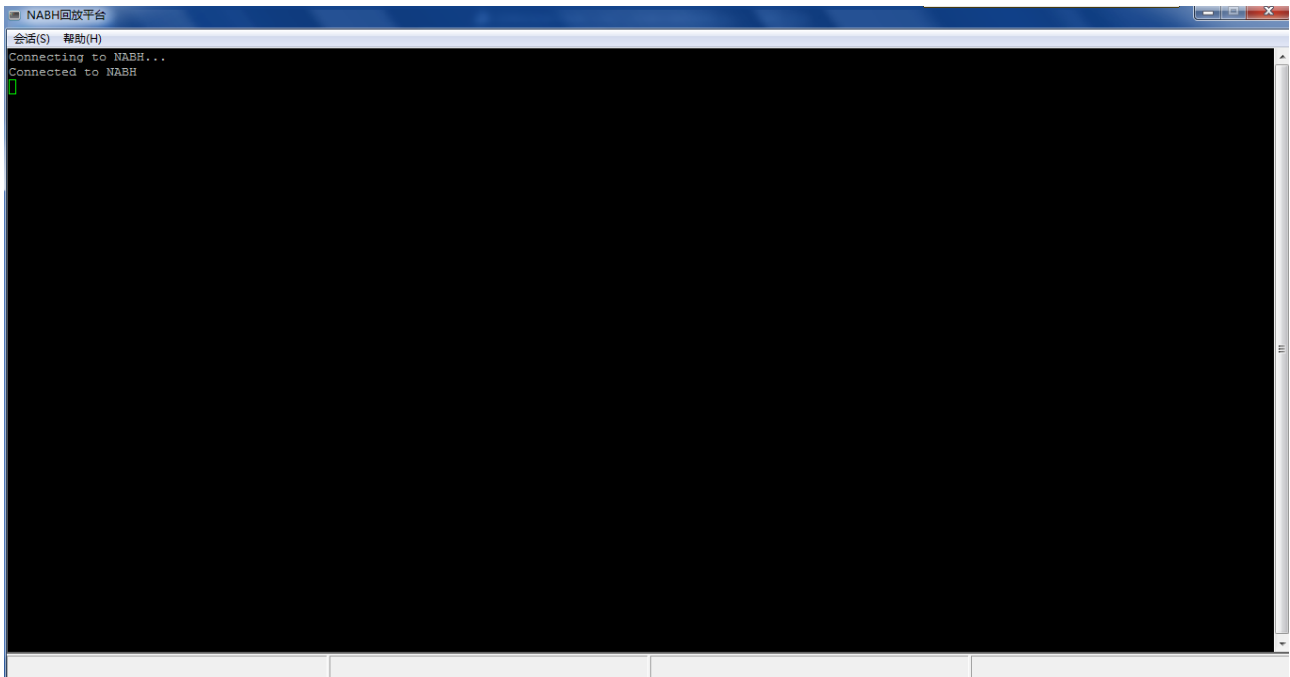
2.1.2 活动会话

显示当前正在进行的会话。包括用户名、客户 IP、设备名、协议、设备 IP、开始时间、设备帐户名等信息。



可根据查询条件进行快速查询。通过“刷新”按钮来查看当前活动会话信息。

选中某个会话后，点击右侧操作栏中的【监控】按钮，可对当前的这个会话进行实时监控。



审计员可通过右侧操作栏中的【中止】按钮，强行终止当前正在进行的会话。

2.1.3 设备状态

显示当前所有设备的活动状态。主要显示设备的设备名、设备 IP、协议、并发数量、端口信息。

设备名	设备IP	协议	并发数量	主机端口	操作
10.10.1.130	10.10.1.130	xwin	0	7000	详细会话
10.10.1.130	10.10.1.130	ssh	0	22	详细会话
10.10.1.130	10.10.1.130	vnc	0	5902	详细会话
10.10.1.130	10.10.1.130	ftp	0	21	详细会话
10.10.1.130	10.10.1.130	sftp	0	22	详细会话
10.10.1.130	10.10.1.130	telnet	0	23	详细会话
10.10.1.254	10.10.1.254	telnet	0	23	详细会话
172.16.1.124	172.16.1.124	vnc	0	5900	详细会话
172.16.1.124	172.16.1.124	https	0	443	详细会话
172.16.1.124	172.16.1.124	ssh	0	22	详细会话

可根据查询条件进行快速查询。点击操作栏中的【详细会话】按钮，可查看该设备对应

协议当前正在进行的会话。



2.2 会话审计

会话审计主要功能是对会话日志进行管理。包括“会话查询”和“会话统计”，可对会话日志的查询，并根据统计条件产生图形和表格两种格式统计报表。

2.2.1 会话查询

会话查询默认显示当天所有的运维操作记录。

通过查看会话查询，可以审计出每条会话的用户名、客户 IP、设备名、协议、设备 IP、开始时间、结束时间、设备帐户名、日志大小等信息。支持按照时间快速查询。

- 在会话审计中，如果某一会话被审计过，则在状态栏里使用符号  标识。
- 在会话审计中，如果某一条会话审计为合规，则在合规栏里使用  标识，若为不

合规则用  标识。

- 如果某一会话中存在命令告警，则使用其他颜色将该会话标识。其中，如果存在阻断告警，则使用红色标识；

hacuser	172.16.1.204	10.10.1.23...	telnet	10.10.1.23	2013-06-0...	2013-06-0...	root	1.571K	回放 下载 详情
---------	--------------	---------------	--------	------------	--------------	--------------	------	--------	--

- 如果存在非阻断告警，则使用橙色标识。

hacuser	172.16.1.204	10.10.1.29...	ssh	10.10.1.29	2013-06-0...	2013-06-0...	root	1.38K	回放 下载 详情
---------	--------------	---------------	-----	------------	--------------	--------------	------	-------	--

在每条会话日志上点击右侧操作栏中的按钮，可实现会话回放、下载、查看详细信息功能。

2.2.1.1 会话详细信息

对任意一条会话日志，通过点击右侧操作栏中的【详情】按钮，可查看这条日志的概要信息、详细信息并可进行审核批注、查看告警、查看审计操作。在每一个标签中均可进行该条会话的事后回放和下载操作。

概要信息：记录此日志的基本信息，包括运维状态和审计状态；



The screenshot shows a web interface for audit management. At the top, there are navigation tabs: 系统首页, 系统管理, 运维管理, 口令管理, 审计管理 (selected), and 运维操作. Below the tabs is a breadcrumb: 审计管理 > 会话审计 > 概要信息. There are five sub-tabs: 概要信息 (selected), 详细信息, 审核批注, 查看告警, and 查看审计. Below the sub-tabs are buttons for 回放 and 下载. The main content area is divided into two sections: 运维状态 and 审计状态.

运维状态							
会话ID:	B40E2C4C59FEA2D6	用户名:	111	设备帐号:	root	设备名:	10.10.1.130
协议名:	telnet	客户IP:	172.16.1.125	设备IP:	10.10.1.130	命令告警状态:	阻断
开始时间:	2014-09-09 06:23:08	结束时间:	2014-09-09 06:24:57	复核人:	linzh		

审计状态			
是否审计:	已审计	合规性:	未设置
批注:			

At the bottom of the interface, there are buttons for 返回, 上一条, and 下一条.

详细信息：记录此日志的详细信息，主要是记录该会话中的每一条命令和命令的回显。

审计管理 > 会话审计 > 详细信息

概要信息 **详细信息** 审核批注 查看告警 查看审计

回放 下载 查找 保存 打印 单页 展开 信息编码: GBK 信息类别: 上下行记录信息

NABH运维会话日志记录表

用户名:	111	设备名:	10.10.1.130	客户IP:	172.16.1.125	设备IP:	10.10.1.130
开始时间:	2014-09-09 06:23:08	结束时间:	2014-09-09 06:24:57	设备帐户:	root	操作命令:	共12条

```

login: root (2014-09-09 06:23:30)
+ Password: (2014-09-09 06:23:36)
+ [root@localhost ~]# ls (2014-09-09 06:23:39)
[root@localhost ~]# (2014-09-09 06:23:49)
[root@localhost ~]# (2014-09-09 06:23:57)
+ [root@localhost ~]# pwd (2014-09-09 06:23:57)
[root@localhost ~]# cd /tmp/ (2014-09-09 06:24:00)
+ [root@localhost tmp]# ls (2014-09-09 06:24:04)
[root@localhost tmp]# cd /mnt/ (2014-09-09 06:24:08)
+ [root@localhost mnt]# ls (2014-09-09 06:24:13)
    
```

查看时间: 2014-09-09 审计员签字:

【查找】按钮，可从当前信息中查找关键内容，并标黄显示。

【保存】【打印】按钮可保存、打印该详细信息。

【单页】按钮，可将详细信息单页或分页显示。

【展开】按钮，可展现或收起该命令的回显内容。

◇ 对于文件传输协议会话查看详细信息，详细信息中包含：键盘记录信息和上下行记录信息，界面如下：

查看键盘记录信息：

- 记录所有的键盘操作，对于所有的特殊字符都保持原样记录；
- 键盘记录作为上行数据进行检索；

审计管理 > 会话审计 > 详细信息

概要信息 **详细信息** 审核批注 查看告警 查看审计

回放 下载 查找 保存 打印 单页 展开 信息编码: GBK 信息类别: 键盘记录信息

NABH运维会话日志记录表

用户名:	111	设备名:	10.10.1.130	客户IP:	172.16.1.125	设备IP:	10.10.1.130
开始时间:	2014-09-09 06:23:08	结束时间:	2014-09-09 06:24:57	设备帐户:	root	操作命令:	共9条

```

***** (2014-09-09 06:23:36)
ls (2014-09-09 06:23:39)
l pwd (2014-09-09 06:23:57)
cd /tm (2014-09-09 06:24:00)
ls (2014-09-09 06:24:04)
cd /mn (2014-09-09 06:24:08)
ls (2014-09-09 06:24:13)
ls (2014-09-09 06:24:16)
exit (2014-09-09 06:24:28)
    
```

查看上下行记录信息:

审计管理 > 会话审计 > 详细信息

概要信息 **详细信息** 审核批注 查看告警 查看审计

回放 下载 查找 保存 打印 单页 展开 信息编码: GBK 信息类别: 上下行记录信息

NABH运维会话日志记录表

用户名:	111	设备名:	10.10.1.130	客户IP:	172.16.1.125	设备IP:	10.10.1.130
开始时间:	2014-09-09 06:23:08	结束时间:	2014-09-09 06:24:57	设备帐户:	root	操作命令:	共12条

```

login: root (2014-09-09 06:23:30)
+ Password: (2014-09-09 06:23:36)
+ [root@localhost ~]# ls (2014-09-09 06:23:39)
[root@localhost ~]# (2014-09-09 06:23:49)
[root@localhost ~]# (2014-09-09 06:23:57)
+ [root@localhost ~]# pwd (2014-09-09 06:23:57)
[root@localhost ~]# cd /tmp/ (2014-09-09 06:24:00)
+ [root@localhost tmp]# ls (2014-09-09 06:24:04)
[root@localhost tmp]# cd /mnt/ (2014-09-09 06:24:08)
+ [root@localhost mnt]# ls (2014-09-09 06:24:13)
    
```

查看时间: 2014-09-09 审计员签字:

✧ 对于 AS400 协议会话比较特殊，只支持会话回放，无详细信息记录，但可对会话进行审计；

✧ 对于 RDP 协议的图形界面会话查看详细信息，详细信息中包含：键盘信息、屏幕信息和

文件读写信息等，如

The screenshot shows the 'Audit Management' interface. The breadcrumb path is 'Audit Management > Session Audit > Detailed Information'. The main title is 'NABH运维会话日志记录表'. The table contains the following data:

用户名:	111	设备名:	10.10.1.130	客户IP:	172.16.1.231	设备IP:	10.10.1.130
开始时间:	2014-09-21 01:16:14	结束时间:	2014-09-21 01:19:59	设备帐户:	xing	操作命令:	共0条

Additional interface elements include: '查看时间: 2014-09-21', '审计员签字:', '第1页/共1页', and '共 0 条信息 首页 < 1/1 > 尾页'.

屏幕信息:

The screenshot shows the 'Audit Management' interface with the 'Screen Information' category selected. The main title is 'NABH运维会话日志记录表'. The table contains the following data:

用户名:	111	设备名:	10.10.1.61	客户IP:	172.16.1.231	设备IP:	10.10.1.61
开始时间:	2014-09-21 01:31:53	结束时间:	2014-09-21 01:32:09	设备帐户:		操作命令:	共0条

Additional interface elements include: '查看时间: 2014-09-21', '审计员签字:', '第1页/共1页', and '共 0 条信息 首页 < 1/1 > 尾页'.

文件读写信息，针对开启磁盘映射后，对本地文件的读写记录:

Neusoft 东软 NetEye 统一身份管控系统 用户: 111 安全退出

系统首页 系统管理 运维管理 口令管理 审计管理 运维操作 工具下载 修改密码

审计管理 > 会话审计 > 详细信息

概要信息 详细信息 审核批注 查看审计

回放 远程回放 下载 查找 保存 打印 单页 展开 信息编码: GBK 信息类别: 文件读写

NABH运维会话日志记录表

用户名:	111	设备名:	10.10.1.61	客户IP:	172.16.1.231	设备IP:	10.10.1.61
开始时间:	2014-09-21 01:31:53	结束时间:	2014-09-21 01:32:09	设备帐户:		操作命令:	共0条

查看时间: 2014-09-21 审计员签字:

第1页/共1页

返回 上一条 下一条 共 0 条信息 首页 < 1/1 > 尾页

◇ 对于应用发布的数据库协议,除了包含上述 RDP 协议的详细“信息种类”外,还有 Oracle、Informix、DB2 等主流数据库信息:

Neusoft 东软 NetEye 统一身份管控系统 用户: 111 安全退出

系统首页 系统管理 运维管理 口令管理 审计管理 运维操作 工具下载 修改密码

审计管理 > 会话审计 > 详细信息

概要信息 详细信息 审核批注 查看审计

回放 远程回放 下载 查找 保存 打印 单页 展开 信息编码: GBK 数据库类别: ORACLE 信息类别: 数据库信

NABH运维会话日志记录表

用户名:	111	设备名:	10.10.1.61	客户IP:	172.16.1.231	设备IP:	10.10.1.61
开始时间:	2014-09-21 01:31:53	结束时间:	2014-09-21 01:32:09	设备帐户:		操作命令:	共0条

查看时间: 2014-09-21 审计员签字:

第1页/共1页

返回 上一条 下一条 共 0 条信息 首页 < 1/1 > 尾页

审核批注: 可对会话进行合规、不合规、填写备注等操作;

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 会话审计 > 审核批注

概要信息 | 详细信息 | **审核批注** | 查看告警 | 查看审计

回放 | 下载

*合规性: 合规 不合规

审核批注:

确定 | 返回

查看告警: 可查看当前会话的告警信息。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 会话审计 > 查看告警

概要信息 | 详细信息 | 审核批注 | **查看告警** | 查看审计

回放 | 下载

时间	操作命令	级别	分类
2014-09-09 06:23:45	ls	普通	黑名单
2014-09-09 06:24:06	ls	普通	黑名单
2014-09-09 06:24:14	ls	普通	黑名单
2014-09-09 06:24:25	ls	普通	黑名单

返回 | 共 4 条信息 首页 < 1/1 > 尾页

查看审计: 可查看当前会话的审计操作。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 会话审计 > 查看审计

概要信息 | 详细信息 | 审核批注 | 查看告警 | **查看审计**

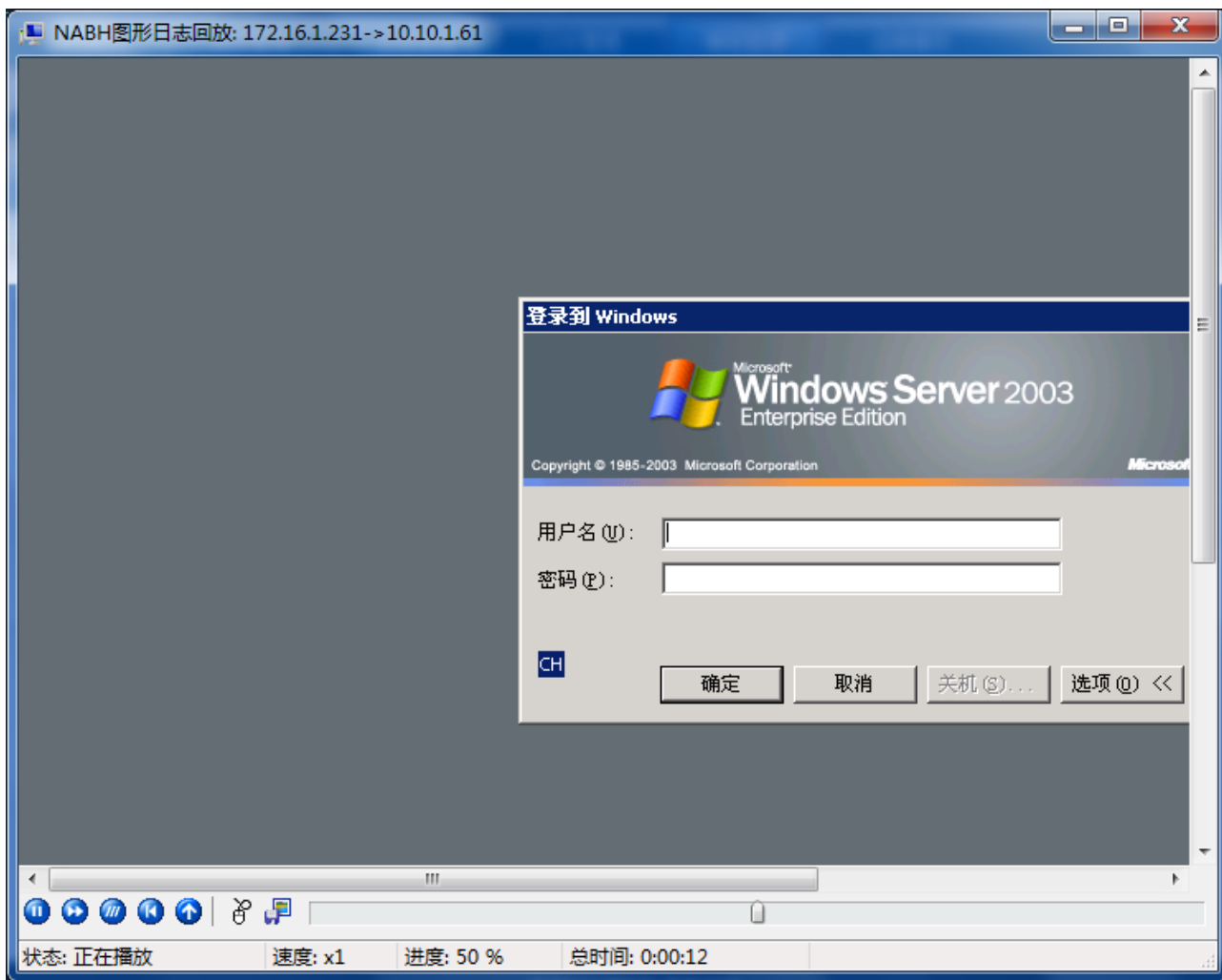
回放 | 下载






时间	操作员	IP地址	操作内容
2014-09-09 07:32:09	linzh	172.16.1.125	用户"linzh"查看ID为B40E2C4C59FEA2D6的会话的概要信息。
2014-09-09 07:32:10	linzh	172.16.1.125	用户"linzh"查看ID为B40E2C4C59FEA2D6的会话的详细信息。
2014-09-09 07:33:14	linzh	172.16.1.125	用户"linzh"查看ID为B40E2C4C59FEA2D6的会话的详细信息。
2014-09-09 07:37:36	linzh	172.16.1.125	用户"linzh"查看ID为B40E2C4C59FEA2D6的会话的概要信息。
2014-09-09 07:39:52	linzh	172.16.1.125	用户"linzh"查看ID为B40E2C4C59FEA2D6会话的告警。
2014-09-09 07:40:10	linzh	172.16.1.125	用户"linzh"查看ID为B40E2C4C59FEA2D6会话的审计操作。

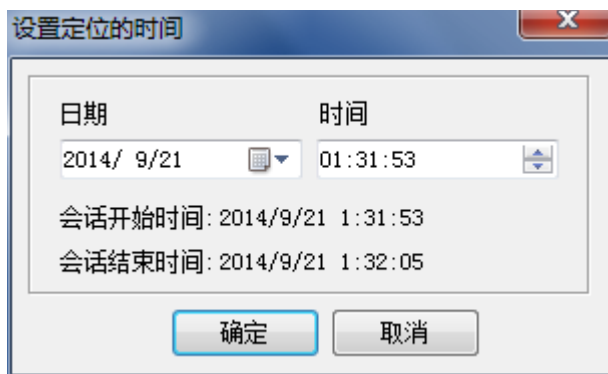
返回 | 共 5 条信息 首页 < 1/1 > 尾页

2.2.1.2 会话回放

对任意一条会话日志，通过点击右侧操作栏中的【回放】按钮，可对此会话进行完整的回放。（注：会话日志较大时下载的等待时间较长，建议使用远程回放，以免页面无法响应）



 : 暂停播放
  : 提高速度
  : 降低速度
  : 从头播放
  : 定位时间

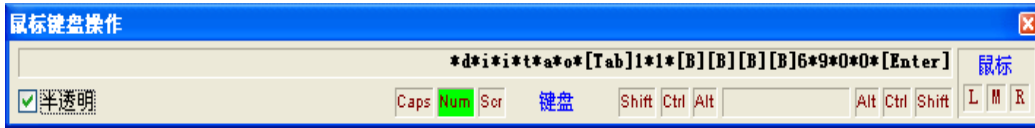




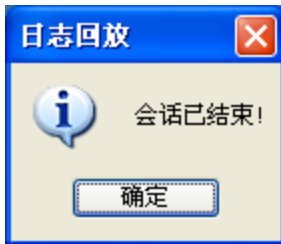
：保存屏幕图像



：显示鼠标键盘操作，高亮显示正在进行的动作，如下图：



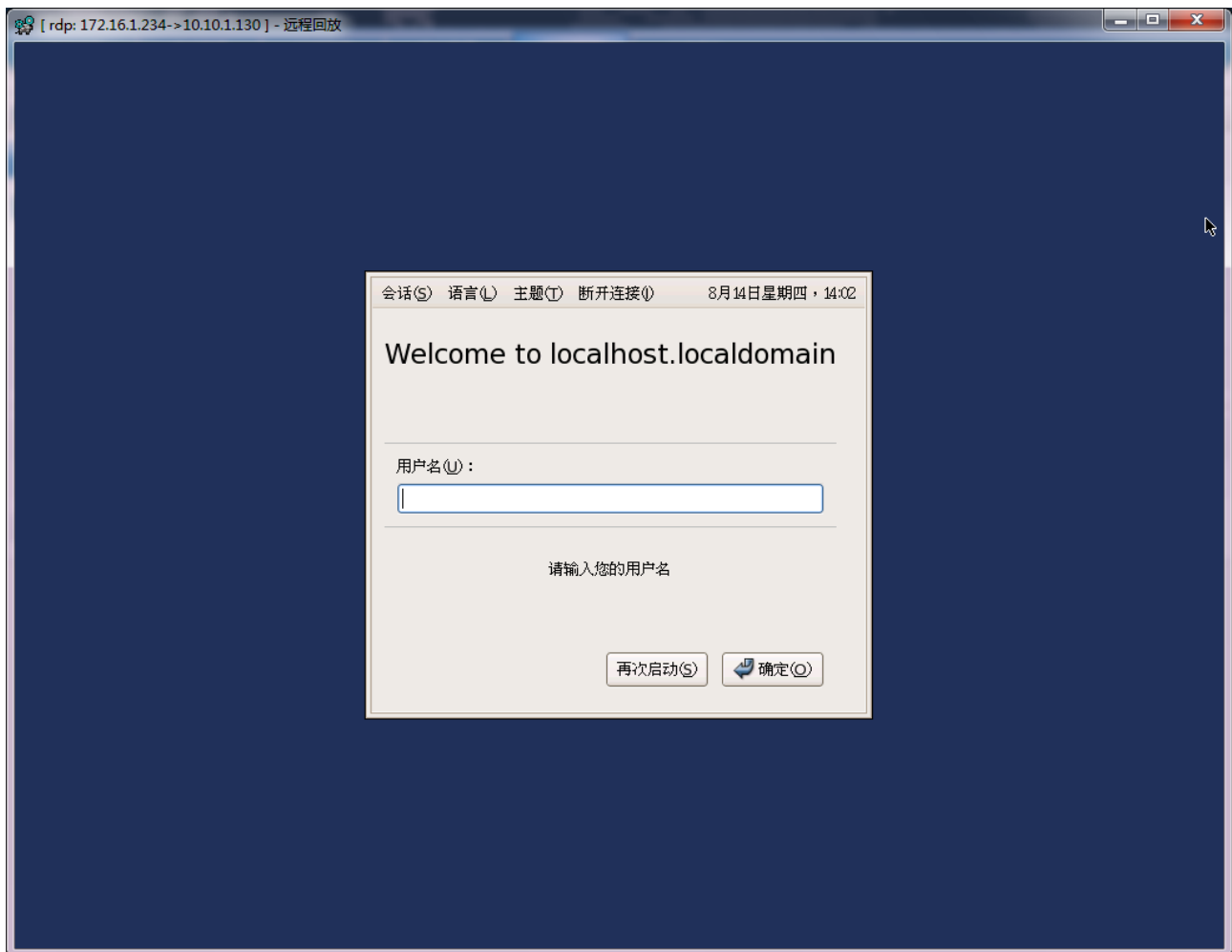
回放结束时：



2.2.1.3 远程回放

针对大数据量的图形协议日志，在详细信息中提供了远程回放的功能。会话-》详情-》概要信息-》远程回放：如下界面。进行远程回放时，不能对会话拖拉拽（快进、后退等）。





2.2.1.4 会话日志下载

在对任意一条会话日志，通过点击右侧操作栏中的【下载】按钮，可对此会话进行下载保存操作。

审计管理 > 会话审计 > 概要信息

概要信息 详细信息 审核批注 查看审计

回放 远程回放 下载

运维状态

会话ID:	B40E238F0DA4CF53	用户名:	yufc	设备帐号:		设备名:	10.10.1.130
协议名:	xwin	客户IP:	172.16.1.234	设备IP:	10.10.1.130	命令告警状态:	正常
开始时间:	2014-09-09 05:45:52	结束时间:	2014-09-09 05:45:57	复核人:			

审计状态

是否审计:	已审计	合规性:	未设置	批注:	
-------	-----	------	-----	-----	--

返回 上一条 下一条

要打开或保存来自 10.10.1.10 的 xwin.B40E238F0DA4CF53.wlog (56.2 KB)吗? 打开(O) 保存(S) 取消(C) 556789

2.2.1.5 会话查询配置

查询配置: 主要是通过定义的查询条件, 对会话进行查询。【查询条件选择】即可直接引用已保存的查询条件, 点击右上角【查询配置】按钮, 打开会话查询条件配置页面。

审计管理 > 会话审计 > 查询配置

可引用条件:	无
会话ID:	
*用户名:	待选中用户 11 111 hjx linzh liu liuxf qq test0 test4 xing yufc 已选中用户
客户IP:	
*设备名:	待选中设备 10.10.1.130 10.10.1.254 172.16.1.211 172.16.1.214 172.16.1.217 172.16.1.241 172.16.1.254 testad.local xing 已选中设备
*协议类型:	全部协议
开始时间:	2014-09-09 00:00:00
结束时间:	2014-09-09 23:59:59
关键字检索:	
	<input type="checkbox"/> 上行检索 <input type="checkbox"/> 下行检索
会话时长:	≥ [] [单位: 分钟]
	≤ [] [单位: 分钟]
*复核人:	任意复核人
*会话是否成功:	任意选项
*会话是否合规:	任意选项
条件数据处理方式:	只应用

可根据需求自行选择会话查询条件，也可引用已定义的会话查询条件。

可引用条件：为 2.6.1 中定义过的会话查询条件，也可通过【条件数据处理方式】将选择的条件进行保存。

字段显示： 审计员可任意定义当前视图中显示的字段，具体可参见 2.6.1 节，审计配置中“自定义字段设置”。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 会话审计 > 会话查询

会话查询 | 会话统计

开始时间: 2014-09-09 00:00:00 结束时间: 2014-09-09 23:59:59 默认字段显示

状态	用户名	客户IP	设备名	协议	设备IP	开始时间	结束时间	设备帐户名	日志大小	操作
✔	111	172.16.1.125	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...		73byte	回拉 下载 详情
	111	172.16.1.125	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...		73byte	回拉 下载 详情
✔	111	172.16.1.125	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...	root	6.723K	回拉 下载 详情
	111	172.16.1.125	10.10.1.130	ssh	10.10.1.130	2014-09-09...	2014-09-09...	root	3.562K	回拉 下载 详情
	linzh	172.16.1.125	10.10.1.130	ssh	10.10.1.130	2014-09-09...	2014-09-09...	root	377byte	回拉 下载 详情
✔	xing	172.16.1.231	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...	xing	2.914K	回拉 下载 详情
	xing	172.16.1.231	10.10.1.254	telnet	10.10.1.254	2014-09-09...	2014-09-09...		1.345K	回拉 下载 详情
	xing	172.16.1.231	10.10.1.254	telnet	10.10.1.254	2014-09-09...	2014-09-09...		1.108K	回拉 下载 详情
	xing	172.16.1.231	172.16.1.254	telnet	172.16.1.254	2014-09-09...	2014-09-09...	jiangnan	3.103K	回拉 下载 详情
	xing	172.16.1.231	172.16.1.211	telnet	172.16.1.211	2014-09-09...	2014-09-09...		486byte	回拉 下载 详情

共 24 条信息 首页 < 1/3 > 尾页 1

默认字段为状态、用户名、客户 IP、设备名、协议、设备 IP、开始时间、结束时间、设备帐户名、日志大小、操作。

2.3 会话统计

“会话统计”是针对会话统计条件产生图形和表格两种格式报表。

1) 选择“会话统计”，下方显示该统计区域，如下图：

系统首页		系统管理		运维管理		口令管理		审计管理		运维操作		工具下载		修改密码			
审计管理 > 会话审计 > 会话统计																	
会话查询		会话统计															
时间访问统计表		日统计		2014		年 9		月 9		日		统计		图表		导出报表	
时间	访问总量 (共计:24)	成功访问数 (共计:24)	认证失败访问数 (共计:0)	授权失败数 (共计:0)	操作												
00	0	0	0	0	查看												
01	0	0	0	0	查看												
02	0	0	0	0	查看												
03	0	0	0	0	查看												
04	0	0	0	0	查看												
05	15	15	0	0	查看												
06	8	8	0	0	查看												
07	1	1	0	0	查看												
08	0	0	0	0	查看												
09	0	0	0	0	查看												
10	0	0	0	0	查看												
11	0	0	0	0	查看												
12	0	0	0	0	查看												
13	0	0	0	0	查看												
14	0	0	0	0	查看												
15	0	0	0	0	查看												
16	0	0	0	0	查看												
17	0	0	0	0	查看												

统计选择条件有：

统计类型：

时间访问统计： 以时间为标准进行统计；

用户访问统计： 以用户为标准进行统计；

用户组访问统计： 以用户组为标准进行统计；

设备访问统计： 以设备为标准进行统计；

设备组访问统计： 以设备组为标准进行统计；

单位时间： 按年、月、日进行统计；

时间范围： 按照指定的时间区间进行统计；

2) 选择好统计条件后，点击【统计】按钮，即统计出相应的统计表格，如：统计 2014 年第三季度户访问次数，则如下图：

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 工具下载 | 修改密码

审计管理 > 会话审计 > 会话统计

会话查询 **会话统计**

时间访问统计表 | 季统计 | 2014 年 第三季度 | 统计 图表 | 导出报表

时间	访问总量 (共计:24)	成功访问数量 (共计:24)	认证失败访问数量 (共计:0)	授权失败数量 (共计:0)	操作
07	0	0	0	0	查看
08	0	0	0	0	查看
09	24	24	0	0	查看

【查看】按钮：则将此行中用户会话量的信息详细列出。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 工具下载 | 修改密码

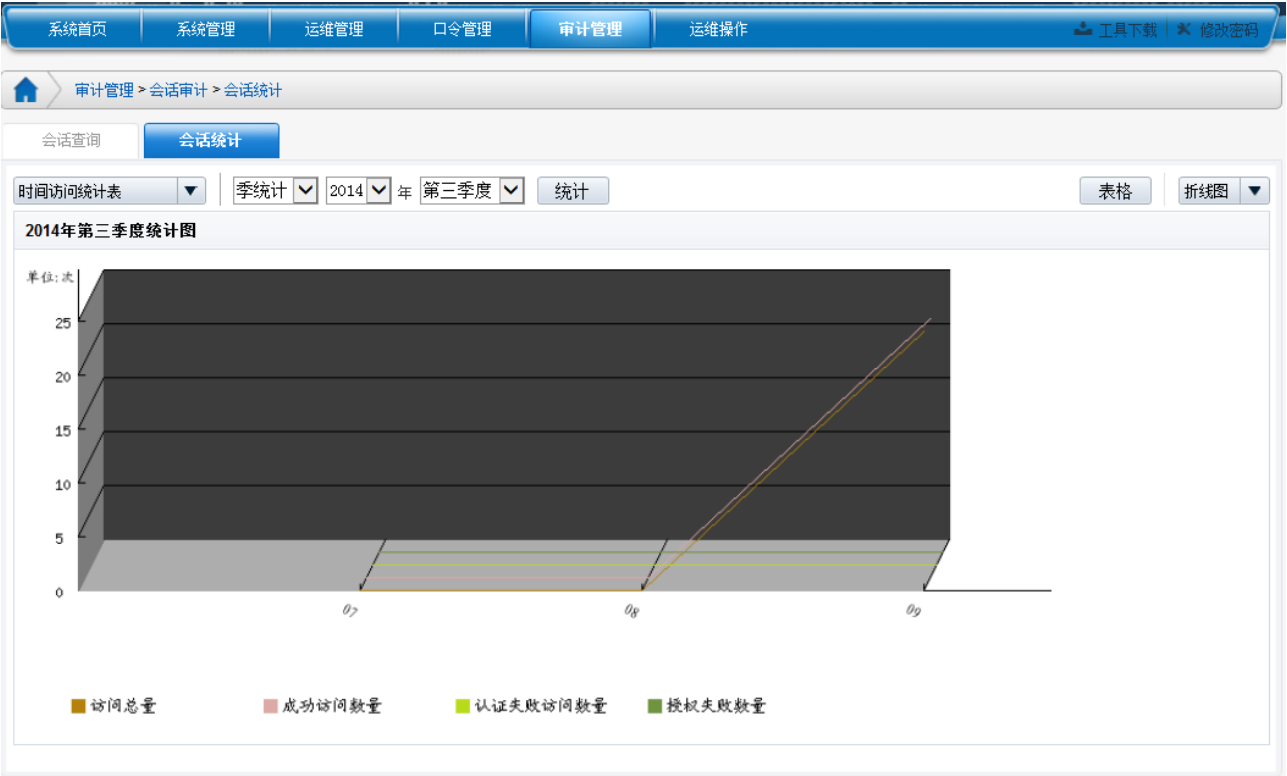
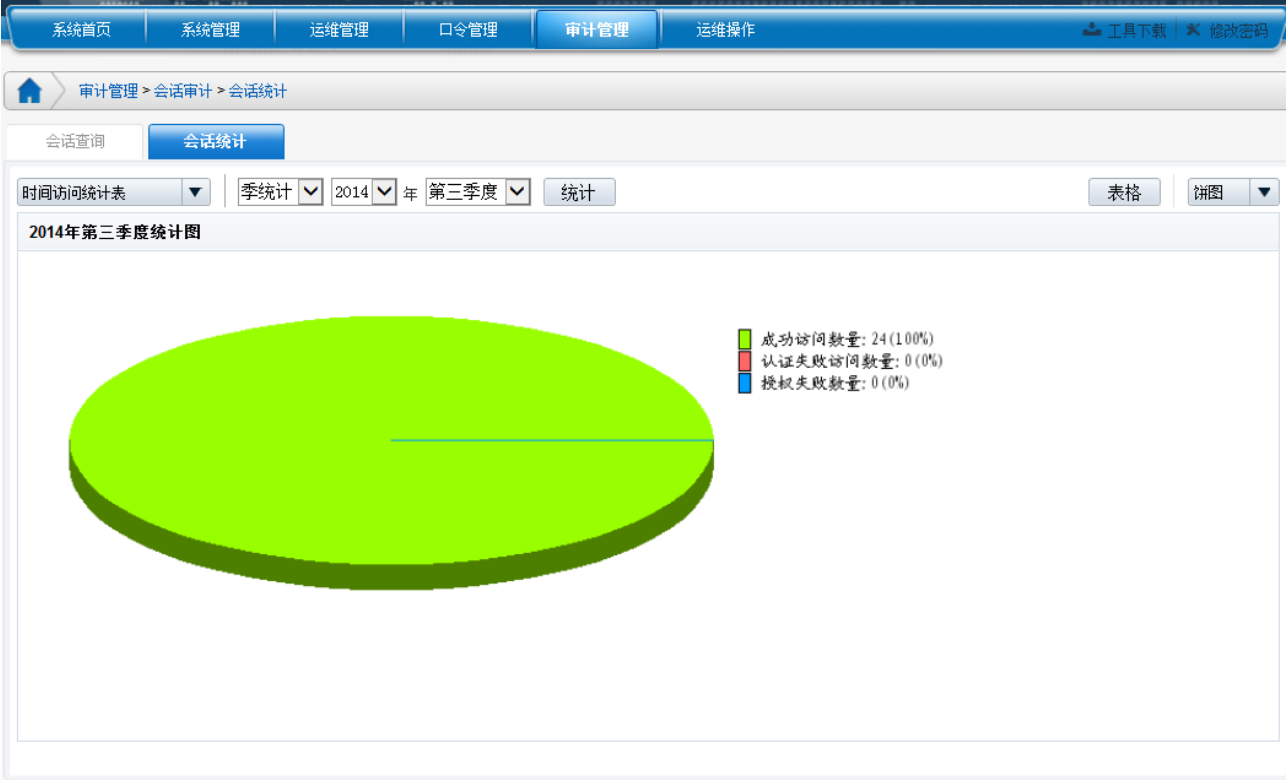
审计管理 > 统计分析

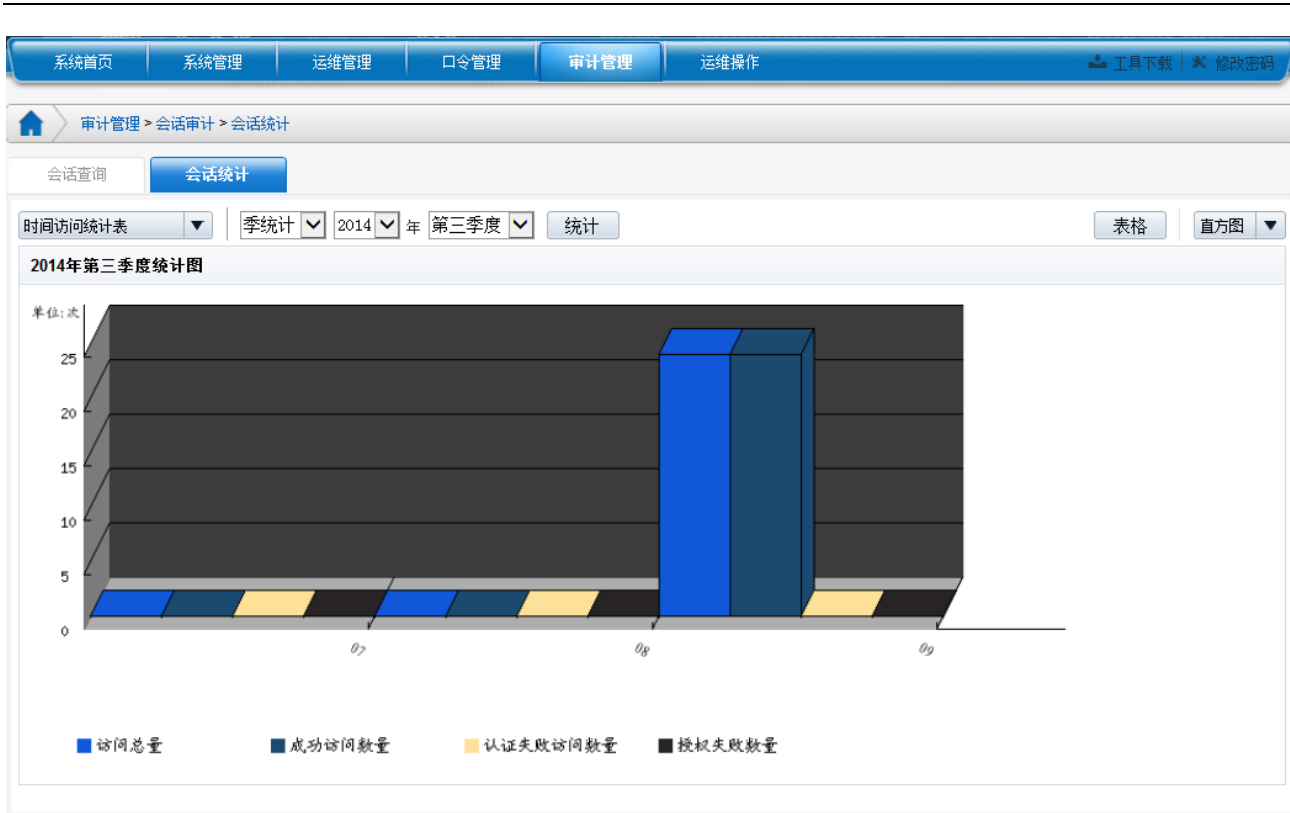
状态	用户名	客户IP	设备名	协议	设备IP	开始时间	结束时间	设备帐户名	日志大小	操作
✔	111	172.16.1....	10.10.1.130	telnet	10.10.1.130	2014-09-...	2014-09-...		73byte	回拉 下载 详情
	111	172.16.1....	10.10.1.130	telnet	10.10.1.130	2014-09-...	2014-09-...		73byte	回拉 下载 详情
✔	111	172.16.1....	10.10.1.130	telnet	10.10.1.130	2014-09-...	2014-09-...	root	6.723K	回拉 下载 详情
	111	172.16.1....	10.10.1.130	ssh	10.10.1.130	2014-09-...	2014-09-...	root	3.562K	回拉 下载 详情
	linzh	172.16.1....	10.10.1.130	ssh	10.10.1.130	2014-09-...	2014-09-...	root	377byte	回拉 下载 详情
✔	xing	172.16.1....	10.10.1.130	telnet	10.10.1.130	2014-09-...	2014-09-...	xing	2.914K	回拉 下载 详情
	xing	172.16.1....	10.10.1.254	telnet	10.10.1.254	2014-09-...	2014-09-...		1.345K	回拉 下载 详情
	xing	172.16.1....	10.10.1.254	telnet	10.10.1.254	2014-09-...	2014-09-...		1.108K	回拉 下载 详情
	xing	172.16.1....	172.16.1.254	telnet	172.16.1.254	2014-09-...	2014-09-...	jiangnan	3.103K	回拉 下载 详情
	xing	172.16.1....	172.16.1.211	telnet	172.16.1.211	2014-09-...	2014-09-...		486byte	回拉 下载 详情

返回 共 24 条信息 首页 < 1/3 > 尾页 1

通过点击右侧操作栏中的按钮可进行相应操作，具体功能可参见 2.2.1 节

- 选择【图片】按钮后，会切换为统计图模式，根据选择统计图类型，显示相应的统计图表。点击【表格】按钮后，可切换为统计表格模式。





2.4 告警审计

2.4.1 告警查询

用户在日常的运维过程中，可能会出现某些误操作或恶意操作。为了防止这些操作造成严重的后果，NABH 系统通过一些相关的设置，对这些操作进行阻断或者警告。告警审计模块的功能就是对告警事件进行审计。

告警审计默认显示当天所有的告警记录。支持按照级别、时间进行快速查询。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 告警审计

级别: 任意 | 开始时间: 2014-09-09 00:00:00 | 结束时间: 2014-09-09 23:59:59 | 确定 | 查询条件选择 | 查询配置

时间	操作命令	级别	运维用户	设备IP	设备名	协议	关联会话状态	操作
2014-09-09...	ls	普通	yufc	10.10.1.130	10.10.1.130	ssh	已结束	查看 关联会话回放
2014-09-09...	ls	普通	yufc	10.10.1.130	10.10.1.130	ssh	已结束	查看 关联会话回放
2014-09-09...	ls	普通	yufc	10.10.1.130	10.10.1.130	ssh	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	telnet	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	telnet	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	telnet	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	telnet	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	ssh	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	ssh	已结束	查看 关联会话回放
2014-09-09...	ls	普通	111	10.10.1.130	10.10.1.130	ssh	已结束	查看 关联会话回放

共 11 条信息 | 首页 < 1/2 > 尾页 1

针对不同的告警级别（普通、警告、严重），使用不同的颜色来区分每个告警
 点击操作栏中的【查看】按钮，可查看会话的详细信息

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 会话审计 > 概要信息

概要信息 | 详细信息 | 审核批注 | 查看告警 | 查看审计

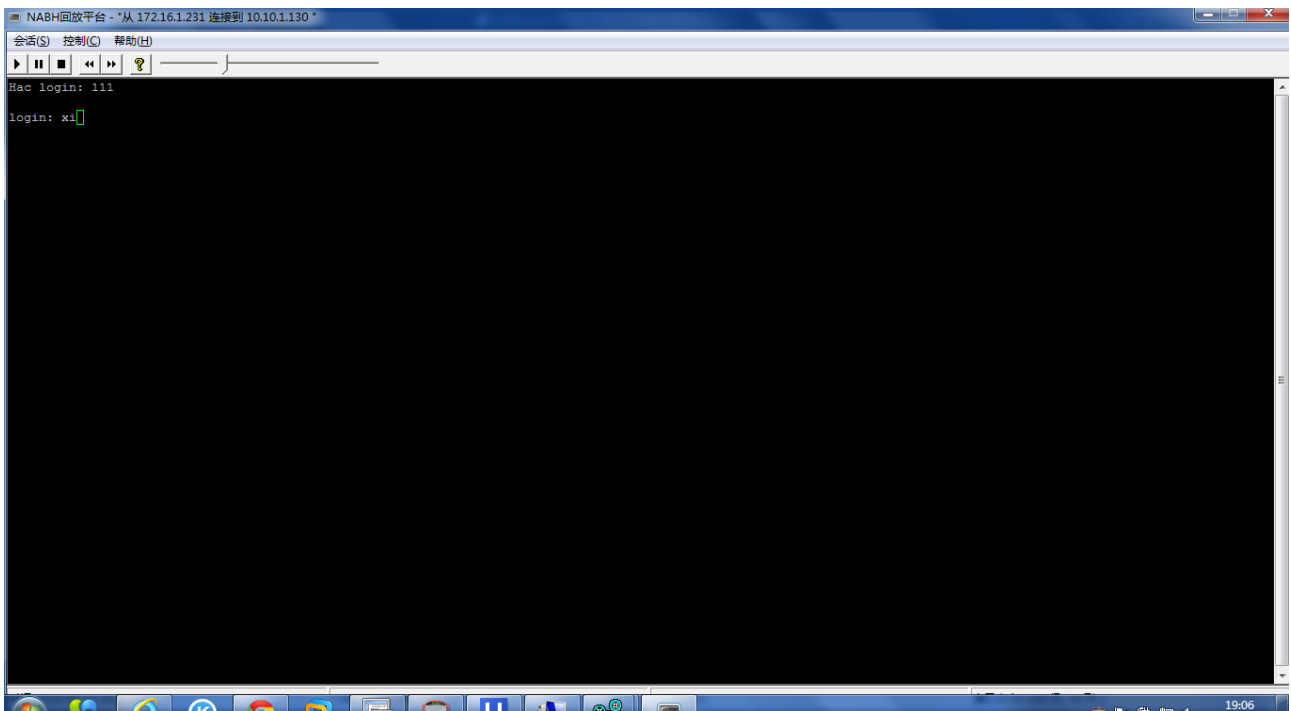
回放 | 下载

运维状态							
会话ID:	B40E24A8A9190F3C	用户名:	yufc	设备帐号:	yufc	设备名:	10.10.1.130
协议名:	ssh	客户IP:	172.16.1.234	设备IP:	10.10.1.130	命令告警状态:	阻断
开始时间:	2014-09-09 05:50:32	结束时间:	2014-09-09 06:09:21	复核人:	test4		

审计状态			
是否审计:	未审计	合规性:	未设置
批注:			

返回 | 上一条 | 下一条

【关联会话按钮】可以进行关联会话回放。



2.4.2 告警查询配置

查询配置：主要是通过定义的查询条件，对告警进行查询。【查询条件选择】即可直接引用已保存的查询条件，点击右上角【查询配置】按钮，打开告警查询条件配置页面。

系统首页	系统管理	运维管理	口令管理	审计管理	运维操作	工具下载	修改密码
审计管理 > 告警审计 > 查询配置							
可引用条件:	无						
告警类型:	任意类型						
告警级别:	任意						
*用户名:	待选中用户	已选中用户					
	11 111 hjx linzh liu liuxf qq test0 test4 xing yufc	>> > < <<					
*设备名:	待选中设备	已选中设备					
	10.10.1.130 10.10.1.254 172.16.1.211 172.16.1.214 172.16.1.217 172.16.1.241 172.16.1.254 testad.local xing	>> > < <<					
*协议类型:	全部协议						
*复核人:	任意复核人						
开始时间:	2014-09-09 00:00:00						
结束时间:	2014-09-09 23:59:59						
条件数据处理方式:	只应用						
<input type="button" value="确定"/> <input type="button" value="返回"/>							

可根据需求自行选择告警查询条件，也可引用已定义的告警查询条件。

可引用条件：为 2.6.1 中定义过的告警查询条件，也可通过【条件数据处理方式】将选择的条件进行保存。

2.5 事件审计

事件审计主要是对 NABH 系统的自审计。包括系统自审计日志的管理，业务权限审计，以及管理员、用户、设备、授权规则的审计等等。

2.5.1 事件查询

事件查询默认显示是审计 NABH 管理员（包括系统管理员、审计员等）在当天的操作，如：增加用户、删除用户、编辑角色等。支持按照模块、操作者和时间进行快速查询。

Neusoft 东软 NetEye 统一身份管控系统 用户: linzh | 安全退出

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 工具下载 | 修改密码

审计管理 > 事件审计

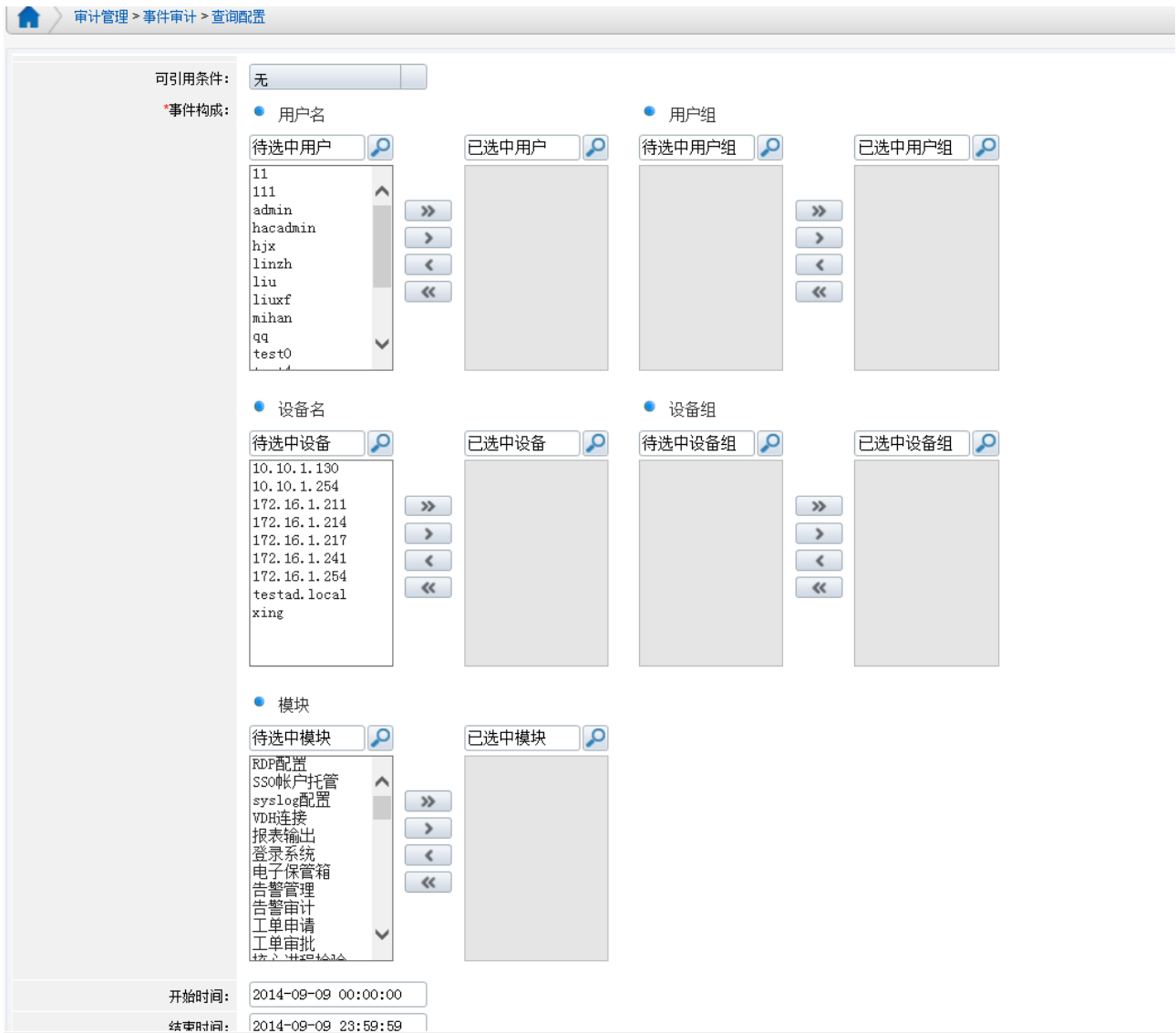
任意模块 | 任意操作者 | 开始时间: 2014-09-09 00:00:00 | 结束时间: 2014-09-09 23:59:59 | 确定 | 查询条件选择 | 查询配置

记录时间	事件主机IP	事件级别	操作者	模块名	日志内容
2014-09-09 00:04:04	172.16.1.125	通知	111	退出系统	用户"111"超时退出WEB系统。
2014-09-09 00:05:34	172.16.1.234	通知	yufc	登录系统	用户"yufc"尝试登录失败。
2014-09-09 00:05:38	172.16.1.234	通知	yufc	登录系统	用户"yufc"尝试登录失败。
2014-09-09 00:05:51	172.16.1.234	通知	hacadmin	登录系统	用户"hacadmin"登录WEB系统。
2014-09-09 00:07:53	172.16.1.233	通知	zouj	登录系统	用户"zouj"尝试登录失败。
2014-09-09 00:08:58	172.16.1.233	通知	hacadmin	登录系统	用户"hacadmin"登录WEB系统。
2014-09-09 00:09:11	172.16.1.233	通知	hacadmin	系统信息	用户"hacadmin"查看系统信息。
2014-09-09 00:29:30	172.16.1.234	通知	yufc	登录系统	用户"yufc"尝试登录失败。
2014-09-09 00:29:38	172.16.1.234	通知	hacadmin	登录系统	用户"hacadmin"登录WEB系统。
2014-09-09 00:30:14	172.16.1.234	通知	hacadmin	用户管理	用户"hacadmin"添加管理员"yufc", 认证方式为口令认证, 组织为RO...

共 400 条信息 首页 < 1/40 > 尾页 1

2.5.2 事件查询配置

查询配置: 主要是通过定义的查询条件, 对事件进行查询。【查询条件选择】即可直接引用已保存的查询条件, 点击右上角【查询配置】按钮, 打开事件查询条件配置页面。



可根据需求自行选择事件查询条件，也可引用已定义的事件查询条件。

可引用条件：为 2.6.1 中定义过的事件查询条件，也可通过【条件数据处理方式】将选择的条件进行保存。

2.6 报表审计

报表审计可将 NABH 配置、会话日志、管理日志、告警、审计员审计操作等信息统计成报表并输出。



2.6.1 日常报表

日常报表主要是将 NABH 系统的基本配置以及当日的会话日志和管理日志生成报表并输出。生成的报表可进行打印和下载，下载支持的格式有 PDF 文档、Word 文档、Excel 文档；



通过选择报表内容，点击确定后即可生成相应的报表。例如：生成今日会话报表，

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载

今日会话信息报表

用户名	设备帐户名	客户IP	设备IP	协议名	复核人	开始时间	结束时间	日志大小
111		172.16.1.125	10.10.1.130	telnet	linzh	2014-09-09 06:19:12	2014-09-09 06:21:17	73byte
111		172.16.1.125	10.10.1.130	telnet		2014-09-09 06:22:00	2014-09-09 06:22:30	73byte
111	root	172.16.1.125	10.10.1.130	telnet	linzh	2014-09-09 06:23:08	2014-09-09 06:24:57	6.723K
111	root	172.16.1.125	10.10.1.130	ssh	linzh	2014-09-09 06:25:17	2014-09-09 07:12:41	3.562K
linzh	root	172.16.1.125	10.10.1.130	ssh		2014-09-09 07:30:06	2014-09-09 07:42:57	377byte
xing	xing	172.16.1.231	10.10.1.130	telnet		2014-09-09 05:31:40	2014-09-09 05:32:16	2.914K
xing		172.16.1.231	10.10.1.254	telnet		2014-09-09 05:53:27	2014-09-09 05:53:58	1.345K
xing		172.16.1.231	10.10.1.254	telnet		2014-09-09 05:56:47	2014-09-09 05:57:10	1.108K
xing	jiangnan	172.16.1.231	172.16.1.254	telnet		2014-09-09 06:00:09	2014-09-09 06:05:18	3.103K
xing		172.16.1.231	172.16.1.211	telnet		2014-09-09 06:16:23	2014-09-09 06:16:36	486byte

共 25 条信息 | 首页 < 1/3 > 尾页 1

2.6.2 创建会话报表

创建会话报表主要是通过定义的查询条件，对会话日志进行统计并生成报表。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计

1. 报表种类选择 | **2. 报表定制** | 3. 报表生成

会话报表定制

报表名称:

报表标题:

*字段选择:

用户名
客户IP
设备名
协议
设备IP
开始时间
结束时间
设备帐户名
日志大小
复核人

排序字段: 用户名

排序规则: 升序

查询条件设置: 显示 (必须配置用户名和设备名)

上一步 | 确定

查询设置展开，如下图所示：

查询条件设置: 隐藏 (必须配置用户名和设备名)

可引用条件: 无

*用户名: 待选中用户 已选中用户

11
111
hjsx
linzh
liu
liuxf
qq
test0
test4
xing
yufc
.....

客户IP:

*设备名: 待选中设备 已选中设备

10.10.1.130
10.10.1.254
172.16.1.211
172.16.1.214
172.16.1.217
172.16.1.241
172.16.1.254
testad.local
xing

*协议类型: 全部协议

开始时间: 2014-09-09 00:00:00

结束时间: 2014-09-09 23:59:59

关键字检索:

上行检索 下行检索

会话时长: ≥ [单位: 分钟]
 ≤ [单位: 分钟]

*复核人: 任意复核人

*会话是否成功: 任意选项

*会话是否合规: 任意选项

条件数据处理方式: 只应用

上一步 确定

基本属性:

定义生成报表的名称和标题;

字段选择:

定义生成的报表中所要显示的字段;

报表排序:

设置报表生成后, 数据的排序字段及规则;

查询条件设置

可根据需求自行设置查询条件, 并且可引用已定义的会话报表查询条件。

可引用条件: 为 2.6.1 中定义过的会话报表查询条件, 也可通过【条件数据处理方式】将选择的条件进行保存。

点击“生成报表”按钮后，在主窗口中显示报表内容

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载

neteye
(2014-09-09 00:00:00至2014-09-09 23:59:59)

会话定制报表

用户名	客户IP	设备名	协议	设备IP	开始时间	结束时间	设备帐户名	日志大小	复核人
111	172.16.1.125	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...		73byte	
111	172.16.1.125	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...		73byte	
111	172.16.1.125	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...	root	6.723K	
111	172.16.1.125	10.10.1.130	ssh	10.10.1.130	2014-09-09...	2014-09-09...	root	3.562K	
linzh	172.16.1.125	10.10.1.130	ssh	10.10.1.130	2014-09-09...	2014-09-09...	root	377byte	
xing	172.16.1.231	10.10.1.130	telnet	10.10.1.130	2014-09-09...	2014-09-09...	xing	2.914K	
xing	172.16.1.231	10.10.1.254	telnet	10.10.1.254	2014-09-09...	2014-09-09...		1.345K	
xing	172.16.1.231	10.10.1.254	telnet	10.10.1.254	2014-09-09...	2014-09-09...		1.108K	
xing	172.16.1.231	172.16.1.254	telnet	172.16.1.254	2014-09-09...	2014-09-09...	jiangnan	3.103K	
xing	172.16.1.231	172.16.1.211	telnet	172.16.1.211	2014-09-09...	2014-09-09...		486byte	

共 25 条信息 首页 < 1/3 > 尾页 1

2.6.3 创建运维操作报表

创建运维操作报表主要是通过定义的查询条件，对 NABH 的运维操作日志进行统计并生成报表。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计

1. 报表种类选择 | **2. 报表定制** | 3. 报表生成

1 运维操作报表定制

报表名称:

报表标题:

排序字段: ▼

排序规则: ▼

查询条件设置: 显示 (必须配置用户名和设备名)

上一步 | 确定

基本属性:

定义生成报表的名称和标题；

报表排序：

设置报表生成后，数据的排序字段及规则；

查询条件设置：

可根据需求自行设置查询条件，并且可引用已定义的运维操作报表查询条件。

可引用条件：为 2.6.1 中定义过的运维操作报表条件，也可通过【条件数据处理方式】将选择的条件进行保存。

点击“生成报表”按钮后，在主窗口中显示报表内容。

系统首页 | 系统管理 | 运维管理 | 口令管理 | 审计管理 | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载

运维操作
(2014-09-09 00:00:00至2014-09-09 23:59:59)

运维操作定制报表

会话ID	用户名	客户端IP	目标主机IP	设备名	协议	操作命令	操作时间
B40E1C9B18D9378B	yufc	172.16.1.234	10.10.1.130	10.10.1.130	telnet		2014-09-09 05:17:38
B40E1C9B18D9378B	yufc	172.16.1.234	10.10.1.130	10.10.1.130	telnet	login: yufc	2014-09-09 05:17:38
B40E1C9B18D9378B	yufc	172.16.1.234	10.10.1.130	10.10.1.130	telnet	Password:	2014-09-09 05:17:45
B40E1C9B18D9378B	yufc	172.16.1.234	10.10.1.130	10.10.1.130	telnet	\$ ls	2014-09-09 05:17:52
B40E203C0B1D6993	xing	172.16.1.231	10.10.1.130	10.10.1.130	telnet		2014-09-09 05:31:40
B40E203C0B1D6993	xing	172.16.1.231	10.10.1.130	10.10.1.130	telnet	login: sulli	2014-09-09 05:31:40
B40E203C0B1D6993	xing	172.16.1.231	10.10.1.130	10.10.1.130	telnet	Password:	2014-09-09 05:31:46
B40E203C0B1D6993	xing	172.16.1.231	10.10.1.130	10.10.1.130	telnet	login: xing	2014-09-09 05:31:50
B40E203C0B1D6993	xing	172.16.1.231	10.10.1.130	10.10.1.130	telnet	Password:	2014-09-09 05:31:58
B40E203C0B1D6993	xing	172.16.1.231	10.10.1.130	10.10.1.130	telnet	login: xing	2014-09-09 05:32:02

共 109 条信息 首页 < 1/1 > 尾页 1

2.6.4 创建帐户分配报表

创建帐户分配报表主要是通过定义的查询条件，对 NABH 的帐户分配情况进行统计并生成报表。

系统首页 | 系统管理 | 运维管理 | 口令管理 | 审计管理 | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计

1. 报表种类选择 | 2. 报表定制 | 3. 报表生成

帐户分配报表定制

报表名称:

报表标题:

排序字段: 设备帐户名

排序规则: 升序

查询条件设置: 显示

上一步 | 确定

基本属性:

定义生成报表的名称和标题;

报表排序:

设置报表生成后, 数据的排序字段及规则;

查询条件设置:

可根据需求自行设置查询条件, 并且可引用已定义的帐户分配报表查询条件。

可引用条件: 为 2.6.1 中定义过的帐户分配报表条件, 也可通过【条件数据处理方式】将选择的条件进行保存。

点击“生成报表”按钮后, 在主窗口中显示报表内容。

系统首页 | 系统管理 | 运维管理 | 口令管理 | 审计管理 | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载

帐户分配定制报表

设备帐户名	设备名	设备IP	操作系统	用户名	用户组名
root	172.16.1.224	172.16.1.224	Redhat_AS4	yufc , zouj	
sulll	172.16.1.124	172.16.1.124	Redhat_AS4	xing	
yuftp	172.16.1.241	172.16.1.241	Redhat_AS4	yufc , zouj	
zouj	172.16.1.224	172.16.1.224	Redhat_AS4	yufc , zouj	

共 4 条信息 | 首页 < 1/1 > 尾页

2.6.5 创建事件报表

创建事件报表主要是通过定义的查询条件，对 NABH 的事件日志进行统计并生成报表。

Neusoft 东软 NetEye 统一身份管控系统 用户: linzh 安全退出

系统首页 系统管理 运维管理 口令管理 审计管理 运维操作 工具下载 修改密码

审计管理 > 报表审计

1. 报表种类选择 2. 报表定制 3. 报表生成

事件报表定制

报表名称:

报表标题:

排序字段: 管理员名

排序规则: 升序

查询条件设置: + 显示 (必须配置模块名和管理员名)

上一步 确定

基本属性:

定义生成报表的名称和标题;

报表排序:

设置报表生成后，数据的排序字段及规则;

查询条件设置:

可根据需求自行设置查询条件，并且可引用已定义的会话报表查询条件。

可引用条件: 为 2.6.1 中定义过的管理报表条件，也可通过【条件数据处理方式】将选择的条件进行保存。

点击“生成报表”按钮后，在主窗口中显示报表内容。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载

事件定制报表

(2014-09-09 00:00:00至2014-09-09 23:59:59)

事件定制报表

管理员名	模块名	事件主机IP	记录时间	操作内容
111	退出系统	172.16.1.125	2014-09-09 00:04:04	用户"111"超时退出WEB系统。
111	登录系统	172.16.1.123	2014-09-09 00:47:52	用户"111"登录WEB系统。
111	系统信息	172.16.1.123	2014-09-09 00:48:16	用户"111"查看系统信息。
111	退出系统	172.16.1.123	2014-09-09 00:49:50	用户"111"退出WEB系统。
111	登录系统	172.16.1.125	2014-09-09 01:25:07	用户"111"登录WEB系统。
111	应用发布	172.16.1.125	2014-09-09 01:25:25	用户"111"添加VDH设备"vdh", IP地址为172.16.1...
111	应用发布	172.16.1.125	2014-09-09 02:00:44	用户"111"删除VDH应用: PLSQL。
111	登录系统	172.16.1.125	2014-09-09 03:21:33	用户"111"登录WEB系统。
111	系统维护	172.16.1.125	2014-09-09 03:29:11	用户"111"执行系统备份。
111	系统维护	172.16.1.125	2014-09-09 03:29:35	用户"111"执行系统恢复。

共 278 条信息 首页 < 1/28 > 尾页 1

2.6.6 创建告警报表

创建告警报表主要是通过定义的查询条件，对系统告警进行统计并生成报表。

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 工具下载 | 修改密码

审计管理 > 报表审计

1. 报表种类选择 2. 报表定制 3. 报表生成

告警报表定制

报表名称:

报表标题:

排序字段:

排序规则:

查询条件设置: 显示 (必须配置用户名和设备名)

基本属性:

定义生成报表的名称和标题;

报表排序:

设置报表生成后，数据的排序字段及规则;

查询条件和条件管理：

可引用条件：为 2.6.1 中定义过的告警报表条件，也可通过【条件数据处理方式】将选择的条件进行保存。

点击“生成报表”按钮后，在主窗口中显示报表内容。

用户名	设备名	协议	分类	级别	操作命令	时间	复核人
111	10.10.1.130	telnet	黑名单	普通	ls	2014-09-09 06:23:45	
111	10.10.1.130	telnet	黑名单	普通	ls	2014-09-09 06:24:06	
111	10.10.1.130	telnet	黑名单	普通	ls	2014-09-09 06:24:14	
111	10.10.1.130	telnet	黑名单	普通	ls	2014-09-09 06:24:25	
111	10.10.1.130	ssh	黑名单	普通	ls	2014-09-09 06:25:51	
111	10.10.1.130	ssh	黑名单	普通	ls	2014-09-09 06:25:56	
111	10.10.1.130	ssh	黑名单	普通	ls	2014-09-09 06:26:01	
111	10.10.1.130	ssh	黑名单	普通	ls	2014-09-09 06:45:59	
yufc	10.10.1.130	ssh	黑名单	普通	ls	2014-09-09 05:51:05	
yufc	10.10.1.130	10.10.1.130	黑名单	普通	ls	2014-09-09 05:53:26	

2.6.7 创建审计员操作报表

创建审计员操作报表是通过定义的统计条件，生成会话审计员对会话操作的报表。

统计条件:

审计员: 指定某一个审计员, 对其审计操作生成报表

时间类型: 指定生成报表的时间单位, 及时间范围

时间范围: 显示具体的时间范围

点击“生成报表”按钮后, 在主窗口中显示报表内容。

审计管理 > 报表审计 > 报表查看

打印 下载

审计员操作定制报表
(2014-09-09 00:00:00至2014-09-09 23:59:59)

审计员	审计时间	用户名	用户IP	设备名	协议	开始时间	结束时间	回显	回放	告警	合规性	复核人
linzh	2014-09-0...	yufc	172.16.1...	10.10.1.130	xwin	2014-09-0...	2014-09-0...	√	√	X		
linzh	2014-09-0...	yufc	172.16.1...	10.10.1.130	ssh	2014-09-0...	2014-09-0...	√	X	X		
linzh	2014-09-0...	111	172.16.1...	10.10.1.130	telnet	2014-09-0...	2014-09-0...	√	X	√		
xing	2014-09-0...	xing	172.16.1...	10.10.1.130	telnet	2014-09-0...	2014-09-0...	√	X	√		
yufc	2014-09-0...	111	172.16.1...	10.10.1.130	telnet	2014-09-0...	2014-09-0...	√	X	X		
yufc	2014-09-0...	111	172.16.1...	10.10.1.130	telnet	2014-09-0...	2014-09-0...	√	X	X		
yufc	2014-09-0...	yufc	172.16.1...	172.16.1.241	ftp	2014-09-0...	2014-09-0...	√	√	X		
yufc	2014-09-0...	yufc	172.16.1...	172.16.1.217	rdp	2014-09-09 06:48:49	...	√	X	X		
yufc	2014-09-0...	yufc	172.16.1...	172.16.1.217	rdp	2014-09-0...	2014-09-0...	√	X	X		

共 9 条信息 首页 < 1/1 > 尾页

2.6.8 创建全局统计报表

可根据用户选择的时间条件, 生成各种全局统计报表。该报表可按照时间、设备、运维帐号等三个方面进行全局统计。

Neusoft 东软 NetEye 统一身份管控系统 用户: linzh 安全退出

系统首页 系统管理 运维管理 口令管理 审计管理 运维操作 工具下载 修改密码

审计管理 > 报表审计

1. 报表种类选择 2. 报表定制 3. 报表生成

1 全局统计报表定制

开始时间: 2014-09-09 00:00:00

结束时间: 2014-09-09 23:59:59

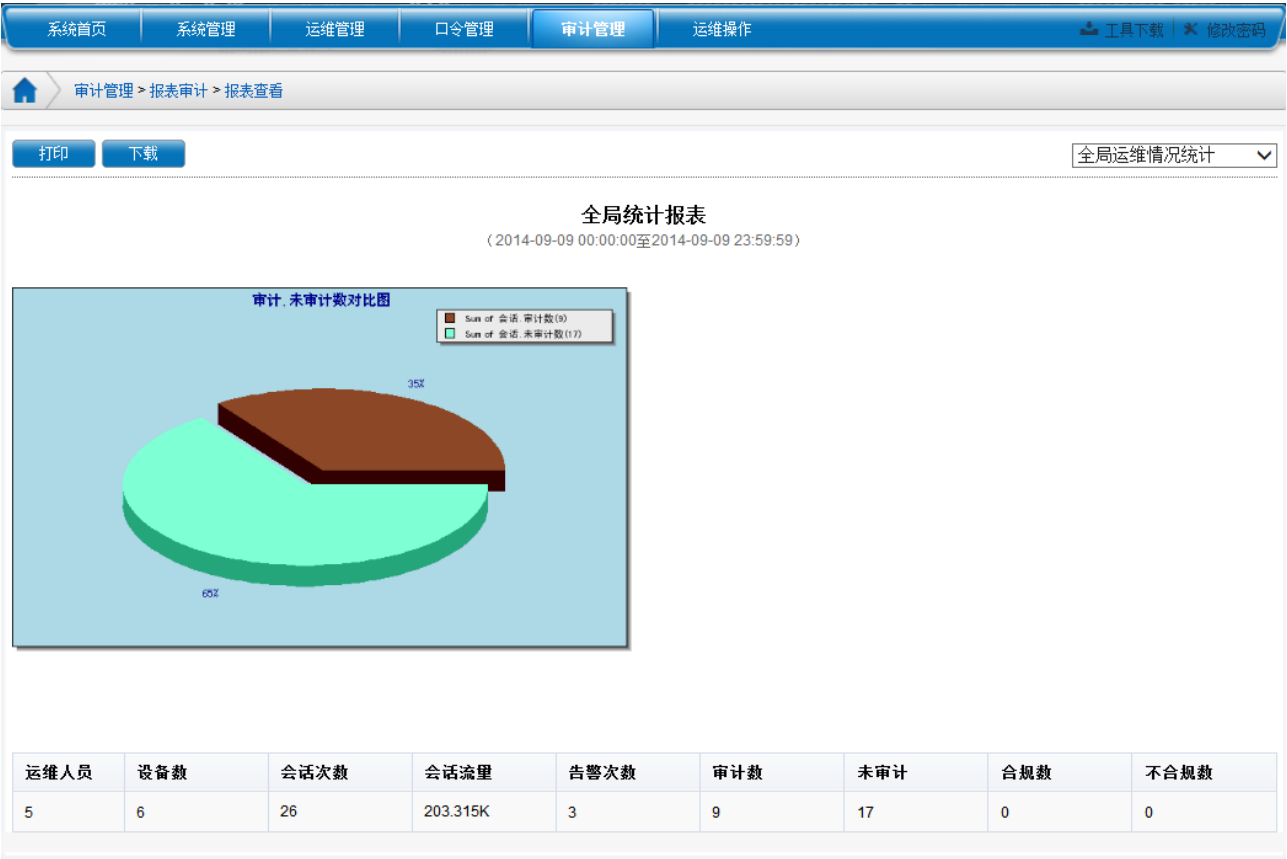
上一步 确定

统计条件:

时间类型: 指定生成报表的时间单位，及时间范围

时间范围: 显示具体的时间范围

点击“生成报表”按钮后，在主窗口中显示报表内容。



可以通过右侧的下拉列表切换不同的报表统计模式，按照时间进行全局统计。



按照设备进行全局统计，如下图所示:

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载 | 设备运维情况统计

全局统计报表

(2014-09-09 00:00:00至2014-09-09 23:59:59)

序号	设备名	协议	服务器IP	会话次数	会话流量	告警次数	审计数	未审计	合规数	不合规数
1	10.10.1.130	ssh	10.10.1.130	8	16.215K	2	1	7	0	0
2	10.10.1.130	telnet	10.10.1.130	6	12.14K	1	4	2	0	0
3	10.10.1.130	vnc	10.10.1.130	1	27.036K	0	0	1	0	0
4	10.10.1.130	xwin	10.10.1.130	1	56.263K	0	1	0	0	0
5	10.10.1.254	telnet	10.10.1.254	4	4.896K	0	0	4	0	0
6	172.16.1.211	telnet	172.16.1.211	1	486byte	0	0	1	0	0
7	172.16.1.217	rdp	172.16.1.217	2	77.509K	0	2	0	0	0
8	172.16.1.241	ftp	172.16.1.241	2	5.68K	0	1	1	0	0
9	172.16.1.254	telnet	172.16.1.254	1	3.103K	0	0	1	0	0

共 9 条信息 首页 < 1/1 > 尾页 1

按照运维帐号全局统计，如下图所示：

系统首页 | 系统管理 | 运维管理 | 口令管理 | **审计管理** | 运维操作 | 工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

打印 | 下载 | 运维帐号运维情况统计

全局统计报表

(2014-09-09 00:00:00至2014-09-09 23:59:59)

序号	运维帐号	姓名	会话次数	会话流量	告警次数	审计数	未审计	合规数	不合规数
1	111		4	10.427K	2	3	1	0	0
2	linzh		1	377byte	0	0	1	0	0
3	xing		5	8.944K	0	1	4	0	0
4	yufc		13	179.803K	1	5	8	0	0
5	zouj		3	3.773K	0	0	3	0	0

共 5 条信息 首页 < 1/1 > 尾页 1

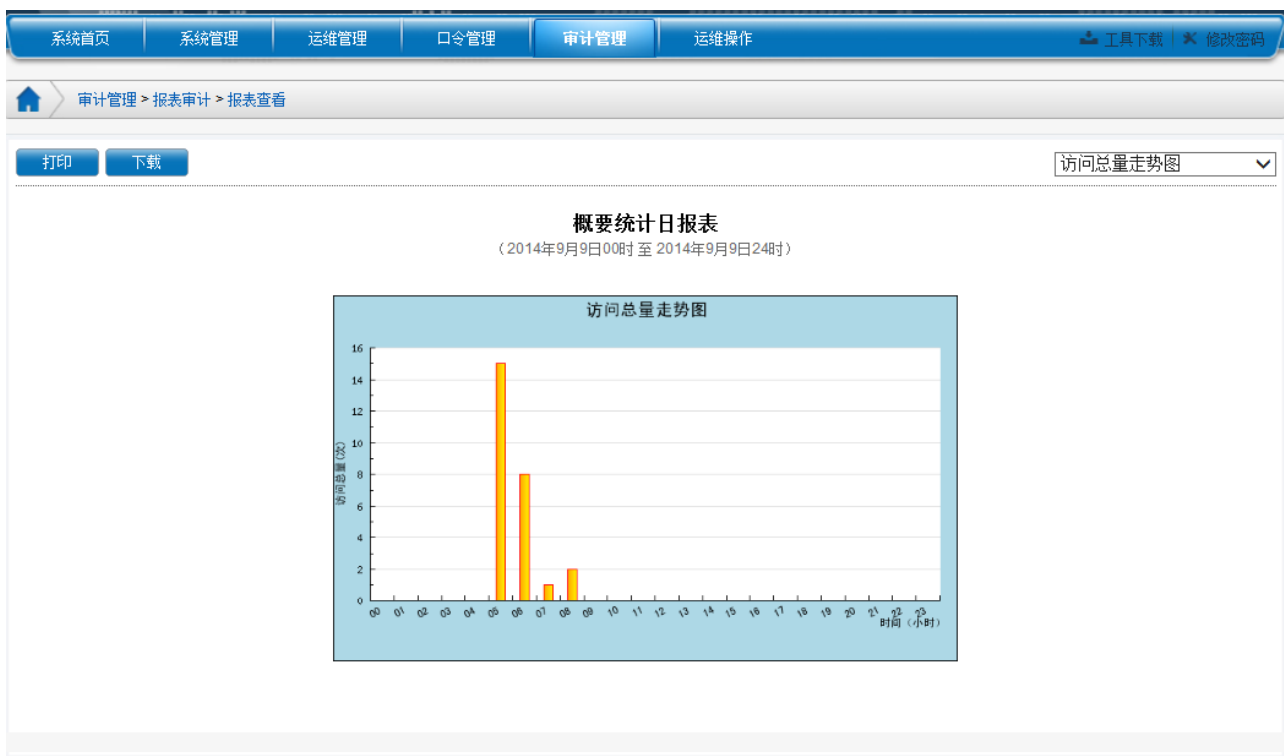
2.6.9 创建会话统计报表

可根据用户选择的时间条件，生成概要统计、用户访问统计、设备访问统计、用户组访问统计、设备组访问统计为分类的报表。例如：



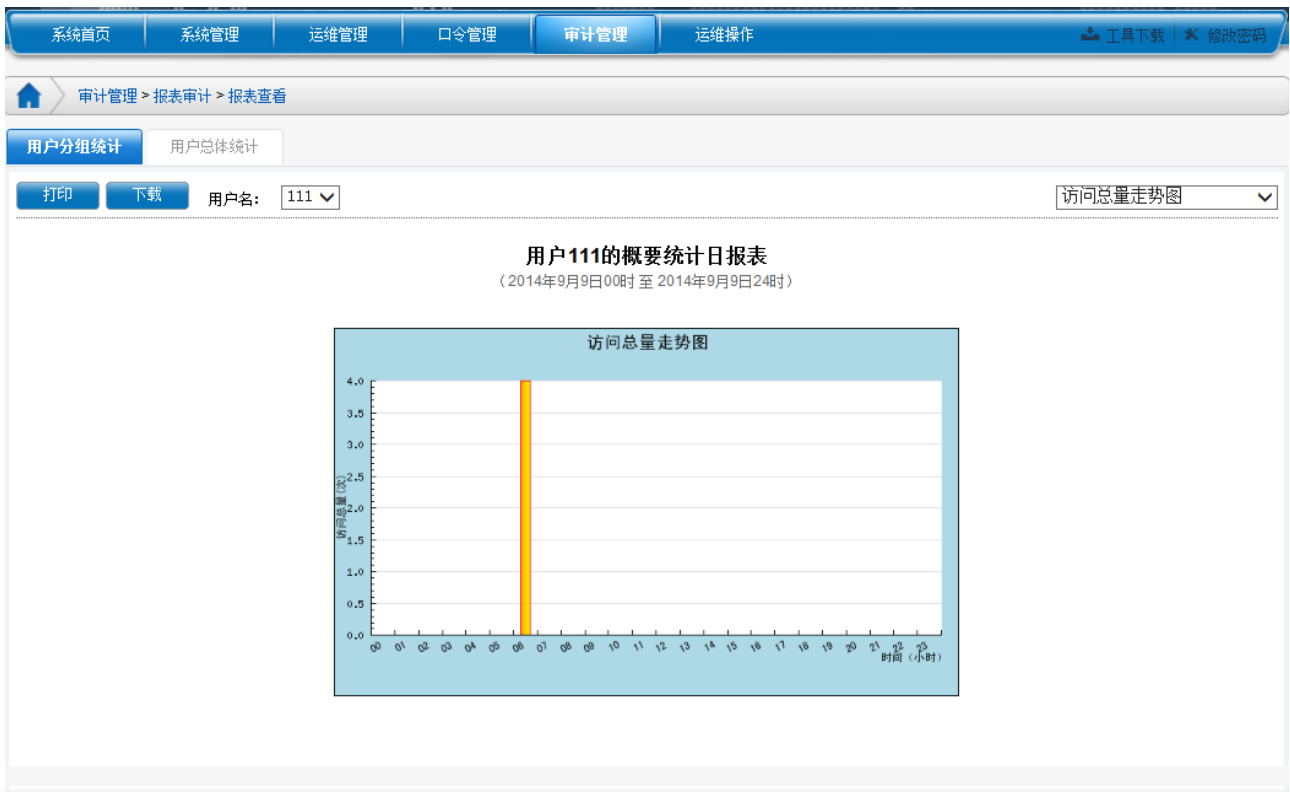
选择“报表类型”后，点击“报表生成”按钮后，生成统计报表。

概要统计日报表，对当日会话进行一总体统计，具体如下图所示：



可以通过右侧的下拉列表切换不同的概要统计内容。

用户概要统计日报表，可针对用户进行分别统计和用户总体统计，具体如下图所示：



其他报表种类生成形式和用户概要统计类似，不一一赘述。

2.6.10 设备日常维护统计报表

对设备日常维护情况进行统计，统计内容包括：用户名、设备名、设备 IP、关键命令、使用次数、系统登录次数、登录总时长等。

选择要在报表中显示的字段，点击“查询条件设置”展开查询条件配置页面，选择用户、设备、协议，及开始、结束时间，点击“确定”按钮。

查询条件设置： 隐藏 (必须配置用户名和设备名)

可引用条件： 无

*用户名： 待选中用户 | 已选中用户

待选中用户： anjw, yangqiao

已选中用户： zdj

*设备名： 待选中设备 | 已选中设备

待选中设备： 1.1.1.1, 10.10.1.113

已选中设备： 10.10.1.130, 10.10.1.61

*协议类型： 全部协议

开始时间： 2015-04-03 00:00:00

结束时间： 2015-04-03 23:59:59

条件数据处理方式： 只应用

上一步 确定

生成设备日常维护统计报表如下图所示：

系统首页 | 系统管理 | 运维管理 | 口令管理 | 审计管理 | 运维操作

工具下载 | 修改密码

审计管理 > 报表审计 > 报表查看

下载

设备日常维护统计报表

(2015-05-01 00:00:00至2015-05-08 23:59:59)

设备日常维护统计报表

用户名	设备名	设备IP	关键命令	使用次数	系统登录次数	登录总时长	首次登录时间	最后登录时间
zdj	10.10.1.130	10.10.1.130		5	10	17分24秒	2015-05-04 18:...	2015-05-06 02:...
			+ exit	1				
			+ [5~vi	...				
zdj	10.10.1.61	10.10.1.61		5	2	45秒	2015-05-04 18:...	2015-05-04 18:...
			d;*a*o*[Tab]...	1				
			ftp> binary	1				

共 2 条信息 首页 < 1/1 > 尾页

选择“下载”，可进行 excel 表格下载



2.7 审计配置

审计配置模块可进行不同审计模块查询条件的配置操作，并进行统一管理，以方便审计员的查询操作，于此同时还可以进行定时报表的配置操作。

2.7.1 条件管理

条件管理：对各审计模块查询条件进行增、删、改、查，进行统一管理，条件类别包括：自定义字段、会话条件管理事件条件管理、告警条件管理、会话报表条件管理、运维操作报表条件管理、帐户分配报表条件管理、管理报表条件管理、告警报表条件管理。

注：各审计员的查询条件为相互独立的，即审计员只能配置并使用自己创建的查询条件。



点击【添加】按钮，可进行条件添加，具体页面如下：



页面会根据选择的类别，进行相应的展示

会话查询自定义字段：进行会话审计列表中字段显示的配置



会话条件管理：会话审计查询条件的配置

[审计管理](#) > [审计配置](#) > [条件管理](#) > [条件添加](#)

*类别:	会话条件管理																																	
*条件名:	<input type="text"/>																																	
会话ID:	<input type="text"/>																																	
*用户名:	<div style="display: flex; justify-content: space-between;"> <div> <input type="text" value="待选中用户"/> <input type="text" value="已选中用户"/> </div> <div style="border: 1px solid gray; padding: 5px;"> <table border="0"> <tr> <td style="border: 1px solid gray; padding: 2px;">hjsx</td> <td style="border: 1px solid gray; padding: 2px;">>></td> <td style="border: 1px solid gray; width: 100px;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">linzh</td> <td style="border: 1px solid gray; padding: 2px;">></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">liu</td> <td style="border: 1px solid gray; padding: 2px;"><</td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">liuxf</td> <td style="border: 1px solid gray; padding: 2px;"><<</td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">qq</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">test0</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">test4</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">xing</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">yufc</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">zouj</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">zz</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> </table> </div> </div>	hjsx	>>		linzh	>		liu	<		liuxf	<<		qq			test0			test4			xing			yufc			zouj			zz		
hjsx	>>																																	
linzh	>																																	
liu	<																																	
liuxf	<<																																	
qq																																		
test0																																		
test4																																		
xing																																		
yufc																																		
zouj																																		
zz																																		
客户IP:	<input type="text"/>																																	
*设备名:	<div style="display: flex; justify-content: space-between;"> <div> <input type="text" value="待选中设备"/> <input type="text" value="已选中设备"/> </div> <div style="border: 1px solid gray; padding: 5px;"> <table border="0"> <tr> <td style="border: 1px solid gray; padding: 2px;">10.10.1.130</td> <td style="border: 1px solid gray; padding: 2px;">>></td> <td style="border: 1px solid gray; width: 100px;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">10.10.1.254</td> <td style="border: 1px solid gray; padding: 2px;">></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">172.16.1.211</td> <td style="border: 1px solid gray; padding: 2px;"><</td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">172.16.1.214</td> <td style="border: 1px solid gray; padding: 2px;"><<</td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">172.16.1.217</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">172.16.1.241</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">172.16.1.254</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">testad.local</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> <tr> <td style="border: 1px solid gray; padding: 2px;">xing</td> <td></td> <td style="border: 1px solid gray;"></td> </tr> </table> </div> </div>	10.10.1.130	>>		10.10.1.254	>		172.16.1.211	<		172.16.1.214	<<		172.16.1.217			172.16.1.241			172.16.1.254			testad.local			xing								
10.10.1.130	>>																																	
10.10.1.254	>																																	
172.16.1.211	<																																	
172.16.1.214	<<																																	
172.16.1.217																																		
172.16.1.241																																		
172.16.1.254																																		
testad.local																																		
xing																																		
*协议类型:	全部协议																																	
开始时间:	2014-09-09 00:00:00																																	
结束时间:	2014-09-09 23:59:59																																	
关键字检索:	<input type="text"/> <input type="checkbox"/> 上行检索 <input type="checkbox"/> 下行检索																																	
会话时长:	<input type="text" value="≥"/> [单位: 分钟] <input type="text" value="≤"/> [单位: 分钟]																																	
*复核人:	任意复核人																																	
*会话是否成功:	任意选项																																	
*会话是否合规:	任意选项																																	

关键字检索:

勾选“上行检索”: 从上行数据中进行检索查询, 包含键盘记录;

勾选“下行检索”: 从下行数据中进行检索查询;

同时勾选“上/下行检索” 则从全文中检索查询。

会话时长:

设置 \geq : 指会话时长大于等于设置的时间的会话;

设置 \leq : 指会话时长小于等于设置的时间的会话;

同时设置 \geq 和 \leq : 指会话时长介于指定时间段的会话;

事件条件管理: 事件审计查询条件的配置

告警条件管理: 告警审计查询条件的配置

会话报表条件管理: 报表审计-创建会话报表, 统计条件的配置

管理报表条件管理：报表审计-创建管理报表，统计条件的配置

告警报表条件管理：报表审计-创建告警报表，统计条件的配置

2.7.2 定时报表

定时报表：对定时发送报表的规则进行配置，包括定时发送报表的时间、报表类型以及文件格式。

支持的文件格式包括：EXCEL、PDF、WORD。

报表类型包括：用户信息报表、资源信息报表、今日会话报表、今日事件报表、会话报表、帐户分配报表、运维操作报表、管理报表、告警报表、审计员操作报表、全局统计报表、会话统计报表。



点击【添加】按钮，可进行定时报表添加，具体页面如下：

