网络卫士安全审计系统
TA-W
使用手册

天融信
TOPSEC®
北京市海淀区上地东路 1 号华控大厦 100085
电话：+8610-82776666
传真：+8610-82776677
服务热线：+8610-8008105119
http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

目　录

1 前言

本手册主要介绍网络卫士安全审计系统（TA-W）的安装、配置、使用和管理。通过阅读本文档，用户可以了解网络卫士安全审计系统的主要功能，并根据实际应用环境安装和配置网络卫士安全审计系统。

1.1文档目的

本文档主要介绍如何配置网络卫士安全审计系统。通过阅读本文档，用户能够正确地配置网络卫士安全审计系统，并综合运用该系统提供的多种安全管理方法，有效地管理网络中的安全设备，实现高效可靠的统一管理。

1.2读者对象

本用户手册适用于具有基本网络知识的系统管理员和网络管理员阅读。

1.3约定

本文档遵循以下约定。

1）命令语法描述采用以下约定：

尖括号（<>）表示该命令参数为必选项。

方括号（[]）表示该命令参数是可选项。

竖线（|）隔开多个相互独立的备选参数。

黑体表示需要用户输入的命令或关键字，例如 **help** 命令。

*斜体*表示需要用户提供实际值的参数。

2）图形界面操作的描述采用以下约定：

“”表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择） **高级管理 > 特殊对象 > 用户**。

文档中出现的提示、警告、说明、示例等，是关于用户在安装和配置网络卫士安全审计系统过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

1.4技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

http://www.topsec.com.cn/

在线技术资料

http://www.topsec.com.cn/support/down.asp

安全解决方案

http://www.topsec.com.cn/solutions/qw.asp

技术支持中心

http://www.topsec.com.cn/support/support.asp

天融信全国安全服务热线

800-810-5119

2 系统简介

本章对网络卫士安全审计系统的系统架构、工作机制以及所涉及的基本概念进行简单介绍。

本章内容主要包括：

- 产品概述：介绍产品的主要功能和适用对象。
- 系统架构：介绍系统的结构及部署。
- 工作机制：介绍系统的基本工作流程。
- 基本概念：介绍本文档所涉及的基本概念。

2.1产品概述

网络卫士安全审计系统是由北京天融信公司自主研发，面向企业级用户，集行为监控与内容审计为一体的产品。它以旁路的方式部署在网络中，不影响网络的性能。网络卫士安全审计系统具有实时的网络数据采集能力、强大的审计分析功能以及智能的信息处理能力。通过使用该系统，可以实现如下目标：

- 监控用户的数据库操作行为、审计用户的网络传输内容。
- 可审计 Sql Server,Oralce,DB2,Sybase 等多种数据库网络协议。
- 实现网络行为后期取证。

该产品适用于对信息保密、非法信息传播/控制比较关心的单位，或需要实施网络行为监控的单位和部门，如政府、军队机关的网络管理部门，公安、保密、司法等国家授权的网络安全监察部门，金融、电信、电力、保险、海关、商检、学校、军工等各行业网络管理中心，以及大中型企业网络管理中心等。

2.2工作机制

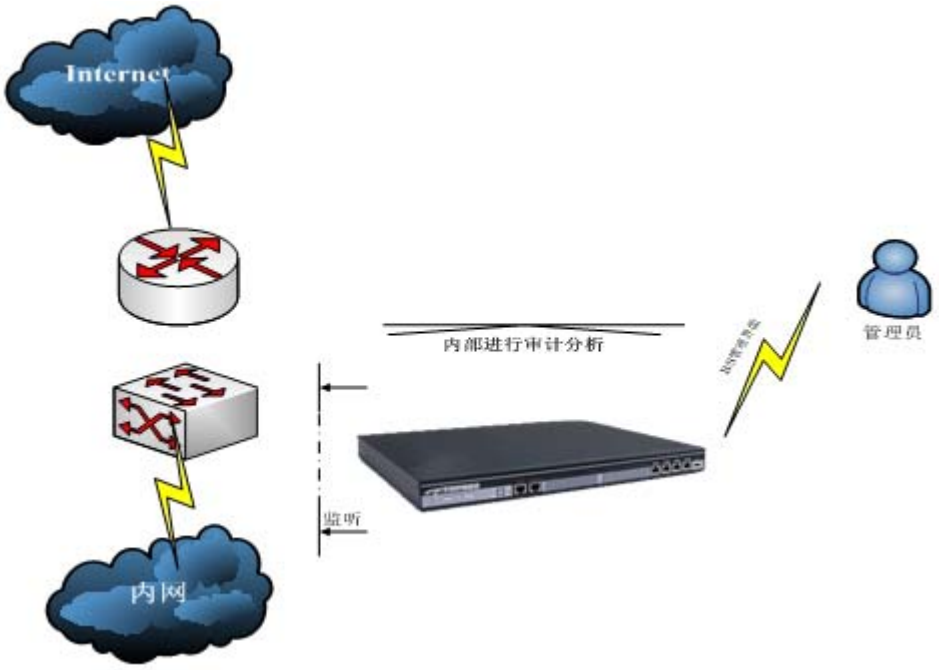


图 2-1 TA-W 审计系统工作机制示意图

在系统开始工作前，管理员需要根据实际应用需求在配置审计引擎的管理口 IP，并设置审计策略。如果没有设置任何策略，则审计引擎将使用默认策略进行行为审计。

审计引擎负责数据采集，并根据已设置的策略进行过滤，分析后将解析结果存储。用户可以通过管理界面对审计引擎进行管理。可以监控、审计已经解析的数据结果，并生成图文报表，以供管理员查询，追踪。

3 安装网络卫士安全审计系统

本章介绍了安装网络卫士安全审计系统（TA-W）前的准备工作，以及物理安装过程。包括如下主要内容：

- 网络卫士安全审计系统的组成与规格
- 配置网络卫士安全审计系统的工作模式
- 网络卫士安全审计系统的安装

3.1系统组成与规格

3.1.1 系统组成

- 网络卫士安全审计系统（硬件）
- 其他配套软件：具体请参见随机光盘的 README.TXT 描述。

3.1.2 系统规格

网络卫士安全审计系统不同型号产品的电源参数、环境规范、物理规格、执行标准和安全规范及标准的内容可能会有所不同。

3.2 硬件设备安装

一般遵循如下步骤安装硬件设备：

1）支架安装

机架式网络卫士安全审计系统采用标准 19 英寸机箱，可以安装固定在标准机柜中。随机附件中有一对上架支架（侧耳），可将其固定在设备上。

2）置于机柜托架上

TA-W 设备要求放在机柜的托架上，并适当调节机柜托架与该设备的相对位置，使其固定支架在垂直方向上受力较小。

3）本地一台管理主机通过 CONSOLE 线缆与网络卫士安全审计系统的 CONSOLE 口连接，供超级管理员进行初步配置。

4）通过电源线连接 TA-W 设备和电源。

5）启动电源（电源开关位于设备后端）。

3.3通过串口连接TA-W

第一次使用网络卫士安全审计系统，管理员可以通过 CONSOLE 口以命令行方式对其进行配置和管理。

1）使用一条串口线（包含在出厂配件中），分别连接计算机的串口（这里假设使用 com1）和 TA-W 的 CONSOLE 口。

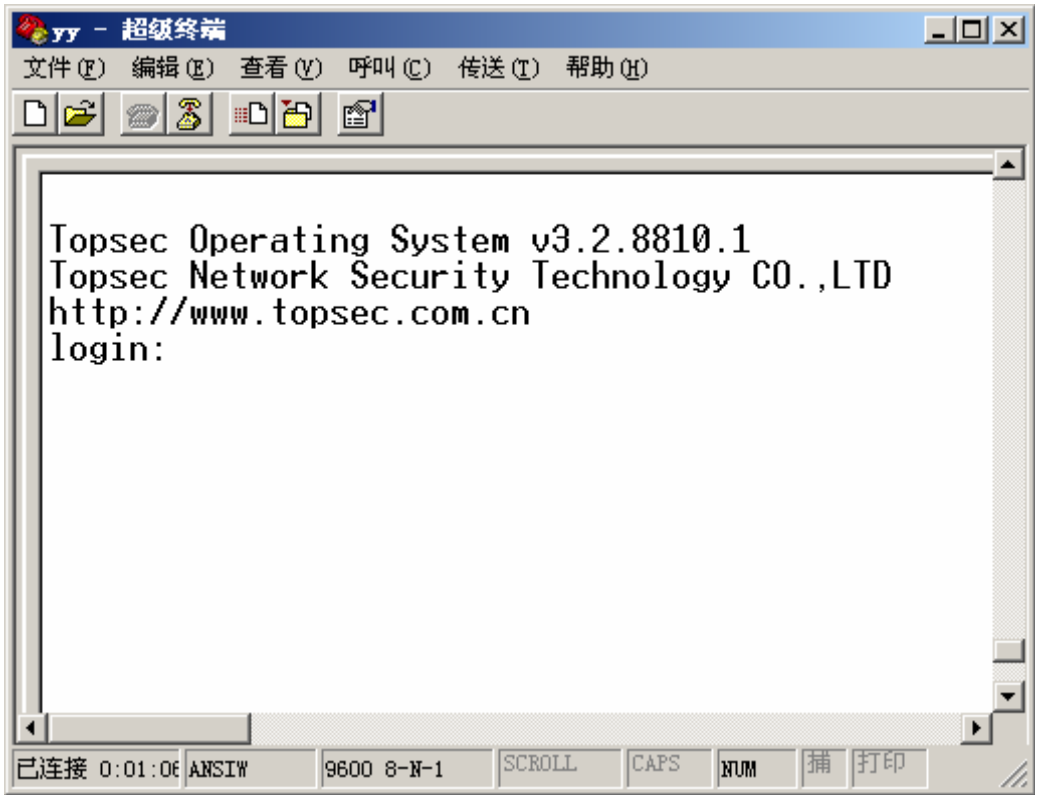
2）选择 **开始 > 程序 > 附件 > 通讯 > 超级终端**，系统提示输入新建连接的名称。

3）输入名称，这里假设名称为“TOPSEC”，点击“确定”后，提示选择使用的接口（假设使用 com1）。

4）设置 com1 口的属性，按照以下参数进行设置。

参数	值
每秒位数	9600
数据位	8
奇偶校验	无
停止位	1

5）成功连接到 TA-W 后，超级终端界面会出现输入用户名/密码的提示，如下图。



6）输入系统默认的用户名：superman 和密码：talent，即可登录到网络卫士安全审计系统。登录后，用户就可使用命令行方式对 TA-W 进行配置管理。

7）运行 cli 命令 **network interface** eth0 **ip add** <*ipaddress*> **mask** <*netmask*>，配置管理口 IP。

运行 **ta interface** <*interface*> **license**， 设置监听口。

运行 **save** 保存配置。

3.4连接TA-W到网络中

连接管理口到网络中，连接监听口到交换机的镜像口。

4 初次使用TA-W

4.1出厂配置

产品出厂配置包括缺省管理用户、缺省空闲超时、缺省系统参数、缺省日志服务器、缺省接口配置、缺省地址对象和访问控制规则。用户可根据实际环境更改出厂配置，具体操作请参照相关章节。

4.1.1 缺省管理用户

TA-W 出厂默认的管理用户：superman，密码 talent。

4.1.2 缺省接口配置

管理口 Eth0，IP：192.168.1.254　netmask：255.255.255.0

缺省抓包口：eth1

4.2 通过CONSOLE口管理TA-W

网络管理员可通过多种方式管理 TA-W。包括通过 CONSOLE 口进行本地管理以及通过 WEBUI 进行远程管理。

第一次使用 TA-W，管理员可以通过 CONSOLE 口以命令行方式进行配置和管理。

通过CONSOLE 口登录到TA-W，可以对TA-W进行一些基本的设置。用户在初次使用TA-W时，通常都会登录到TA-W更改出厂配置（接口、IP 地址等），使在不改变现有网络结构的情况下将TA-W接入网络中。具体操作请参见3.3通过串口连接TA-W。

4.3通过WEBUI管理

本手册将主要介绍如何通过 WEBUI 方式对网络卫士安全审计系统进行管理。

4.3.1 通过浏览器登录TA-W

1）管理员在管理主机的浏览器上输入 TA-W 的管理 URL，例如：http://192.168.1.254，弹出如下的登录页面。

2）输入用户名密码后（TA-W 默认出厂用户名/密码为：superman/talent），点击“登录”，就可以进入管理页面，如下图。

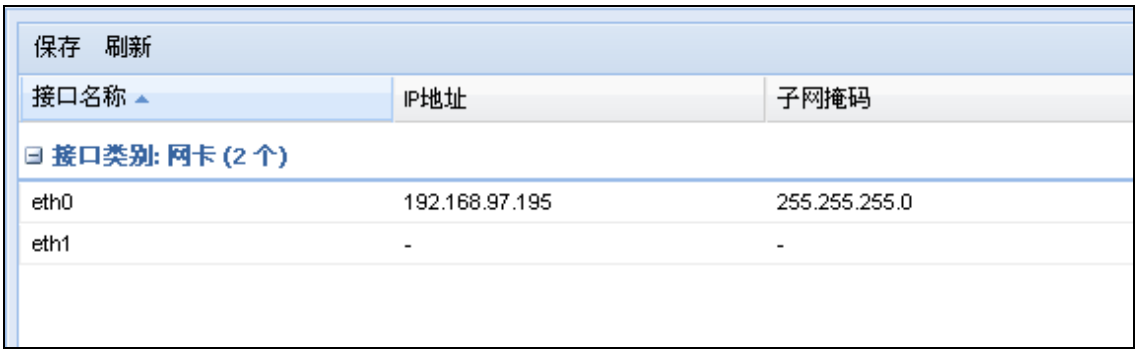
管理界面默认显示系统状态，系统状态页面因 TA－W 型号不同，显示内容略有区别。

3）点击界面右上角的“退出”按钮可以退出登录。

4.3.2 基本配置

4.3.2.1 接口配置

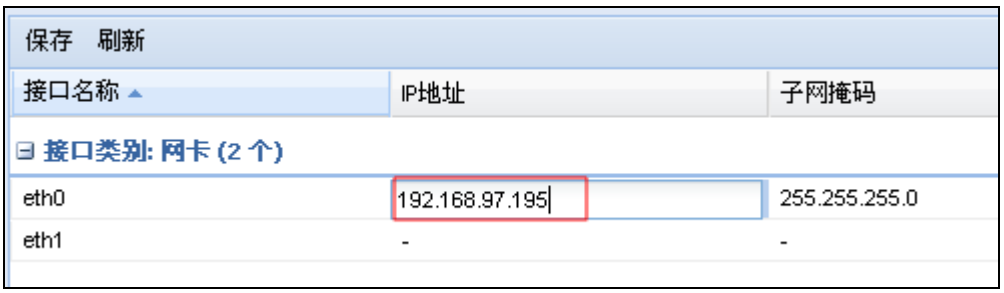
1）在 **系统管理** > **网络配置** > **接口配置** 中可以配置各接口卡的 IP 地址。抓包接口不需要配置 IP。



2）双击接口名称打开接口的配置窗口，如下图。

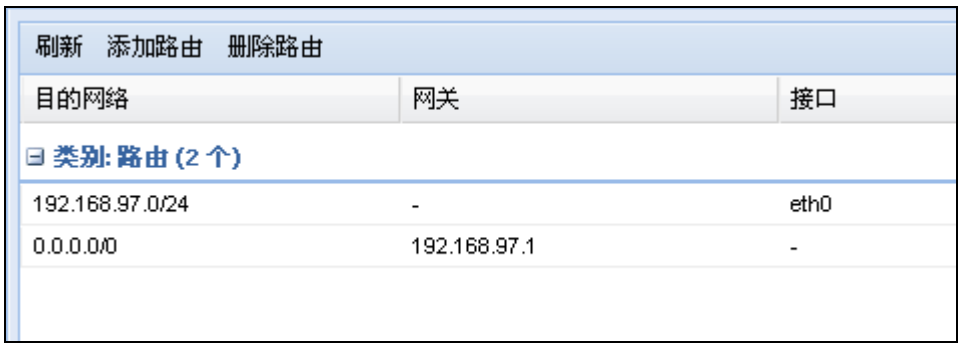
填写接口“IP 地址”和“子网掩码”，点击“保存”后配置便可生效。

用户也可以在列表中双击 IP 或掩码单元格直接更改数据，如下图。



4.3.2.2 路由配置

1）选择 **系统管理** > **网络配置** > **路由配置**，进入如下窗口。

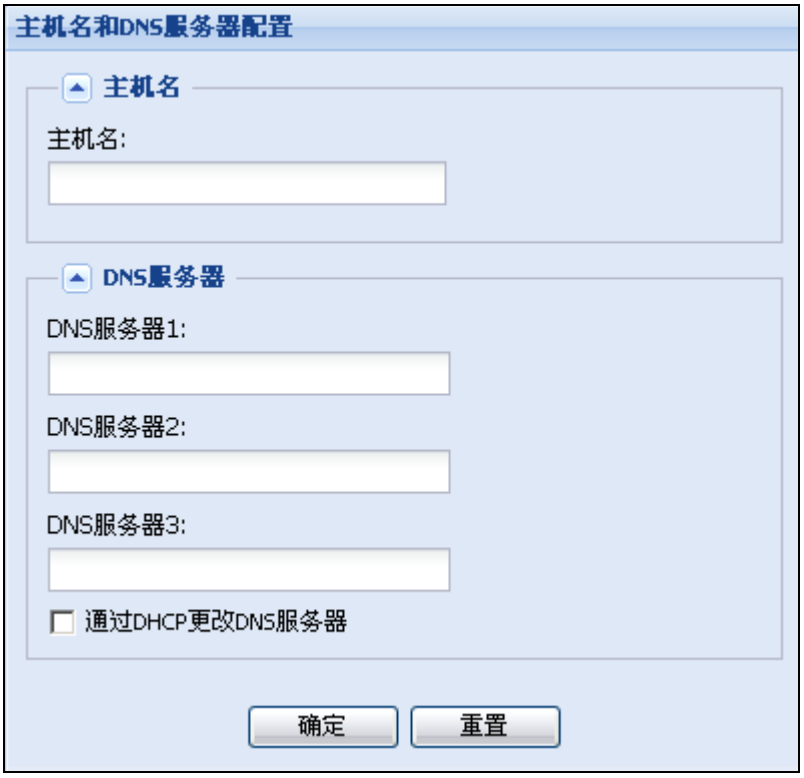


2）点击“添加路由”，显示添加路由窗口，如下图。

可以通过设置“网关地址”或指定“出口网卡”的方式添加路由。

4.3.2.3 DNS与主机名

1）选择 **系统管理 > DNS 服务器配置**，设置 DNS 服务器，如下图。



主机名配置：

填写主机名后点击“确定”配置主机名。

DNS 配置：

填写 DNS 服务器的 IP 地址，最多可填写 3 个 DNS 服务器。DNS 服务器 1 作为主 DNS 服务器。

2）点击“确定”后可配置系统 DNS 服务器。

4.3.2.4 FTP服务器配置

1）选择 **系统管理 > FTP 服务器配置**，将会显示当前已经添加的 FTP 服务器列表，如下图。

FTP 服务器主要用于进行上传/下载备份文件等操作。

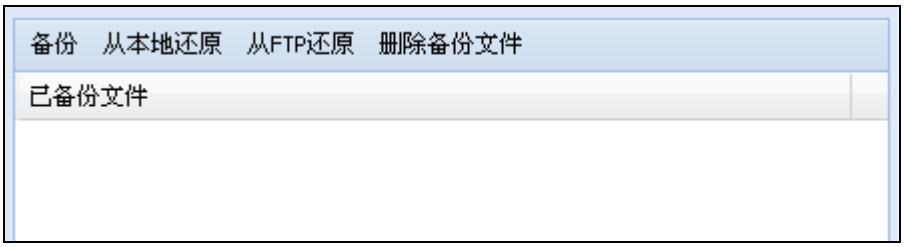
2）选择 **系统管理 > FTP 服务器配置**，并点击“添加”添加 FTP 服务器，如下图。

填写FTP服务器的IP地址、端口（默认为 21）、用户名（默认为anonymous）、密码（默认为taw@topsec.com.cn）、文件路径（默认为/）。 并为新添加的FTP服务器填写一个名称。

3）填写完成后点击“保存”，完成 FTP 服务器的添加。

4.3.2.5 数据备份与还原

1）选择 **系统管理 > 数据备份与还原**，如下图。



备份与还原页面列出了当前系统中已经存在的备份文件。

2）选中一个备份文件，点击“还原”后，系统将在后台开始还原任务。

3）点击“备份”，会打开备份窗口，如下图。

在“备份”处设置要备份最近多少天之内的数据。

如果要把备份文件保存在 FTP 服务器上，请选择要上传的 FTP 服务器的名称。

“备份后删除”表示将数据库中已经备份的数据清除。

点击“备份”按钮后，系统会在后台开始备份任务。

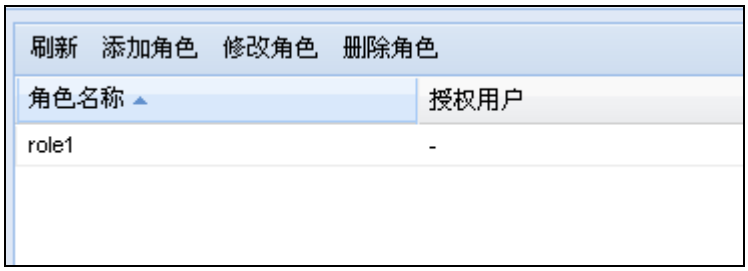
用户可以根据情况选中一个备份文件，然后点击“删除备份文件”，将该备份文件进行删除。这样，可以释放存储空间。

点击“从 FTP 还原”，打开 FTP 还原窗口，选择要下载备份文件的 FTP 服务器，并填写备份文件名，点击确定后，系统会在后台自动下载备份文件并还原。

4.3.3 用户管理

4.3.3.1 角色管理

1）选择 **用户管理** > **角色管理** 打开角色管理界面，如下图所示。



2）点击“添加角色”可以打开添加角色窗口，如下图。

填写“角色名”，如果想把新添加的角色直接指派给某一个用户，则要选择“指定授权用户选项”并在授权用户下拉列表中选择用户。

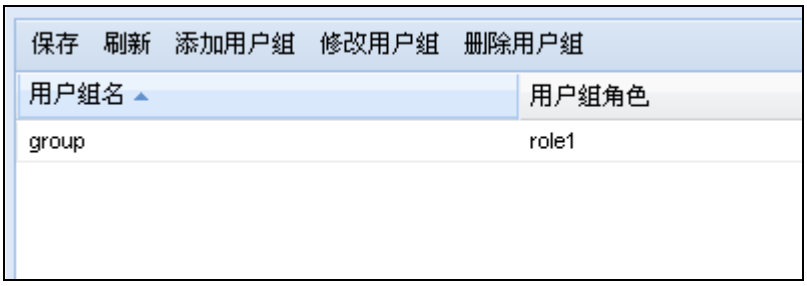
3）配置完成后点击“添加”，以保存新添加的角色。

用户可以通过“删除角色”功能删除已添加的角色。也可通过“修改角色”功能，配置角色的权限。

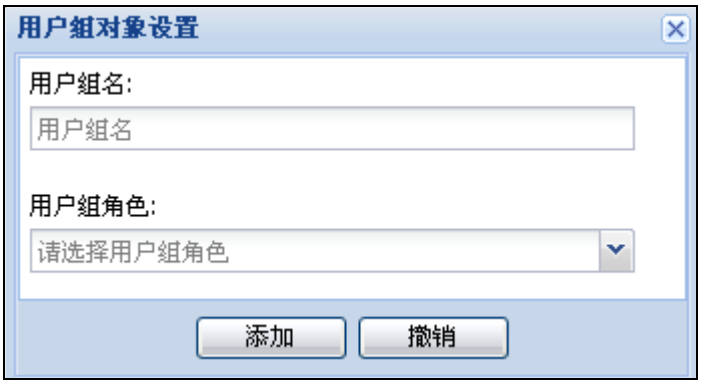
4.3.3.2 用户组管理

TA-W 系统的用户必须属于某一个用户组。

1）选择 **用户管理 > 用户组管理**，进入用户组管理窗口，如下图。



2）点击“添加用户组”，打开添加用户组窗口，如下图。



填写用户组名，并选择用户组的角色。

3）点击“添加”完成用户组添加。

点击“修改用户组”可以修改用户组的角色。也可在用户组列表中双击对应的“用户组角色”文本，更改用户组角色，修改完成后点击“保存”来保存设置。

4.3.3.3 用户管理

1）选择 **用户管理 > 用户管理**，进入用户管理窗口，如下图。

2）点击“添加用户”，弹出添加用户窗口，如下图。

填写用户名、密码和用户的 EMAIL 地址，同时选择用户角色和用户分组。

如果没有选择用户角色，则用户会自动采用用户组的角色。

3）点击“添加”完成用户添加。

点击“修改用户”可以更改除用户名以外的其它所有用户信息。

4.3.4 审计策略

用户可以针对网络情况，配置相关审计策略。通常情况下采用默认的审计策略就可以正常工作，但有时数据库服务器的 TCP 端口会发生改变，这时就需要用户自行配置审计策略。例如，某台 DB2 数据库的端口为 60000，则需要添加一条新的审计策略，设置目

的 IP 为数据库 IP，端口为 60000，协议为 db2，以保证系统可以正确识别数据库的访问操作。

4.3.4.1 主机管理

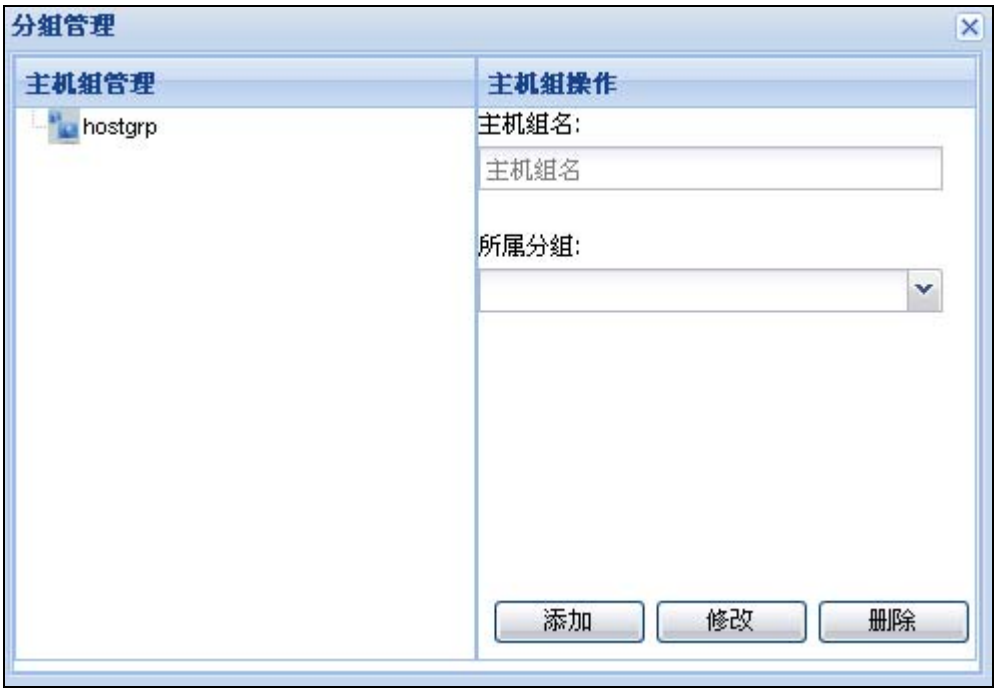
1）选择 **审计策略 > 主机管理**，显示当前主机列表，如下图。

2）点击“添加主机”显示添加主机窗口。

设置主机名、主机 IP 地址（用于系统把审计日志对应到真实主机）、主机 MAC 地址、主机所有人、主机所在分组等信息。

3）设置完成后，点击“保存”，完成主机添加。

4）点击“分组管理”可以进行主机组的添加、删除和更改。



在左侧选择新建主机组的父组，填写主机组名 点击“添加”完成主机组添加。

在左侧主机组树中，选择要更改的主机组，并点击“修改”按钮可以更改分组所属的父组。

在左侧主机组树中，选择要删除的主机组，点击“删除”按钮可以删除该主机组。

选择“全部删除”可以删除该分组中的所有主机对象。

选择“移动到分组”可以把该分组中所有主机移动到目标分组中。

点击“确定”完成主机组的删除操作。

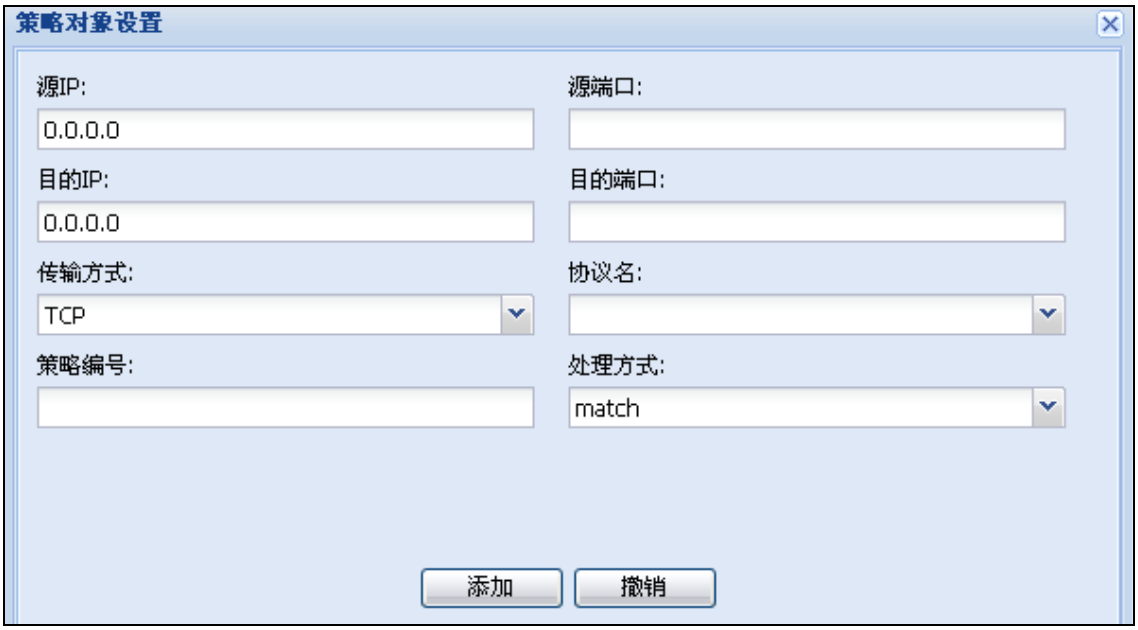
点击“修改主机”可以更改除主机名外的全部信息。

点击“删除主机”可以删除选中的主机对象

4.3.4.2 配置审计策略

1）选择 **审计策略 > 策略管理**，用户可以根据自己网络情况，配置审计规则。

2）点击“添加策略”打开策略添加窗口，如下图。



窗口中各参数的说明请参见下表。

参数	说明
源地址	审计规则的源 IP 地址，默认为所有 IP。
目的地址	审计规则的目的 IP 地址，默认为所有 IP。
源端口	审计规则的源端口，默认为所有端口。
目的端口	审计规则的目的端口，默认为所有端口。
传输方式	设置要审计哪些格式的数据，可选项为 TCP、UDP。
协议名	设置审计哪些协议的数据，可选值为 sqlserver、oracle、sybase、db2。
处理方式	设置是否要对匹配该规则的数据进行审计。可选值为 drop、match、auto，“drop”表示不审计；“match”表示审计，“auto”表示自动匹配协议，进行审计。
策略编号	默认为在现有策略后追加策略，编号越小优先级越高。

3）点击“添加”完成规则添加。

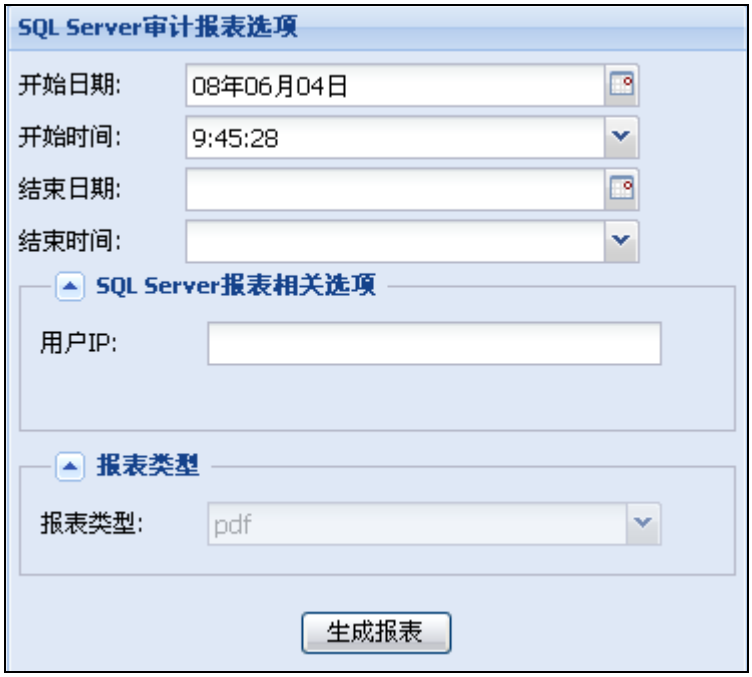
双击策略可以打开策略编辑窗口，可以对审计策略进行更改。

选中策略并点击“策略上移”、“策略下移”可以更改策略优先级（策略移动会改变策略编号）。

4.3.5 审计报表

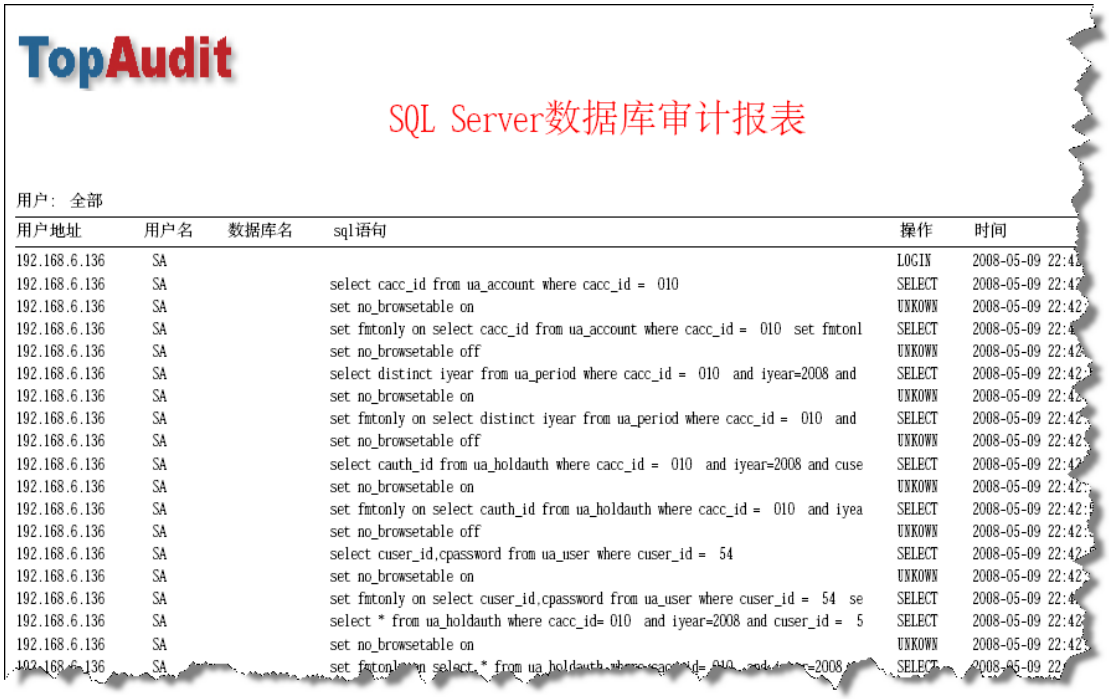
通过 **审计报表**，用户可以选择报表类型：SQL Server 审计报表、Oracle 审计报表、数据库连接审计报表。

“SQL Server 审计报表”设置



设置报表的开始日期、开始时间、结束日期和结束时间。并在“用户 IP”文本框中设置要审计的用户的 IP 地址。

点击“生成报表”按钮后，系统会在新窗口打开生成的 PDF 格式的报表，如下图。



TopAudit

SQL Server数据库审计报表

用户： 全部

用户地址	用户名	数据库名	sql语句	操作	时间
192.168.6.136	SA			LOGIN	2008-05-09 22:43
192.168.6.136	SA		select cacc_id from ua_account where cacc_id = 010	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable on	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		set fmtonly on select cacc_id from ua_account where cacc_id = 010 set fmtonl	SELECT	2008-05-09 22:4
192.168.6.136	SA		set no_browsetable off	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		select distinct iyear from ua_period where cacc_id = 010 and iyear=2008 and	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable on	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		set fmtonly on select distinct iyear from ua_period where cacc_id = 010 and	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable off	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		select cauth_id from ua_holdauth where cacc_id = 010 and iyear=2008 and cuse	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable on	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		set fmtonly on select cauth_id from ua_holdauth where cacc_id = 010 and iyea	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable off	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		select cuser_id,cpassword from ua_user where cuser_id = 54	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable on	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		set fmtonly on select cuser_id,cpassword from ua_user where cuser_id = 54 se	SELECT	2008-05-09 22:4
192.168.6.136	SA		select * from ua_holdauth where cacc_id= 010 and iyear=2008 and cuser_id = 5	SELECT	2008-05-09 22:42
192.168.6.136	SA		set no_browsetable on	UNKOWN	2008-05-09 22:42
192.168.6.136	SA		set fmtonly on select * from ua_holdauth where cacc_id= 010 and iyear=2008	SELECT	2008-05-09 22:

“Oracle 审计报表”和“数据库连接审计报表”的设置与此类似，在此不再赘述。

4.3.6 安全审计

在 **安全审计** 菜单树中选择要审计的数据库类型，便可打开数据库审计选项窗口。“SQL Server”审计，如下图。

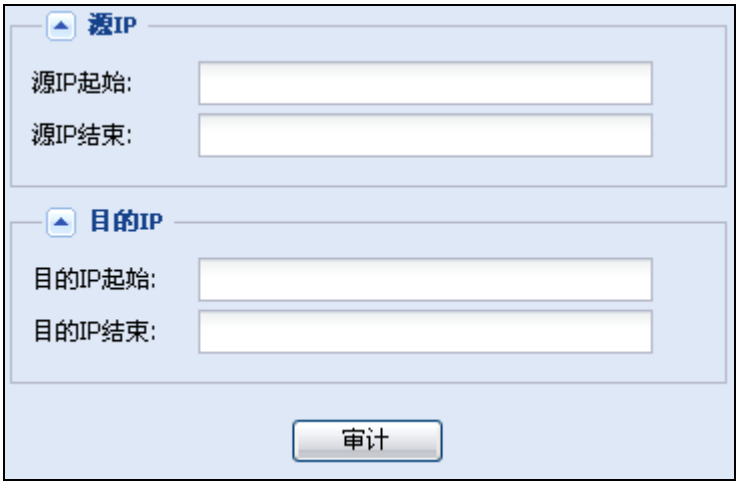
填写审计条件

a）设置审计的开始日期/时间和结束日期/时间。

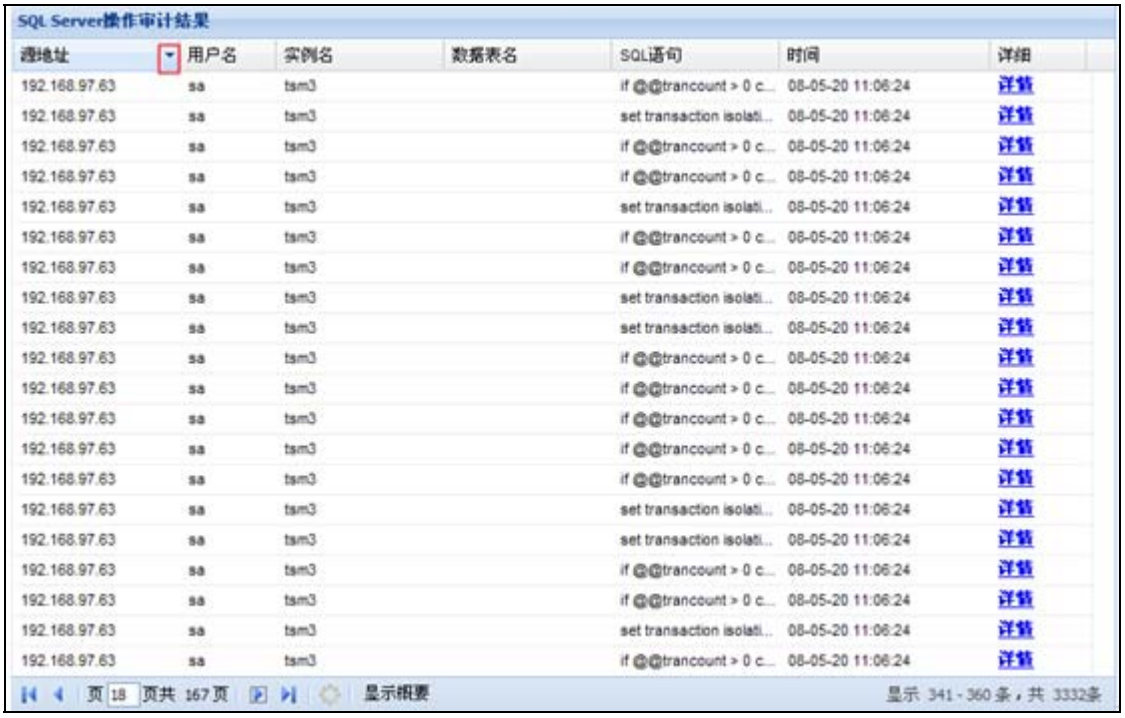
b）设置数据库操作相关选项，用户名、数据库名、数据库表、操作类别等。

数据库操作相关选项中每一项都可以用通配符 * 表示匹配任意字符。如：用户名为“sa”表示审计用户 sa 的所有操作，填写“*sa”则表示审计所有以 sa 结尾的用户的所有操作。

c）点击“源 IP”和“目的 IP”旁边的三角符号，设置源 IP 和结束 IP，如下图。



d）点击“审计”开始显示审计结果，如下图。



用户可以点击每个字段的标题栏进行排序，也可点击字段标题栏右侧的三角图标选择要显示的列。

另外，用户也可通过窗口下方的分页工具栏，对审计信息进行翻页查看。

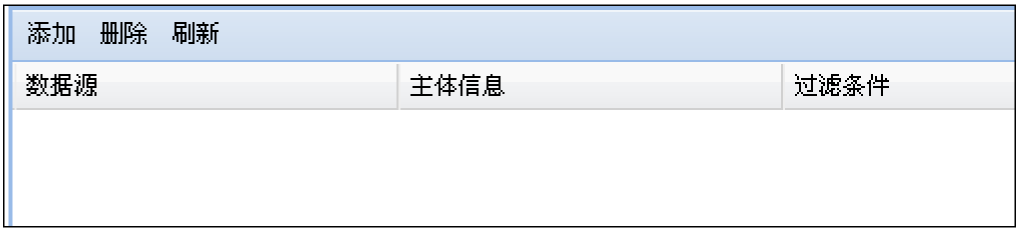
点击“显示概要”将会显示更详细的日志信息。

点击“详情”则可查看数据库连接过程中运行的 SQL 语句，如下图。

4.3.6.1 自定义审计

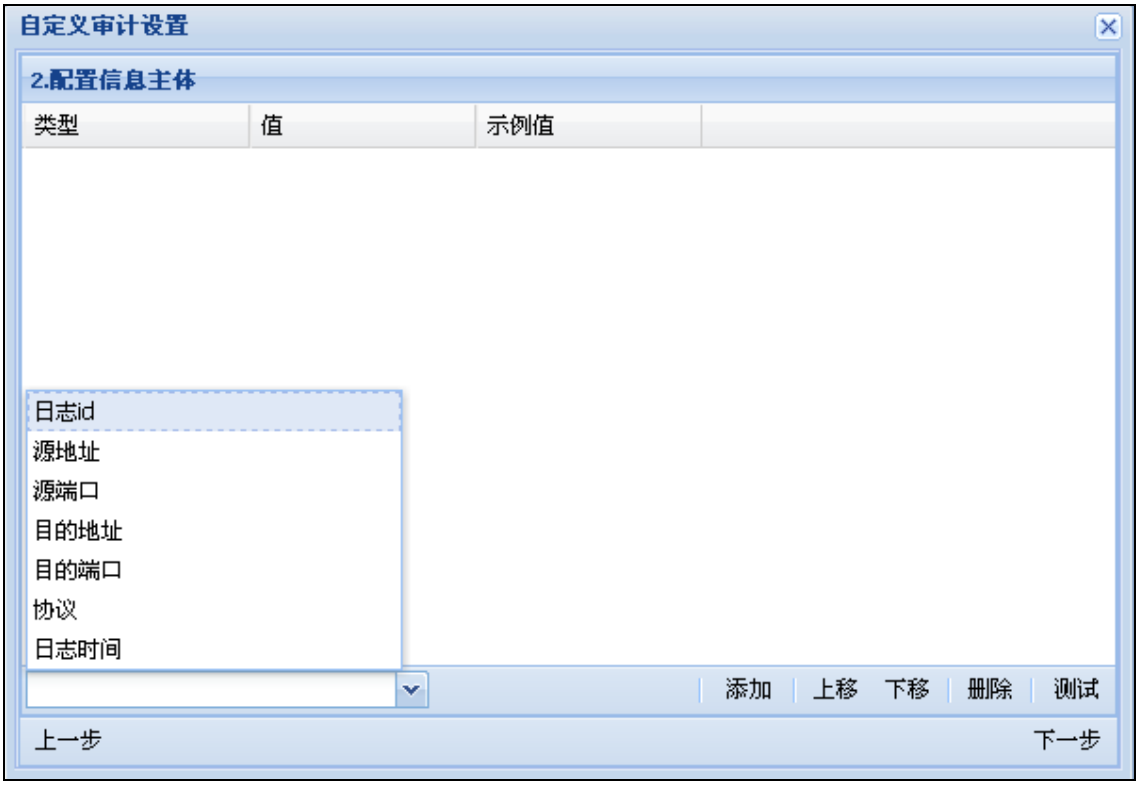
如果用户有较为复杂的审计条件，或常用的审计条件，可以通过自定义审计保存审计条件。

1）选择 **安全审计 > 自定义审计** 打开自定义审计页面，如下图。



2）点击“添加”，添加新的自定义审计，如下图。

3）点击“下一步”选择要显示的主体内容。



4）选择要显示的字段，点击“添加”，该字段将会被添加到信息主体中。如：要查看产生日志的时间则选择“日志时间”，并点击“添加“。

如果要看多个字段可以添加多个，同时可以添加一些字符串连接这些字段。如：有一条日志部分字段为：

源地址：192.168.0.1

日志时间：2008-8-8 08:08:08

目的地址：10.0.0.1

用户希望显示为“192.168.0.1 access 192.168.83.6 at 2008-8-8 08:08:08“，则可以按下图添加主体字段。

点击“测试“可以预览实际运行时的结果。

5）点击“下一步“配置审计条件，如下图。

“添加与条件组合”表示本组合与同级别的其它组合为与关系。

“添加或条件组合”表示本组合与同级别的其它组合为或关系。

选择一个条件组合，并点击“作为与关系添加”会把当前配置的审计条件作为一个与关系添加到所选组合中。

选择一个条件组合 并点击“作为或关系添加”会把当前配置的审计条件作为一个或关系添加到所选组合中。

6）点击“下一步”设置自定义审计的名称。

7）点击“确定”，完成自定义审计的添加。

提示

✧ 如果已有同名的自定义审计，则同名的审计结果会合并后显示。

4.3.6.2 自定义审计结果查看

选择 **我的 TopAudit > 自定义审计通道**，并选择要查看的自定义审计的名称，便可查看自定义审计结果。

4.3.7 实时监控

通过 **实时监控** 中的各级子菜单，可以分别打开各种数据库的实时监控。

源地址	目的地址	用户名	数据库名	数据表名	SQL语句	操作类别	时间
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38
192.168.97.63	192.168.97.156	sa	tsm3		if @@tranco...	UNKOWN	08-05-20 11:21:38

通过“数据库选项”下拉框可以选择要监控的数据库类别。

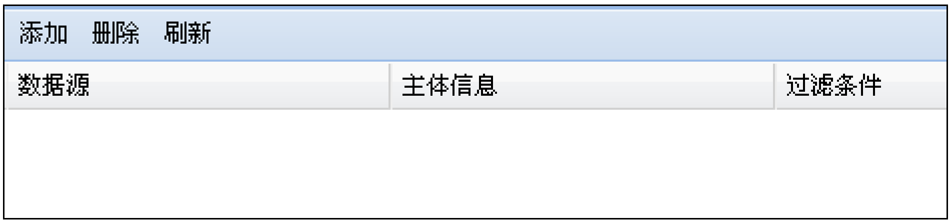
通过“源地址”、“目的地址”则可以设置监控条件。

“显示行数”与刷新时间用于配置监控和刷新状态。

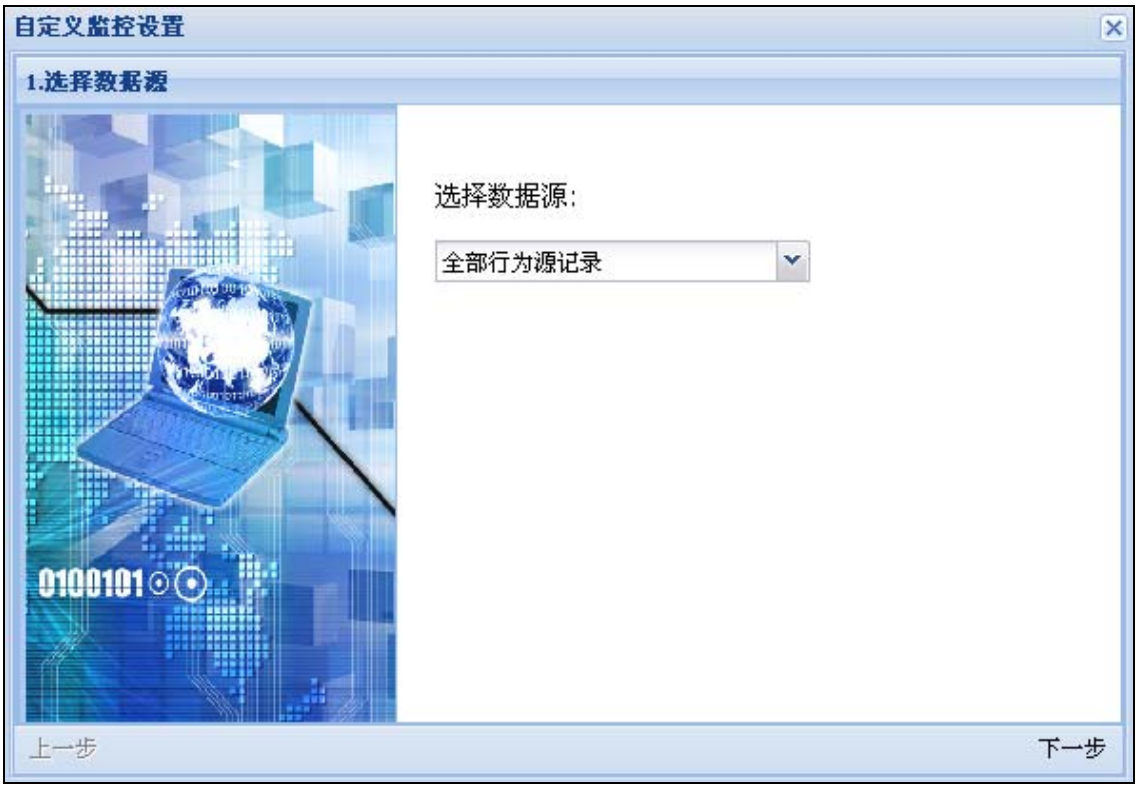
4.3.7.1 自定义监控

如果用户有较为复杂的监控，或常用的监控条件，可以通过自定义监控保存监控条件。

1）选择 **实时监控 > 自定义监控** 打开自定义监控页面，如下图。

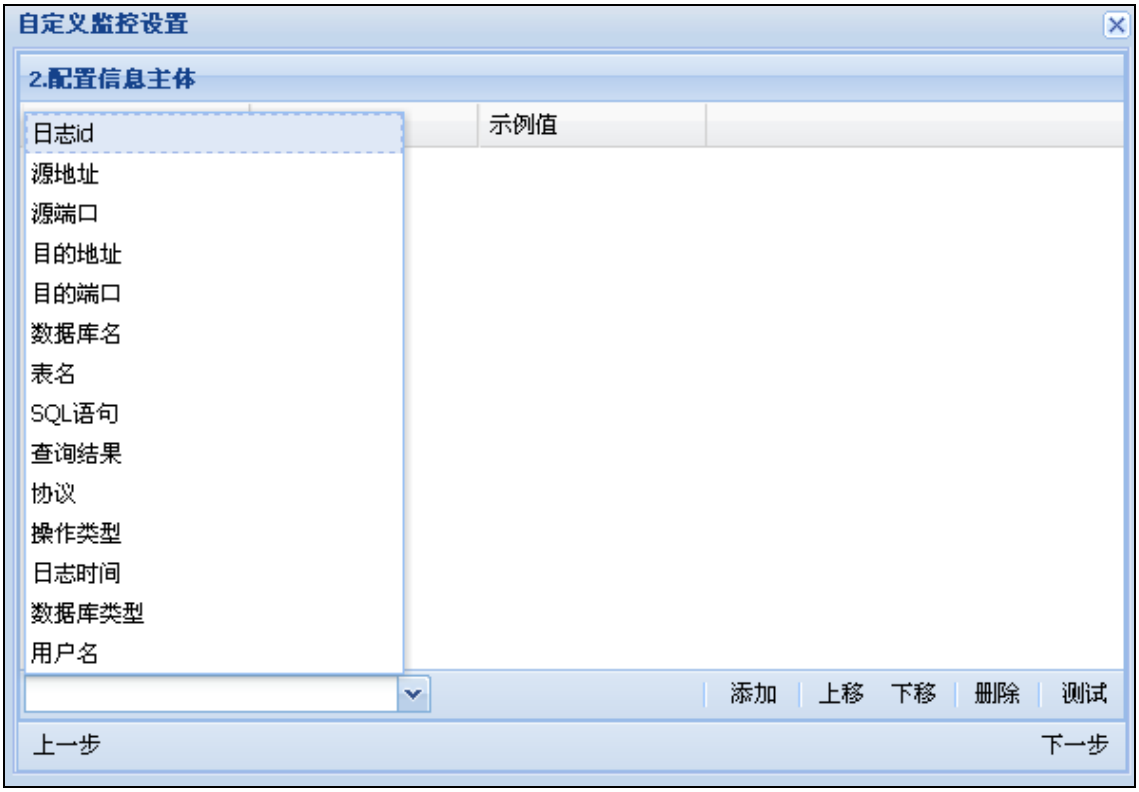


2）点击“添加”，添加新的自定义监控，如下图。



在“选择数据源”处选择要监控的数据类型。

3）点击“下一步”选择要显示的主体内容。



4）选择要显示的字段，点击“添加”，该字段将会被添加到信息主体中。如：要查看产生日志的时间则选择“日志时间”，并点击“添加“。

如果要看多个字段可以添加多个，同时可以添加一些字符串连接这些字段。

点击“测试“可以预览实际运行时的结果。

5）点击“下一步“配置监控条件，如下图。

“添加与条件组合”表示本组合与同级别的其它组合为与关系。

“添加或条件组合”表示本组合与同级别的其它组合为或关系。

选择一个条件组合，并点击“作为与关系添加”会把当前配置的监控条件作为一个与关系添加到所选组合中。

选择一个条件组合 并点击“作为或关系添加”会把当前配置的监控条件作为一个或关系添加到所选组合中。

6）点击“下一步”设置自定义监控的名称。

7）点击“确定”，完成自定义监控的添加。

4.3.7.2 自定义监控结果查看

点击 **我的 TopAudit > 自定义监控通道**，并选择要查看的自定义监控的名称，便可查看自定义监控结果。

附录 A 命令行使用说明

SYSTEM

系统配置。

System devname set *<hostname>*

命令描述：设置系统名称。

参数说明：

hostname	系统名称字符串。

System devname show

命令描述：显示系统名称。

System time set clock *<str>*

命令描述：设置系统时间

参数说明：

str	系统时间字符串,格式为 HH:MM:SS。

System time set date *<str>*

命令描述：设置系统日期

参数说明：

str	系统日期字符串，格式为 YYYY-MM-DD。

System time show

命令描述：显示系统时间日期。

System authset show

命令描述：显示系统用户信息。

System authset add username <*name*> **password** <*password*> **password_again** <*password_second*> **Email** <*email*> **group** <*groupid*> **role** <*roleid*>

命令描述：添加一个系统用户

参数说明：

name	用户名字符串
Password	密码字符串
Password_second	确认密码字符串
Email	用户邮箱字符串
Groupid	用户所在分组 id，数字
Roleid	用户所有的角色 id，即是权限，数字

System authset modify username <*name*> **password** <*password*> **password_again** <*password_second*> **Email** <*email*> **group** <*groupid*> **role** <*roleid*>

命令描述：修改系统用户信息

参数说明：

name	用户名字符串
Password	密码字符串
Password_second	确认密码字符串
Email	用户邮箱字符串
Groupid	用户所在分组 id，数字，该分组必须存在
Roleid	用户所有的角色 id，即是权限，数字，可以为空，为空时用户角色由所在用户组继承。

System authset delete username <*username*>

命令描述：删除系统用户

参数说明：

username	用户名字符串，必须存在

System authset usergroup show

命令描述：显示系统所有的用户组信息。

system authset authgroup add groupname <*groupname*> **role** <*roleid*>

命令描述：添加一个用户分组

参数说明：

groupname	分组名字符串
Roleid	分组角色 id，数字，该角色必须存在

system authset authgroup modify groupname <*groupname*> **role** <*roleid*>

命令描述：修改用户分组信息

参数说明：

groupname	分组名字符串
Roleid	分组角色 id，数字，该角色必须存在

system authset authgroup delete groupname <*groupname*>

命令描述：删除用户分组

参数说明：

groupname	分组名字符串

注意：删除一个用户组会把组里所有用户都删除。

System authset authrole show

命令描述：显示系统所有的角色信息。

System authset authrole add rolename <*rolename*> **username** <*username*> **sysconfig** <*sysconfig*> **userconfig** <*userconfig*> **auditconfig** <*auditconfig*> **logconfig** <*logconfig*>

命令描述：添加一个角色

参数说明：

rolename	角色名字符串
Username	继承用户名字符串，可以为空；不为空时必须和角色名一致，角色的权限由用户继承，该用户必须存在
Sysconfig	是否有系统配置权限，数字 0 或 1
userconfig	是否有用户配置权限，数字 0 或 1
auditconfig	是否有系统审计权限，数字 0 或 1
logconfig	是否有系统日志查看权限，数字 0 或 1

system authset authrole modify oldname <*oldname*> **newname** <*newname*>

命令描述：修改用户角色名称

参数说明：

oldname	原来的角色名，字符串

Newname	新的角色名，字符串

system authset authrole delete rolename <*rolename*>

命令描述：删除一个用户角色

参数说明：

rolename	用户角色字符串，该角色必须存在

注意：如果该角色被授权予用户，则该角色不能被删除。

system ftp_server list

命令描述：显示系统所有的 FTP 服务信息。

system ftp_server add servername <*servername*> **ip** <*ip*> **port** <*port*> **name** <*name*> **password** <*password*> **path** <*path*>

命令描述：添加一个 FTP 服务

参数说明：

servername	FTP 服务名字符串，唯一标识
Ip	FTP 服务器 IP，IP 地址
Port	FTP 服务器端口，数字，为空时默认为 21
Name	用户名字符串，为空时默认为 anonymous
Password	用户密码字符串，为空时默认为taw@topsec.com.cn;
Path	路径字符串

system ftp_server modif servername <*servername*> **ip** <*ip*> **port** <*port*> **name** <*name*> **password** <*password*> **path** <*path*>

命令描述：修改 FTP 服务信息

参数说明：

servername	FTP 服务名字符串，必须存在
Ip	FTP 服务器 IP，IP 地址
Port	FTP 服务器端口，数字，为空时默认为 21
Name	用户名字符串，为空时默认为 anonymous
Password	用户密码字符串，为空时默认为taw@topsec.com.cn;
Path	路径字符串

system ftp_server delete servername <*servername*>

命令描述：删除一个 FTP 服务信息

参数说明：

servername	FTP 服务名字符串，必须存在

system smtp_server list

命令描述：显示系统所有的 SMTP 服务信息。

System ftp_server add ip <*ip*> **port** <*port*> **name** <*name*> **password** <*password*>

命令描述：添加一个 SMTP 服务

参数说明：

Ip	SMTP 服务器 IP，IP 地址
Port	SMTP 服务器端口，数字，为空时默认为 25
Name	用户名字符串，不能为空
Password	用户密码字符串，不能为空

system ftp_server modif ip <*ip*> **port** <*port*> **name** <*name*> **password** <*password*>

命令描述：修改 SMTP 服务信息

参数说明：

Ip	SMTP 服务器 IP，IP 地址，必须存在
Port	SMTP 服务器端口，数字，为空时默认为 25
Name	用户名字符串，不能为空
Password	用户密码字符串，不能为空

system smtp_server delete ip <*ip*>

命令描述：删除一个 SMTP 服务信息

参数说明：

ip	SMTP 服务器 IP，IP 地址，必须存在

NETWORK

网络配置

network dns show <*dnsname*>

命令描述：显示系统 DNS 服务器

参数说明：

dnsname	可选，dns 名字字符串，dns1，dns2 或 dns3

network dns set dns1 <*dns1*> [**dns2** <*dns2*> [**dns3** <*dns3*>]]

命令描述：设置系统 DNS 服务器，最多 3 个。

参数说明：

Dns1	dns1 的 IP 地址
Dns2	dns2 的 IP 地址
Dns3	dns3 的 IP 地址

network interface list

命令描述：显示系统网卡概括信息。

network interface show

命令描述：显示系统网卡具体信息。

network interface <*dev*> **shutdown**

命令描述：关闭系统网卡

参数说明：

dev	所要关闭的系统网卡名字符串，eth0，eth1 等

network interface <*dev*> **up**

命令描述：启用系统网卡

参数说明：

dev	所要启用的系统网卡名字符串，eth0，eth1 等

network interface <*dev*> **ip add** <*ipstr*> **mask** <*maskstr*>

命令描述：为网卡配置地址

参数说明：

dev	所要配置的网卡名字符串，如 eth0，eth1

ipstr	网卡 IP 地址
maskstr	网卡掩码

network interface <*dec*> **ip modify** <*ipstr*> **mask** <*maskstr*>

命令描述：修改网卡地址

参数说明：

dev	所要配置的网卡名字符串，如 eth0，eth1
ipstr	网卡 IP 地址
maskstr	网卡掩码

network interface <*dev*> **ip delete** <*ipstr*>

命令描述：删除网卡地址

参数说明：

dev	所要配置的网卡名字符串，如 eth0，eth1
ipstr	所要删除的网卡 IP 地址。

network route list

命令描述：显示系统路由。

network route add dst <*dipstr*> **var** <*str*> **metric** <*num*> **dev** <*devnum*>

命令描述：添加一条路由；

参数说明：

dipstr	目的 IP 地址；
Str	网关地址；
Num	路由度量值，数字
dev	指定接口字符串，如 eth0，eth1。

network route delete dst <*dipstr*> **var** <*str*> **metric** <*num*> **dev** <*devnum*>

命令描述：添加一条路由

参数说明：

dipstr	目的 IP 地址；
Str	网关地址；
Num	路由度量值，数字

dev	指定接口字符串，如 eth0，eth1。

TA

TA 其他配置

ta interface *<dev>* **listen**

命令描述：监听口配置

参数说明：

dev	指定监听接口字符串，如 eth0，eth1

ta auto_protocol show

命令描述：显示所有匹配协议。

ta policy show

命令描述：显示所有策略。

ta policy add *<src>* *<sport>* *<dst>* *<dport>* *<transmit>* *<protocol>* *<deal>* *<pid>*

命令描述：添加一条策略

参数说明：

src	源 IP，IP 地址，为空时默认为“0.0.0.0”，表示所有 IP
sport	源端口，数字，可以为空
dst	目的 IP，IP 地址，为空时默认为“0.0.0.0”，表示所有 IP
dport	目的端口，数字，可以为空
transmit	传输方式，“TCP”或者“UDP”，不能为空
protocol	协议名字符串
deal	处理方式，可以为空
pid	策略号 id，数字，可以为空

ta policy delete *<src>*

命令描述：根据源 IP 删除一条策略

参数说明：

src	源 IP，IP 地址

ta policy delete pid <*pid*>

命令描述：根据策略 ID 号删除一条策略

参数说明：

pid	策略 ID 号，数字，必须存在

ta protocol <*protocol*> **auto**

命令描述：自动匹配协议

参数说明：

protocol	自动匹配的协议名字符串，协议名必须存在协议表里

ta protocol <*protocol*> **nonauto**

命令描述：取消自动匹配协议

参数说明：

protocol	取消自动匹配的协议名字符串，协议名必须存在自动匹配协议表里

声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。

3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。

4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。