毕方数据库安全审计系统

用户手册-V1.0

北京携推信息技术有限公司

2019 年 12 月

声明

本文档所提到的产品信息仅供参考，有关内容可能会随时更新，北京携推信息技术有限公司恕不另行通知。

1．本文档中提到的产品功能、性能、规格可能因产品具体型号、应用环境、配置方法不同而有所差异，此类差异为正常现象，相关问题请咨询北京携推信息技术有限公司

2．本文档包含了毕方数据库安全审计系统的硬件上架安装、快速使用指南、系统功能配置以及 FAQ 等内容。手册中涉及相关文档、文字内容、标识等信息均受版权保护，手册的任何部分未经许可均不得复制或者传播，违者必究。

3．本手册适用于毕方数据库安全审计系统的最终用户。

目 录

1 术语和缩写

数据库审计

数据库审计是通过记录数据库的操作行为作为审计记录，反映出数据库被使用的状况；数据库审计支持通过网络访问方式把对数据库的操作及内容进行实时的监控审计。

审计类型

审计类型指数据库审计系统支持的各种类型，包括数据库类型（Oracle、DB2、MSSql、MySql、Sybase、Infomix）、数据库运维类型（Ssh、Ftp、Telnet）以及 web 中间件类型。

数据库 sql 操作类型

数据库审计支持的 sql 操作类型，包括

- 插入操作（Insert）
  - 数据插入操作（INSERT， SELECT … INTO）
  - 新建数据表、数据库、视图、索引等操作（CREATE TABLE，CREATE DATABASE，CREATE VIEW， CREATE INDEX， …）
- 查询操作（Select）
  - 数据查询操作（SELECT）
  - 数据表结构查询操作（show/desc）
- 删除操作（Delete）
  - 删除数据操作（DELETE， TRUNCATE TABLE， TRUNCATE DATABASE， …）

    - 删除数据表、数据库、视图、索引等操作（DROP TABLE， DROP DATABASE，DROP VIEW， DROP INDEX， ...）
- 更新操作（Update）
    - 数据更新操作（UPDATE）
    - 数据表结构更新操作（ALTER， RENAME ... TO ...， MERGE INTO ... USING ...）
- 用户访问（Access）
    - 用户登录
- 特权操作（Privilege）
    - 用户权限改变（GRANT， DENY， REVOKE）
    - 用户建立与删除
    - 备份与恢复操作（BACKUP， RESTORE）
    - 事务操作（COMMIT， ROLLBACK TO）
- 数据库特有操作
    - Microsoft SQL Server 特有操作：DBCC，SP_*， OPENDATASOURCE， ...
    - ORALCE 特有操作
- 其他操作
    - 特定字符串审计

数据库运维审计

数据库运维是针对用户数据库的软件安装、配置、备份及实施，数据恢复、迁移，故障排除、预防性巡检等一系列服务；数据库运维审计是对通过远程访问方式，对数据库进行运维操作的行为及内容审计，如 telnet、ftp、ssh 等。

Web 中间件审计

web 中间件泛指客户端访问 web 应用服务器，web 应用服务器再访问数据库的应用环境中的 web 应用服务；web 中间件审计支持对客户端访问 web 应用服务器的行为及内容的审计，同时支持客户端访问 web 应用服务器和 web 应用服务器访问数据库关联行为及内容的审计。

审计服务器

审计服务器指数据库服务器、数据库运维服务器以及 web 中间件服务器。

审计客户端

审计客户端指访问审计服务器的用户终端。

审计记录

用户访问审计服务器产生的每一个 sql 操作、运维操作或者 web 访问记录下来的行为及内容作为一条审计记录。

自身日志

自身日志指数据库审计系统的配置或状态的变更时生成的记录。

AMC

AMC 是审计管理中心（Audit Management Center）的简写，它实现了产品功能服务层面的功能，其目标是对安全产品的管理。

探针

探针是数据库审计系统用于采集各种审计数据的分布式模块。探针和 AMC 一体安装。

策略

对监控数据进行处理，生成审计记录以及执行某种操作的集合。

数据转储

数据转储指将数据库审计系统的审计记录，导出转存到系统之外的空间，并能通过手段查询转存到系统外的历史记录的功能。

TAP 设备

TAP 是分路器设备，提供网络流量的副本，以便进行实时监控和分析；接口分为电口和光接口。

2 产品简介

2.1 产品背景

萨班斯法案（SOX）诞生之日起，为数不少的安全公司就已经预测到数据安全审计将成为企业无法回避的问题。只要是正规的企业，都无法回避自身的数据安全问题。当

然，上市公司就更加需要重视。事实上，这里所说的数据库安全审计，不仅包括了数据源的安全，而且也涵盖了审计方法与企业 IT 流程的结合。

数据库是每个企业数据管理的基础，尽管这些系统的数据完整性和安全性是相当重要的，但对数据库采取的安全检查措施的级别还比不上操作系统和网络的安全检查措施的级别。许多因素都可能破坏数据的完整性并导致非法访问，这些因素包括密码安全性较差、误配置、未被察觉的系统后门以及自适应数据库安全方法的强制性常规使用等。

针对以上破坏数据完整性的威胁都来自于数据库本身的安全策略的漏洞和使用方面的问题，然而对于数据库合法用户的违规操作，以及内部用户对数据资源的故意泄露或破坏等问题，对企业带来的危害会更加严重，损失也会相当巨大。当然，数据库系统本身会提供一些日志审计功能，但是想要审计较为细致的操作日志就必然要影响到数据库服务器的性能，一般应用数据库的企业用户 ，都不愿意开设多一些的日志审计功能，这样必然会对数据库的安全埋下了安全隐患。

当产生数据安全问题时，为了寻找案件线索，执法机构需要从网络上寻找犯罪嫌疑人的活动和留下的痕迹并获取可靠的犯罪证据，对于侦破犯罪案件，保障社会稳定，维护公民利益具有十分重要的意义。

因此，安全管理要从网络系统安全和应用安全两个方面推进，才能有效地全面解决安全问题。数据库网络安全审计是网络安全管理工作中的一个重要组成部分，它可以通过对网络数据库的‘信息活动”实时地进行监控审计，使管理者对网络数据库的‘信息活动”一目了然，能够及时掌握数据库服务器的应用情况，及时发现客户端的使用问题，存在着哪些安全问题和隐患并予以纠正，预防应用安全事件的发生，即便发生了也能够可以快速查证并追根寻源。

2.2 产品特点

毕方数据库安全审计系统是集数据库审计、数据库安全检测、数据库优化分析三大功能为一体的综合监控审计系统。该系统采用网络旁路实时侦听方式，全线速采集网络上所有会话流，对网络中的各种应用行为和应用内容进行监控、报警、记录。

数据库审计系统不参与被监控网络的数据传输活动，因此不对网络结构和性能产生任何影响，具有很好的透明性和安全性。

2.3 产品功能

数据库操作和数据库运维监控、审计、报警

能够对网络数据库的各种操作进行记录审计并报警，提供详细的审计信息（4W：何时 When 、何地 Where 、何人 Who 以及何种行为 What）查询功能和邮件、syslog 报警方式。同时提供多种审计条件，实现分类审计或组合审计。

数据库事件审计分析

能够对网络数据库接收发送的流量包数进行统计，并提供详细的统计条件（如：时间、IP 地址、操作类型等）。

攻击监测

能够对网络中对数据库、操作系统、运维行为的攻击进行监测，并记录攻击行为特征。

日志信息查询

能够对网络中其他设备发来的 syslog 和 SNMP 日志信息进行接收和查询，并提供多种查询条件，实现分类或组合查询。

报表系统

可以实现手动报表和自动定制报表邮件发送功能。同时提供灵活的可定制报表和 doc、html 和 pdf 多种报表格式。

系统状态配置、查看

可以通过界面查看系统状态、进行系统管理。

数据保护

拥有数据存储区磁盘空间预警和数据保护功能。在数据存储区磁盘空间使用率达到预设的预警阀值时通过界面显示和邮件方式实现预警，达到预设的保护阀值时根据设定的数据保护机制采取相应的处理对审计数据进行保护。

自身日志

支持完善的自身日志记录和查询功能。

补丁升级

可以通过界面上传补丁包进行补丁的升级和卸载。

用户/角色权限管理

实现用户权限三权分立，支持基于用户、产品功能模块和内容访问三级的权限管理。

3 硬件安装

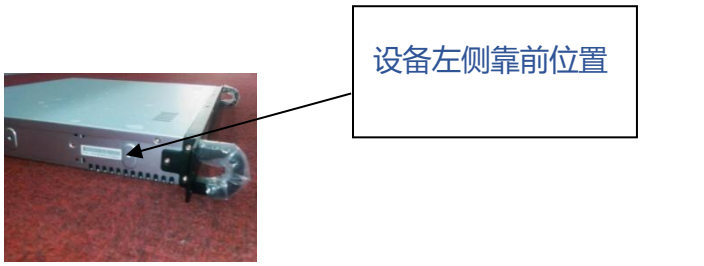
3.1 拆箱检查

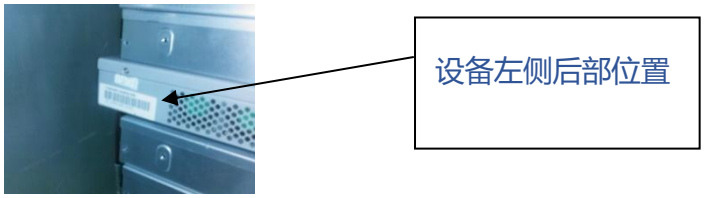
在打开包装之后，请您先检查随机附带的电源线、网线、随机光盘等附件是否齐全，所有部件请对照装箱单进行检查，如有缺损请及时和销售人员联系。

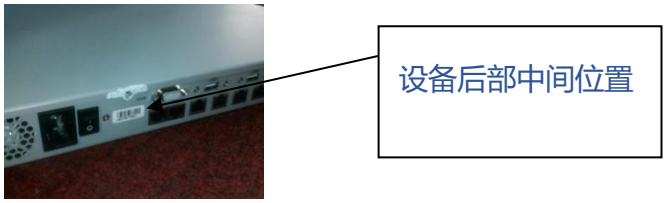
注意：取出设备后，不要将外包装丢弃，在需要搬运时，请务必使用原包装，它是为您的审计设备专门设计的包装，具备良好的防震功能。

物 品 名 称	数量
数据库审计设备	1
电源线	1
网线	2
随机光盘	1
小托架	1
装箱单	1

每台设备有固定的序列号，且是唯一的。设备序列号的位置随设备类型不同而不同，一般分 3 种情况：







3.2 设备上架

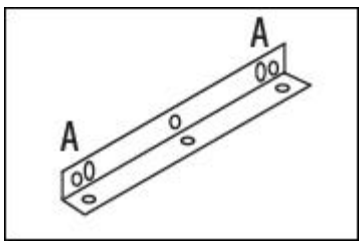
数据库审计设备机箱符合工业机柜的标准，它的高度为 1U 或者 2U，可以顺利的安装到 19”标准机柜中去。

3.2.1 1U 设备上架

安装支架

1.在每个 1U 设备附件中，都包括一个支架。

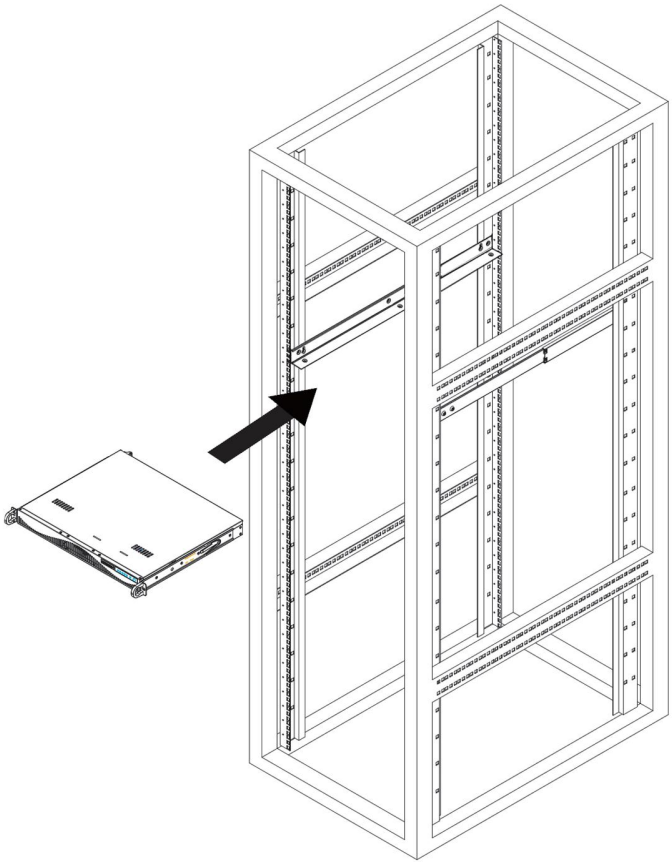
2.将支架安装在机柜上，将 A 点安装在机架内侧。如图所示:



设备上架

1.将设备放到刚装好的支架上，调整好位置。

2.将位于设备前面耳朵的孔与机架前侧的孔对应，加螺丝固定。



3.2.2 2U 设备上架

安装内侧导轨（固定在机箱上）

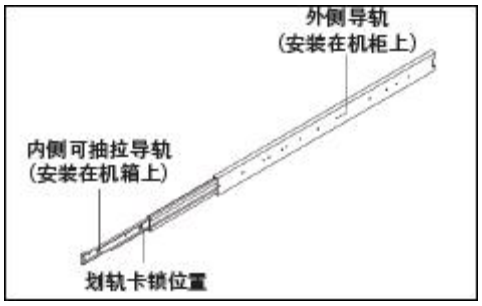
1. 在每个导轨装置中，都包括一副内侧可抽拉导轨和外侧导轨。

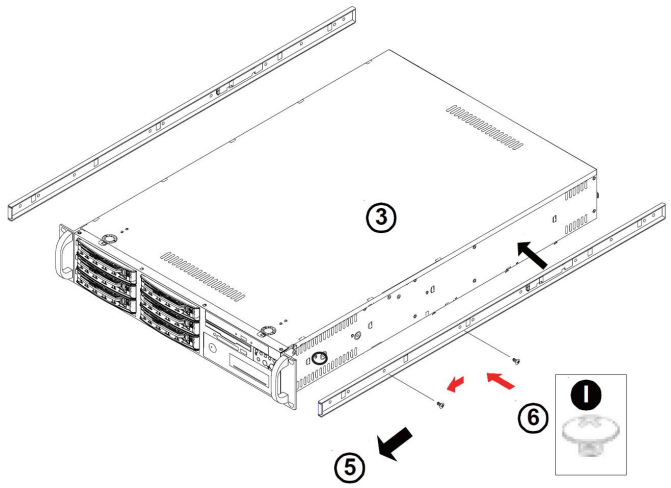
2. 按住内侧抽拉导轨装置上的卡锁，将内导轨抽出并安装在机箱侧面。(内侧导轨安

装在机箱两侧，外侧导轨安装在机柜两侧上)

3. 将位于内侧抽拉导轨的五个孔和机箱上侧身的五个孔相对应，加螺丝固定。

4. 固定好一侧导轨在机箱上，重复以上步骤再安装另一侧导轨在机箱上即可。





外侧导轨安装（固定在机柜上）

在机箱料包盒里，有前面（短）和后面（长）各一副导轨片。请按照导轨片上箭头标注的方向排好。

1. 排好后固定前面的导轨片（短）在外侧导轨上；

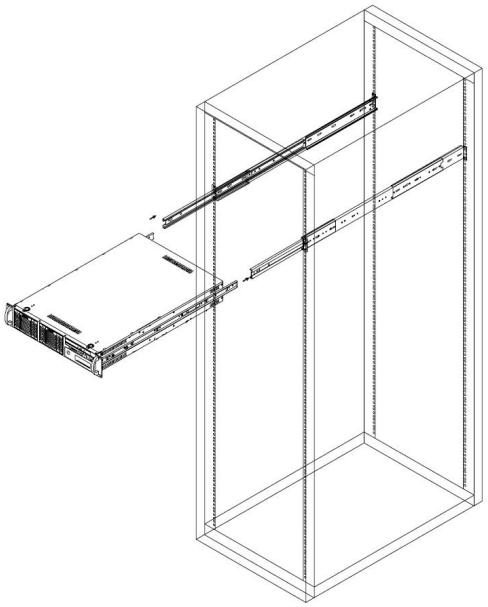
2. 再附上后面的导轨片（长）固定在外侧导轨上；

3. 量出外侧导轨安装到机柜的具体深度和长度，调节好短、长副导轨片和外侧导轨合适机柜的距离；

4. 重复相同的步骤安装另一侧的导轨到机柜上；

5. 将机箱插入机柜上的外侧导轨并推进时，听见“咔”的声响后，机箱便顺利装入机柜中（第一次安装时，机箱上导轨插入机柜外部导轨的过程和推入过程不是很容易，在推入时不要用力过猛）；

6. 当拉出机箱时，只要扳动机箱两侧导轨上的卡锁扣即可拉出。



3.3 设备连接

3.3.1 设备面板指示

设备面板指示：（以 1U 服务器为例）

如图：（自右至左）分别为：

电源开关、重新复位按钮、电源指示灯、硬盘工作指示灯、通信口指示灯、备用通信口指示灯、CPU 温度过高指示灯；

电源开关：软件式开关，按一下为开，再按一下为关；

重新复位按钮：暗埋式设计，使用时用细物按下，设备在任何情况下重新启动；

电源指示灯：此灯亮时指示电源为开（只有此灯亮时代表电源打开）；

硬盘工作指示灯：此灯亮时指示硬盘工作；

通信口指示灯：LAN0 号网口接通指示灯（此灯亮时只代表网口接通，不代表电源打开）；

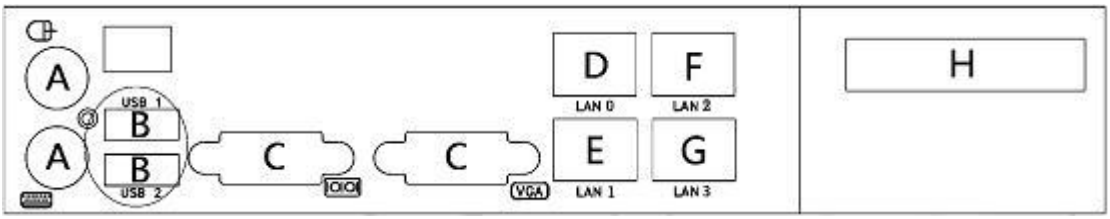
备用通信口指示灯：LAN1 号网口接通指示灯（此灯亮时只代表网口接通，不代表电源打开）；

CPU 温度过高指示灯：此灯亮时说明 CPU 温度超过 BIOS 中设定温度。

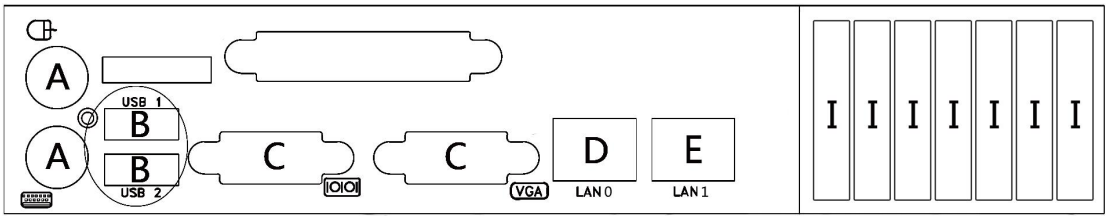
（该设备为 4 网口，LAN2、LAN3 指示灯在机箱背面网口处。）

3.3.2 设备接口说明

1U 设备：



2U 设备：



A：鼠标键盘

B：USB 接口

C：COM/Video 接口

D：通信口：用于用户访问系统的通信接口

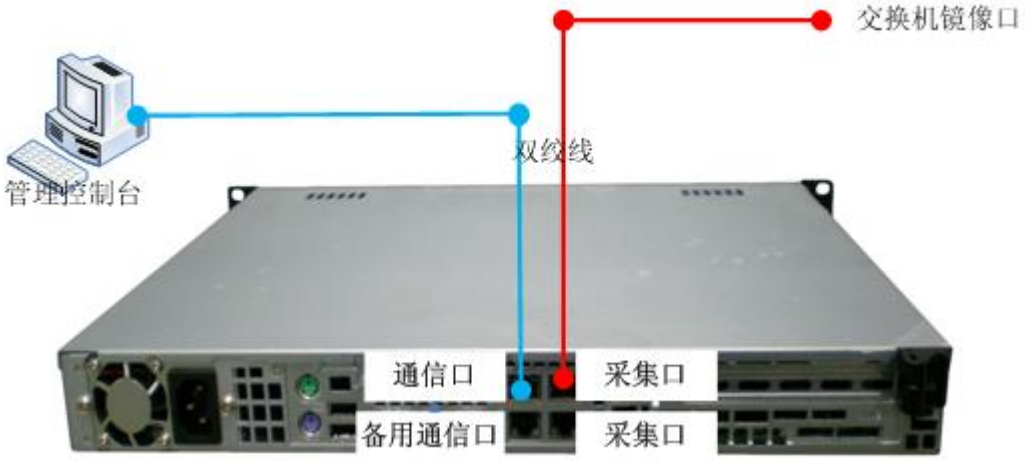
E：备用通信口：用于通过网络进行设备内部维护时使用

F、G：采集口：用于采集网络数据包的接口，可以使用两个接口中的任何一个或两个同时使用

H、I：扩展卡插口（可以为光接口卡或者电接口卡）

3.3.3 镜像端口接入

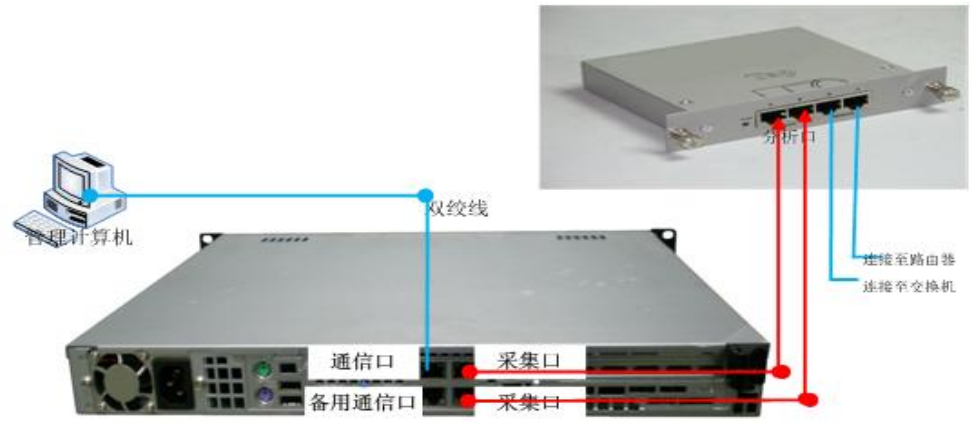
数据库审计设备一般采用镜像端口的接入方式，将一个采集口连接到交换机的镜像端口，交换机镜像端口的具体配置视不同厂家和型号的交换机会有所不同，具体配置方法参见相应厂家和型号的交换机配置手册。



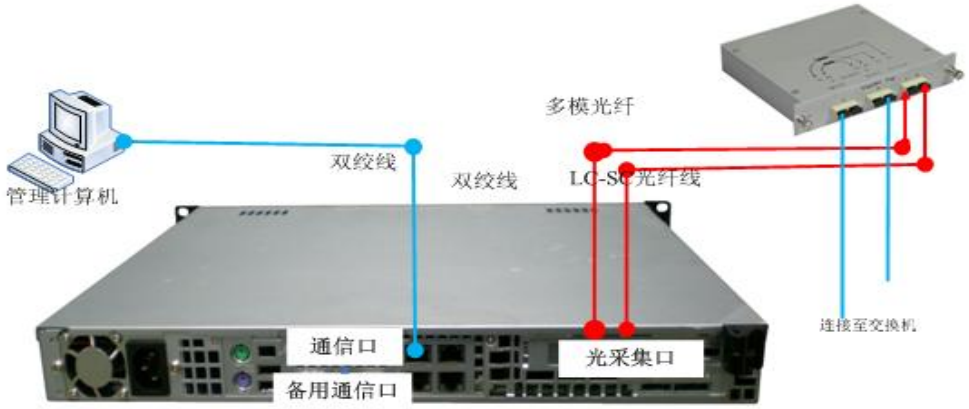
3.3.4 TAP 接入

当现场情况由于镜像端口已经被其他设备占用，或者因为某种原因无法接镜像端口，建议采用 TAP 的接入方式。

电口 TAP 接入示意图：



光接口 TAP 接入示意图：

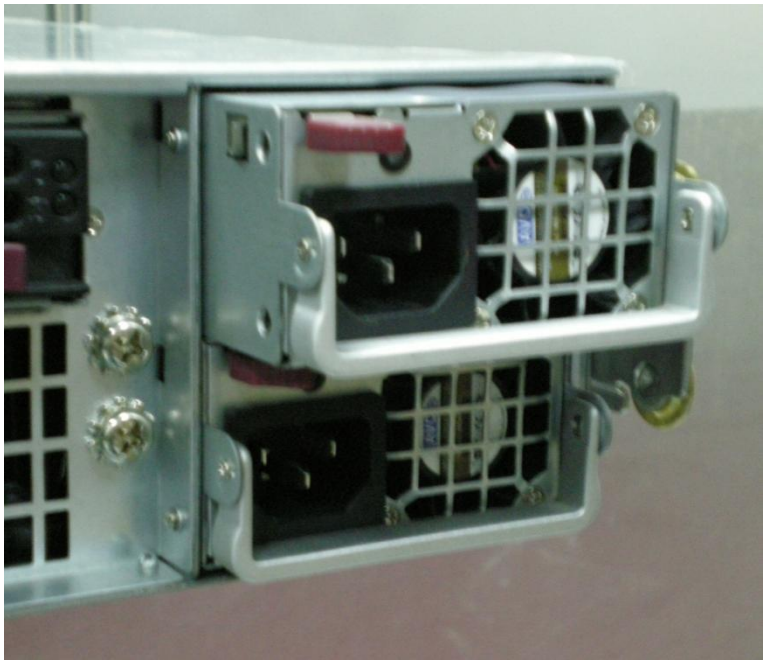


冗余电源：（以 2U 服务器为例）

如图所示：为 2U 设备的冗余电源；

要求上下两个电源都要接入 220V 交流电源；任何一个未接入，即会报警；

若不想使用两个电源供电，可任意拔出一个电源，就不会产生报警（如下两图）；



拔电源时，按住电源上面的按钮，向右侧按，同时拉电源后面的把手，即可将单个电源拉出；复原时，直接推电源到底，同时听到“卡”一声时，表示电源推到位并锁住。

4 连接登录

4.1 连接方式

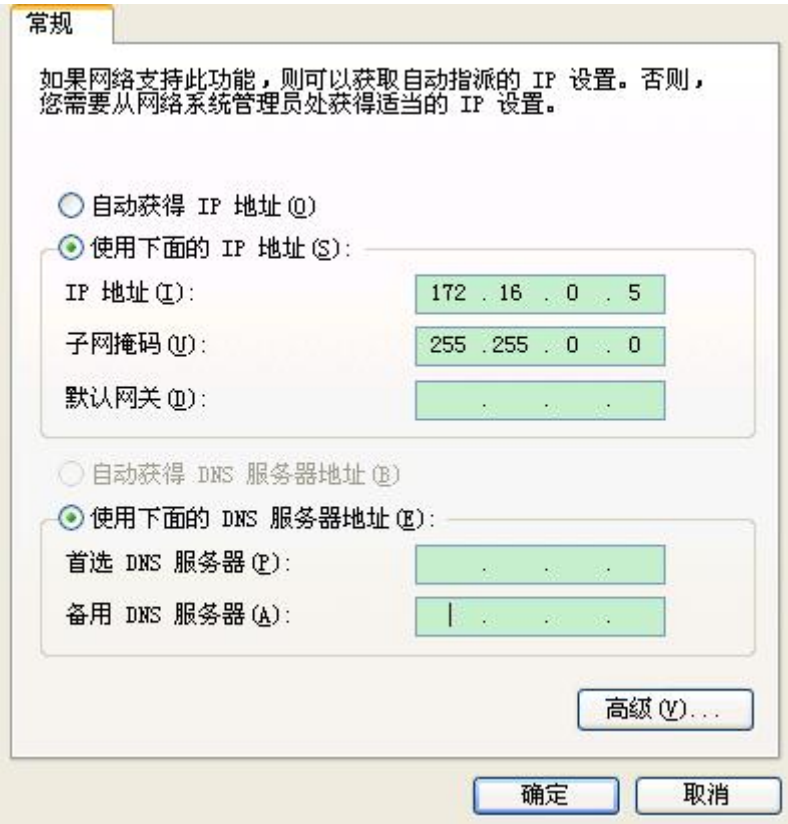
产品为 B/S 架构，使用 IE 浏览器软件即可以对产品进行配置和管理。将管理计算机通过交换机和通信口相连即可对设备进行管理。

通信口为 ETH0，备用通信口为 ETH1。

4.2 修改通信口的 IP 设置

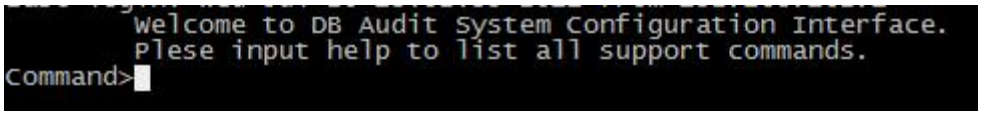
将数据库审计系统的默认 IP 修改修改为用户管理环境要求的 IP，通过备用通信口（ETH1）进入到数据库审计系统中，修改通信口 ETH0（审计中心 IP）地址，ETH1 出厂默认的 IP 地址 172.19.11.26，子网掩码 255.255.255.0，只能通过网线直连，不支持将备用通信口连到交换机。

在使用命令行修改通信口的 IP 时，首先要保证笔记本的 IP 地址和 ETH1 的 IP 在同一个网段，如果不在同一个网段，要先修改笔记本的 IP，如下图以 windows xp 为例：

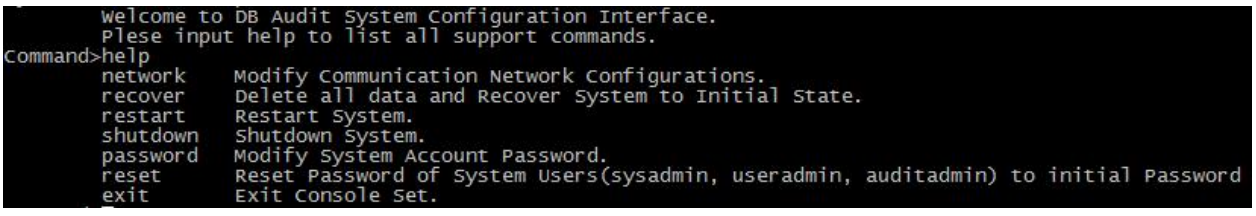


然后，用户可以使用 SecureCRT 登录，因系统安全加固，其他 SSH 工具可能无法正常连接，通过备用口的 IP 连接到后台系统，账号是 system，密码是 system。

用户登录后台系统后可以看到如下界面：



用户可以依次输入 help，network，如下图所示：



依次按照提示修改 IP、子网掩码以及网关。具体操作方法参见“命令手册 2.1 修改网络配置 network”。

4.3 登录系统

使用 IE 浏览器(要求用 IE8 或以上版本，IE6 不能完全支持，flashplayer10.3 或以上版本)，在地址栏中输入：http://审计中心 IP （此处的审计中心 IP 指审计中心通信口的 IP） 如：http://192.168.1.254 按照以下步骤进行即可登录系统。

通信口　　IP 地址：192.168.1.254

掩码：　255.255.255.0

网关：　192.168.1.1

备用通信口　　IP 地址：172.19.11.26

掩码：　255.255.255.0

系统内置用户和初始密码：

内置默认用户	用户名	密码	权限
系统管理员	sysadmin	sysadmin@1234	首页、审计中心、攻击监测、性能分析、策略中心、报表中心、系统配置
用户管理员	useradmin	useradmin@1234	普通用户的创建和删除等管理
系统审计员	auditadmin	auditadmin@1234	查看系统自身操作日志的审计信息

说明：

数据库审计系统目前只支持使用 IE 8 及以上版本浏览器，使用其他浏览器有可能出现部分功能显示异常现象。Flash 支持 10.3.32.18 以上版本。

1) 输入用户名和密码，即可登录系统。

2) 部署首次安装的数据库审计系统应以系统管理员身份登录系统，系统管理员默认用户名和密码为 sysadmin，sysadmin@1234。

3) 用户首次登录系统的时候需要更改当前的密码，且密码必须符合以下规范：

    1. 字母、数字、特殊字符的组合
    2. 长度大于 8 位
    3. 不能与原密码相同

注意：

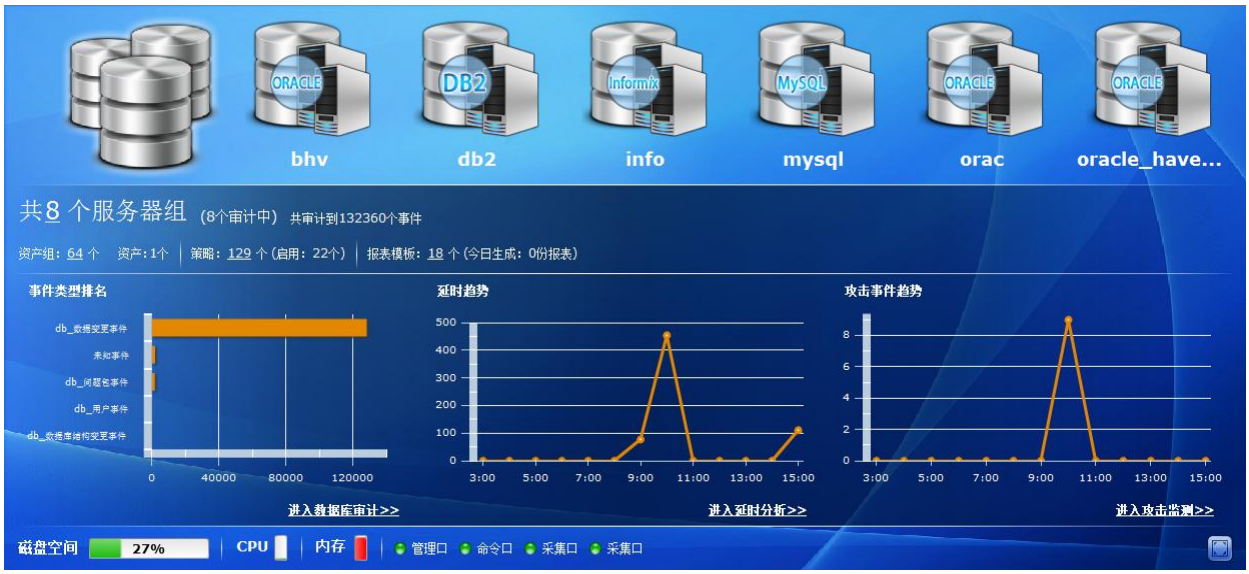
当用户连续 5 次输入错误的密码进行登录，系统将弹出提示，如下图所示：

此时需要等待 5 分钟后再刷新界面进行登录。

5 数据库审计系统管理

5.1 首页

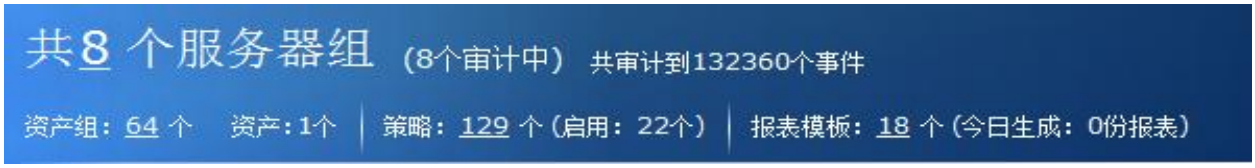
“首页”主要反映该审计系统的全局信息，包括审计服务器及策略相关配置情况、事件类型及 SQL 操作延时及安全攻击事件趋势、磁盘信息、CPU、内存以及网口通信状态信息等。如下图所示。



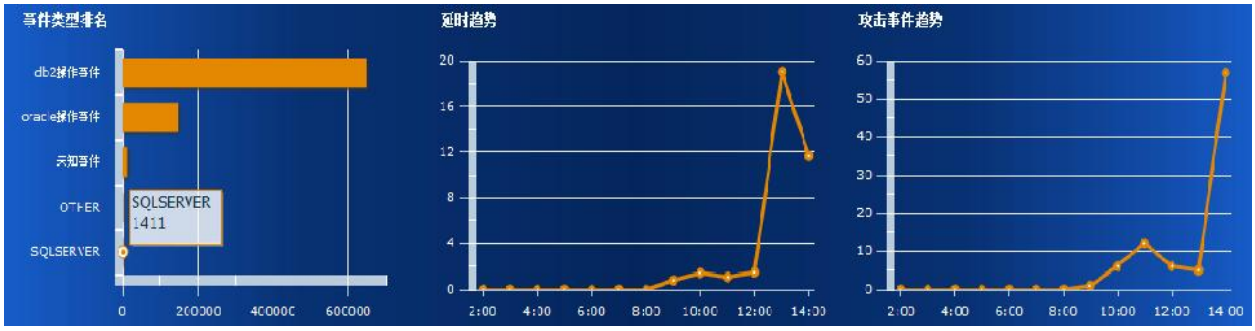
其中，上面部分列出了所有数据库审计服务器，可点击后面的单个图标查看针对各个服务器的统计信息。系统初装无审计服务器时显示如下：

点击“添加”即可跳转到“审计数据库服务器”界面。

第二部分显示过去的 12 个小时数据库操作事件的统计情况，如下图所示：



第三部分是针对数据库服务器的各事件类型、SQL 操作的延时、服务器遭受安全攻击的数量进行展示。



鼠标移到折线整点处，可看到当时时间段的数据统计数：

事件类型排名：单点显示过去的 12 小时内数据库服务器发生的相应事件类型的审计记录总数，总体显

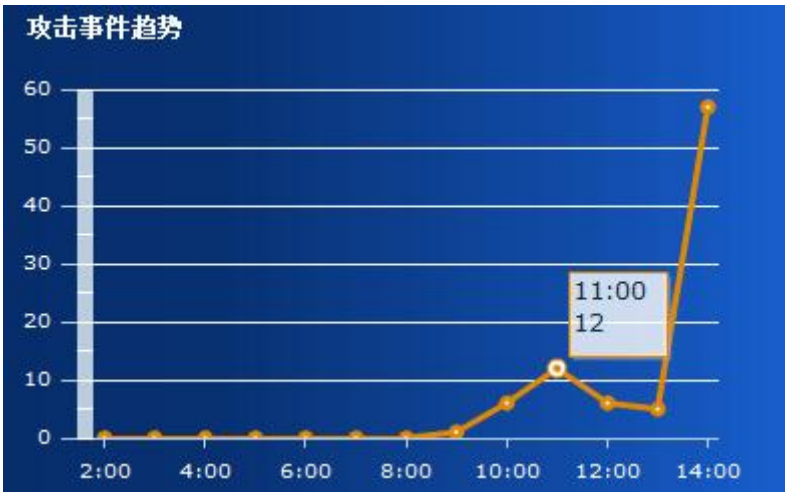
示总数前 5 名的事件类型，如上图所示单点为过去的 12 小时发生名为“SQLSERVER”事件的记录数为 1411 条；

延时趋势：单点显示当时的 1 小时内数据库服务器操作的平均延时时间（以毫秒为单位），总体显示过

去的 12 个小时的延时趋势；

攻击事件趋势：单点显示当时的 1 小时内数据库服务器遭受攻击的总数，总体显示过去 12 小时的攻击

事件趋势，如下图所示单点为 11：00 至 12：00 的数据库服务器遭受攻击的总数为 12。



首页下方显示的是当前系统磁盘的使用情况（以百分比表示），以及各以太网口的使用状态（当网口未连接网线时，显示红色，否则显示绿色），鼠标移到相应的图标处，可显示具体信息。如下图所示：

5.2 门户框架

以系统管理员 sysadmin 登录系统后，在界面的右上角可以看到如下图所示的门户菜单栏：

从左依次为：个人设置、实时监控、系统消息提示、时间设置、注销。

5.2.1 个人设置

以系统管理员 sysadmin 登录系统后，点击  按钮，弹出个人设置界面，如下图所示：

个人设置包括用户名全名、电子邮箱、密码三项。

全名：输入系统用户的名称，默认的全名是 sysadmin。**注：与登录时的用户名不同。**

当输入“全名”后，“保存”和“重置”两个按钮变为可用状态。若点击“重置”按钮，状态变为用户上一次保存时的“全名”；若点击“保存”按钮，将输入信息进行保存，然后“保存”和“重置”两个按钮再次变为不可用状态，并且，再次登录系统后，保存了的名称将显示在门户菜单中，例如：输入用户全名为：abcdef，如下图所示：

电子邮箱：输入电子邮箱地址。同上，当输入“电子邮箱”后，“保存”和“重置”两个按钮变为可用状态。若点击“重置”按钮，状态变为用户上一次保存时的“电子邮箱”；若点击“保存”按钮，将输入信息进行保存，然后“保存”和“重置”两个按钮再次变为不可用状态。

密码：是否修改密码。

若要修改密码，密码长度不能少于 8 位，并且密码必须包含字母、数字和特殊字符。例如：abc@1234。

若显示密码被勾选，显示输入的密码，否则以“*”代替。

输入新密码后，“保存”和“重置”两个按钮变为可用，点击“保存”按钮，保存新密码，再次登录系统时，要使用新设定的“密码”进行登录；点击“重置”按钮，不保存。然后，返回到初始登录个人设置界面的状态。

5.2.2 实时监控

如上图所示，报警信息以红、黄、绿三个颜色圆圈代表审计数据库服务器监控到的数据风险级别为高、中、低。数字表示审计数据库服务器按相应风险级别所实时监控到的数据。

注：**提示数据个数范围为 0-9999 条。**当超过 9999 条数据时，以"9999+"形式表示。

1）点击三个风险级别的颜色圆圈，分别会弹出当前风险级别的审计记录页面。

2）若点击 

，将显示当前实时审计的数据，最多显示 1000 条数据。同时，数据列表按照风险级别（包括高、中、低、无）的不同显示颜色也不同，与门户菜单的风险级别圆圈相对应，即"高"对应红色，"中"对应黄色，"低"对应绿色，"无"对应无色。如下图所示：

数据列表显示数据范围为 0-1000 条。每 5 秒钟刷新一次进行数据更新，最新监控到的数据将显示在列表的最下方。并且，监控数据具有排重功能。

数据列表区域的颜色与门户菜单代表风险级别的圆圈颜色相同，如上图，风险级别为"中"，门户菜单中以黄色圆圈表示，那么数据列表的区域显示为黄色。

并且，可以对列表的数据进行排序，如上图所示，按事件 ID 进行排序，那么点击"事件ID ▲"后面的三角即可，上三角表示时间 ID 从小到大排序，下三角与其相反。

同理，也可按风险级别、审计数据库服务器、事件类型、操作来源、操作时间中的任意一项进行排序。

选中某一条事件，将在界面的下方显示出详细信息（红色框内区域）。

点击 条 件，可配置来源、操作类型及风险级别的过滤条件，过滤条件创建后，对界面上已展示数据进行过滤。

5.2.3 系统消息提示

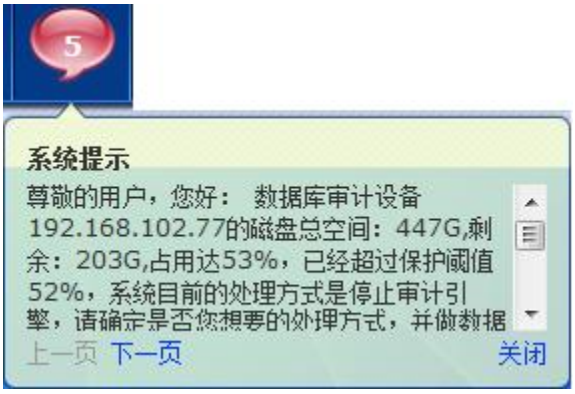
，此图片代表系统消息提示，气泡里面的数字，代表消息条数。

系统默认有 6 条消息提示。即：配置 IP 采集条件、配置邮件服务器、配置时间服务器、配置审计服务器、配置授权告警、配置磁盘预警阀值。若增加配置或完成某个配置，那么系统会在 1 分钟内监测到，数字会相应增加或减小，配置过的消息提示将不再进行提示。

点击气泡， 可查看具体提示信息。

当有授权告警时，会在此增加提示，如下图所示：

当有磁盘预警时，会在此增加提示，如下图所示：



当系统修改某一信息或者配置后，**会在此增加“同步”提示**，需要点击气泡，进行同步。

例如：在策略配置中，添加了一条事件类型，并且为它新建了一条策略，此时，点击气泡，将有如下提示：

提示内容：策略发生了变化，点击“同步”按钮，进行系统同步配置。

当缓存表数据达到工作参数里的数据处理的缓存表数据超过值以后，**会在此增加”清空”提示**，点击清空，系统将清空缓存表数据。“清空”提示如下图：

注：每增加一个消息提示，都会显示在消息提示的首页。

5.2.4 时间设置

点击门户菜单的系统时间设置，那么直接跳转到“系统配置->工作参数”界面，进行时间设置。

5.2.5 注销

在任意时刻，点击门户菜单的 

按钮，弹出如下对话框：

若点击“确定”按钮，跳转到初始登录界面；若点击“取消”，关闭此对话框。

5.3 审计中心

审计中心包括： 数据库审计、其它审计、实名审计、DOMINO 审计和本地审计。通过审计中心，可以对系统已审计到的数据进行查看，通过设置时间等查询条件对审计到的数据进行更精确的查询。

5.3.1 数据库审计

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏“审计中心->数据库审计”，即可进入数据库审计界面。

数据库审计是对系统记录的对数据库的操作行为进行的审计。

进入数据库审计页面以后，默认的查询条件是今天，点击查询，可以查看今天已审计到的对数据库的操作行为的记录。

选择查看日期： 通过点击下方的日期选择需要查看的日期的审计记录，点击 和 分别向左和向右滑动日期， 点击 滑到日期列表的最左边，点击 滑到日期列表的最右边。

详细信息： 点击一条数据，在右边列表页面可以查看到选中数据的详细信息。

导出：在查询结果区域的“导出”按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

SQL 回放：点击一条数据，在右边列表页面的详细信息中点击“SQL 回放”，可对同一会话中的 SQL 语句进行回放。点击播放，界面展示 SQL 语句已经 SQL 语句的返回状态。播放时可进行暂停、查看第一条和查看最后的操作。

用户关联： 对操作来源 IP 可以通过点击“用户关联”，在新的页面上设置时间关联到登录 SMP 认证系统的用户名。下图是点击操作来源 IP“192.168.10.208”右侧的“用户关联”页面以后，查到的关联结果示例：

排序： 可以通过点击查询结果中的列名进行升、倒序排列。

点击"查询"按钮的下拉箭头，进入到查询设置页面，当鼠标移动到查询条件上时，下方的说明框里是对查询条件的详细说明。

通过设置查询条件，可以更精确的查询到审计记录。

5.3.2 其它审计

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏"审计中心->其它审计"，即可进入其它审计界面。

其它审计中包含了：运维，WEB 中间件，WEB 中间件关联，SYSLOG 日志，SNMP 日志。

点击“其它审计”右侧的单选框，可以切换到具体的审计页面。比如，点击运维单选框，运维审计页面被打开。

5.3.2.1运维

运维是对访问数据库服务器行为的审计。

进入运维审计页面以后，默认的查询条件是今天，点击查询，可以查看今天已审计到的对数据库服务器访问的记录。

选择查看日期： 通过点击下方的日期选择需要查看的日期的审计记录，点击 和 分别向左和向滑动日期， 点击 滑到日期列表的最左边，点击 滑到日期列表的最右边。

详细信息： 点击一条数据，在右边列表页面可以查看到选中数据的详细信息。

导出：在查询结果区域的“导出”按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

用户关联： 对操作来源 IP 可以通过点击“用户关联”，在新的页面上设置时间关联到来源 IP 的用户名，同数据库审计中的该功能。

排序： 可以通过点击查询结果中的列名进行升、倒序排列。

点击“查询”按钮的下拉箭头，进入到查询设置页面，

当鼠标移动到查询条件上时，下方的说明框里是对查询条件的详细说明。

通过设置查询条件，可以更精确的查询到审计记录。

5.3.2.2WEB 中间件

WEB 中间件审计是对中间件访问记录的审计。

进入 WEB 中间件审计页面以后，默认的查询条件是今天，点击查询，可以查看今天已审计到的对 WEB 中间件访问情况的记录。

选择查看日期： 通过点击下方的日期选择需要查看的日期的审计记录，点击 和 分别向左和向滑动日期， 点击 滑到日期列表的最左边，点击 滑到日期列表的最右边。

详细信息： 点击一条数据，在右边列表页面可以查看到选中数据的详细信息。

导出：在查询结果区域的“导出”按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

排序： 可以通过点击查询结果中的列名进行升、倒序排列。

点击“查询”按钮的下拉箭头，进入到查询设置页面，如下图：

当鼠标移动到查询条件上时，下方的说明框里是对查询条件的详细说明。

通过设置查询条件，可以更精确的查询到审计记录。

5.3.2.3WEB 中间件关联

WEB 中间件关联是对通过访问 WEB 中间件来访问数据库服务器的行为进行关联的结果的审计。

进入 WEB 中间件关联审计页面以后，默认的查询条件是今天，点击查询，可以查看今天已审计到的数据库操作与 WEB 中间件访问的两者之间已关联到的信息的记录。

选择查看日期： 通过点击下方的日期选择需要查看的日期的审计记录，点击 和 分别向左和向滑动日期， 点击 滑到日期列表的最左边，点击 滑到日期列表的最右边。

详细信息： 点击一条数据，在右边列表页面可以查看到选中数据的详细信息。

导出：在查询结果区域的“导出”按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

排序： 可以通过点击查询结果中的列名进行升、倒序排列。

点击“查询”按钮的下拉箭头，进入到查询设置页面，如下图：

当鼠标移动到查询条件上时，下方的说明框里是对查询条件的详细说明。

通过设置查询条件，可以更精确的查询到审计记录。

5.3.2.4SYSLOG 日志

SYSLOG 日志是对审计数据库所在主机的 SYSLOG 日志的审计。

进入 SYSLOG 日志审计页面以后，默认的查询条件是今天，点击查询，可以查看今天已审计到的数据库所在主机的 SYSLOG 日志审计记录。

选择查看日期： 通过点击下方的日期选择需要查看的日期的审计记录，点击 和 分别向左和向滑动日期， 点击 滑到日期列表的最左边，点击 滑到日期列表的最右边。

详细信息： 点击一条数据，在右边列表页面可以查看到选中数据的详细信息。

导出：在查询结果区域的“导出”按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

排序： 可以通过点击查询结果中的列名进行升、倒序排列。

点击“查询”按钮的下拉箭头，进入到查询设置页面

当鼠标移动到查询条件上时，下方的说明框里是对查询条件的详细说明。

通过设置查询条件，可以更精确的查询到审计记录。

5.3.2.5SNMP 日志

SNMP 日志是对审计数据库所在主机的 SNMP 日志的审计。

进入 SNMP 日志审计页面以后，默认的查询条件是今天，点击查询，可以查看今天已审计到的数据库所在主机的 SNMP 日志审计记录。

选择查看日期： 通过点击下方的日期选择需要查看的日期的审计记录，点击 和 分别向左和向滑动日期， 点击 滑到日期列表的最左边，点击 滑到日期列表的最右边。

详细信息： 点击一条数据，在右边列表页面可以查看到选中数据的详细信息。

导出：在查询结果区域的“导出”按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

排序： 可以通过点击查询结果中的列名进行升、倒序排列。

点击“查询”按钮的下拉箭头，进入到查询设置页面。

当鼠标移动到查询条件上时，下方的说明框里是对查询条件的详细说明。

通过设置查询条件，可以更精确的查询到审计记录。

5.3.3 实名审计

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏“审计中心->实名审计”，即可进入实名审计界面。

实名审计是此处展示的是访问 SMP 系统的用户登入（用户活动开始时间）登出（用户活动结束时间）时间和用户的 IP。

该功能默认为关闭状态，默认用户需要首先进行 SMP 配置：在“查询”按钮下方点击“SMP 配置”，弹出对话框，如下图所示：

状态：用户可点击选择是否开启 SMP 审计功能，默认为"关"即不审计；

IP、端口：指定 SMP 关联系统服务器的 IP 和端口；

保存后即可生效。

查询条件包括用户活动开始时间、用户活动结束时间、用户名和 IP。

查询条件可以以单一条件进行查询也可以以组合条件进行查询（默认的查询条件是今天）。

用户活动开始时间即用户登入数据库的时间，用户活动结束时间即用户登出数据库的时间，只要用户的登入和登出时间在开始时间和结束时间范围内就会将该用户的信息查询出来。

例如：设置的开始时间和结束时间分别是：2011-03-17 00:00:00 和 2011-03-18 23:59:59。则查询结果为所有登入时间大于等于开始时间和登出时间小于等于结束时间的记录。

排序： 点击查询结果中的列名，可对选择列进行升、倒序排列。

5.3.4 DOMINO 审计

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏"审计中心->DOMINO 审计"，即可进入 DOMINO 审计界面。

DOMINO 审计是针对 DOMINO 文档型数据库产品而进行的数据库审计。通过 DOMINO 审计查询可以根据查询条件，把审计到的数据包括用户名、服务器名、端口、流量、事务数、读写文档数、会话时长以及数据库等相关信息查询出来。

DOMINO 审计支持的查询条件包括：时间范围、DOMINO 服务器名、用户名以及数据库名。对于 DOMINO 服务器名信息，系统可以自动从审计数据中获取，查询时用户手动选取服务器即可。而对于用户名和数据库名信息，需要用户手动输入关键字，其中支持关键字的模糊查询。例如：在用户名输入框中输入 admin 为关键字，就可以查询出用户名含有 admin 字段的所有用户。

DOMINO 审计查询界面包括两部分，查询结果和详细信息。

查询结果以表格形式展现 DOMINO 审计信息，点击列名可以按照该列数据进行排序。查询结果每次返回 100 条记录，可以拖动鼠标至底部进行再次查询，直至返回所有符合条件的记录。点击查询结果标题右上侧的导出标志，可以对符合查询条件的记录进行导出，其中导出文件将以 csv 格式保存。

详细信息包括数据库和其他相关信息，用户也可以点击导出标志，对单条审计记录进行导出，导出文件以 txt 格式保存。

注：**用户需要以 DOMINO 服务器名，在审计数据库服务器页面内添加 DOMINO 类型的服务器。**首页就可以展现基于该 DOMINO 服务器的统计信息，其中包括：会话趋势、流量趋势以及事务趋势。

5.3.5 本地审计

注意：本地审计当前只支持 oracle10、11 和 sqlserver2008 版本。

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏"审计中心->本地审计"，即可进入本地审计界面。

本地审计是通过数据库账号、密码（实例名）连接到数据库服务器，查询数据库本身提供的审计功能审计到的数据。

本地审计界面中，从数据库服务器列表中选择数据库服务器，点击"审计"，进行配置后查询。

第一次进入审计界面后，系统默认从数据库服务器列表中选择一个数据库服务器，并提示需要配置访问连接所需要的数据库账号、密码等（最好使用系统管理员账号，本地审计系统不会记录此账号相关信息），如下图：

输入数据库账号、密码、实例名（ORACLE 数据库需要提供实例名）后，点击“保存并审计”后，系统可连接到选中的数据库服务器，并查询出该数据库服务器自身审计的结果。

5.4 攻击监测

攻击监测主要是监测网络上攻击数据库的行为，包括对数据库服务器的网络攻击检测、运维服务攻击检测和操作系统的攻击检测。用户可以开启或关闭该监测，并且可以进行监测引擎配置，也可以设置条件对各种监测结果进行查询。

5.4.1 如何开启或关闭攻击监测

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏“攻击监测->监测引擎配置”，鼠标点击左上角显示开关按钮，即可实现攻击检测的开启或关闭。如图所示：

在系统安装初始状态下，该监测事件处于开启状态。当攻击检测引擎处于停止状态时，该按钮显示如下图所示：

切换开/关状态时，会弹出如下对话框：

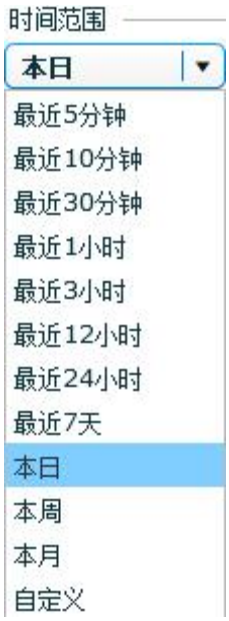
点击“确定”按钮，返回到监测引擎配置界面。

5.4.2 攻击事件查询

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的“攻击监测->攻击事件查询”，进入“攻击事件查询”界面。

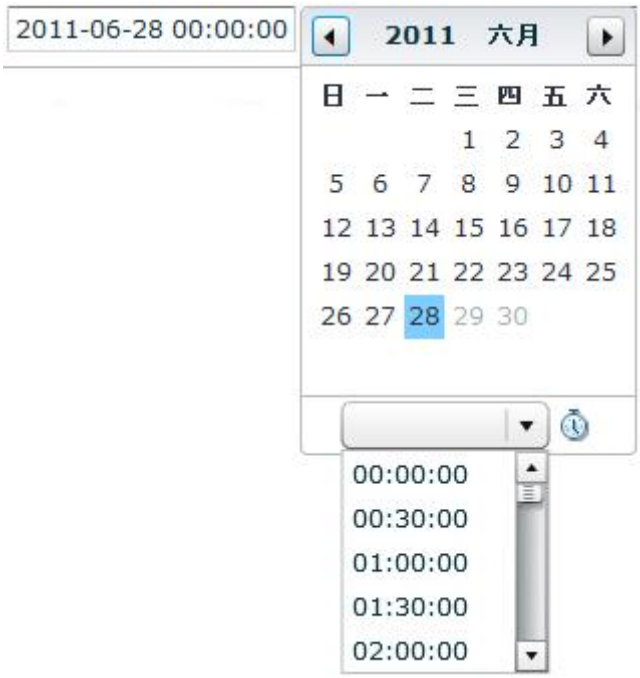
5.4.2.1如何设置时间范围查询

系统默认的时间范围查询条件为：本日，点击下拉按钮可打开并选择其余时间查询条件。如下图所示：



时间范围的查询条件有：最近 5 分钟、最近 10 分钟、最近 30 分钟、最近 1 小时、最近 3 小时、最近 12 小时、最近 24 小时、最近 7 天、本日、本周、本月和自定义。

用户可以通过单击按钮更改日期和时间，如下图所示：



用户可以单击时间按钮，在下拉菜单中选取时间，如上图所示：

也可以进行手动输入，如下图所示：

5.4.2.2如何查看查询结果

在攻击事件查询界面，点击“查询”按钮，左侧是查询结果列表，右侧是详细信息列表。

1）查询结果列表

在查询结果中，默认的展示列为：

时间日期：数据库攻击事件发生的日期和时间；

源 IP：发生数据库攻击事件的源 IP 地址；

目的 IP：发生数据库攻击事件的目的 IP 地址；

源端口：发生数据库攻击事件的源 IP 端口

目的端口：发生数据库攻击事件的目的端口；

协议：数据库攻击事件的网络应用协议；

级别：数据库攻击事件的报警级别；

特征规则：数据库攻击事件匹配的安全特征规则；

攻击事件描述：数据库攻击事件的简单文字描述。

查询结果会以天为单位分页显示，点击其中一天就可以查看当天的记录（如上图所示）。当前被查看的日期以灰色显示。

如果查询条件所设置的时间范围的跨度比较大，例如：2011.06.01 到 2011.06.28，则可通过  和  进行上翻和下翻，通过  和  进行翻到最前和最后。

如果没有符合查询条件的数据，会在查询结果中间显示："没有找到符合条件的结果"。

2）详细信息列表

选择某一条记录，在右侧的"详细信息"区域即显示出该条记录的详细信息。

5.4.2.3如何将监测事件导出

在查询结果区域的"导出"按钮可批量导出前 1 万条记录。点击每条记录右侧详细信息处可以导出当前对应的一条数据。

导出文件可用 Excel 工具打开，内容如下图所示：

	A	B	C
1	datetime	时间日期	2011/6/28 4:35
2	level	级别	高
3	ruleName	特征规则	EXPLOIT ssh CRC32 overflow filler
4	netProtocol	协议	TCP
5	sourceIp	源IP	192.168.10.1
6	sourcePort	源端口	3450
7	destIp	目的IP	192.168.10.16
8	destPort	目的端口	22
9	ruleDesc	攻击事件描述	ssh CRC32校验缓存溢出漏洞利用

5.4.2.4如何设置详细查询条件

在“攻击事件查询”界面，点击 

按钮右侧的下拉三角按钮，即可在下方弹出详细查询条件。

当前系统主要提供以下几个条件的查询：攻击事件源 IP、攻击事件源端口、攻击事件目的 IP、攻击事件目的端口、攻击事件协议、攻击事件级别、说明。

其中攻击事件源 IP 和攻击事件目的 IP 条件需要按照 IP 地址的标准格式输入，攻击事件源端口和攻击事件目的端口条件的端口范围在 0~65535 之间，**其中 0 表示无相应的端口。**

设置条件后，点击“查询”按钮后详细条件将隐藏，相应的查询结果将会显示在界面上。

点击左下角的“重置所有条件”按钮，将清空所有的查询条件，包括将“时间范围”条件重新置为默认条件“本日”。

注：当鼠标移动到相应查询条件时，在“说明”对话框对相应查询条件进行详细说明。

5.4.3 监测引擎配置

监测引擎配置是系统内置的安全攻击事件匹配的配置，用户可以自定义修改报警级别、启用或者停用该配置。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏“攻击监测->监测引擎配置”，即可进入监测引擎配置界面，如下图所示：

监测引擎配置界面的展示列如下：

名称：系统内置的数据库网络攻击特征规则的名称，按照攻击对象类型主要分为三种：数据库、操作系统、网络应用。其中数据库类型主要是对数据库服务器的攻击特征规则，操作系统类型主要是对操作系统级别的攻击特征规则，网络应用主要是对运维服务的攻击特征规则；如下图所示：

类型：攻击事件的安全类型，如缓冲区溢出、权限提升、漏洞利用、口令猜测等；

级别：攻击事件的检测报警级别，分为高、中高、中、中低、低五种；

描述：攻击特征规则的简单文字描述；

影响：此攻击的影响；

描述：此攻击的具体描述信息。

默认状态下所有的规则都是处于启用状态。

用户可以自定义修改特征规则的报警级别，或者通过勾选某条规则设置启用或着停用该规则。修改后，用户可点击右下方的"保存"按钮保存相应的设置。

5.5 性能分析

“性能分析”主要是基于现有的数据记录的分析，通过查看各数据库服务器的响应延时协助用户分析定位服务器的性能。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏中的"性能分析->延时分析"菜单，进入延时分析界面。

5.5.1 如何指定时间范围进行延时分析

系统默认的时间范围查询条件为：本日，点击下拉按钮可打开并选择其余时间查询条件。

用户可以通过单击按钮更改日期和时间。

用户可以单击时间按钮，在下拉菜单中选取时间，如上图所示：

也可以采用手动输入，如下图所示：

5.5.2 如何查看分析结果

设置查询条件后点击"分析"按钮，查询结果即显示在下方列表

在查询结果的上方会显示查询结果（成功/失败）、查询结果的总记录数和查询用时；

查询结果会以天为单位分页显示点击其中一天就可以查看当天的记录。当前被查看的日期以灰色显示。

如果查询条件所设置的日期范围的跨度比较大，例如：2011.06.01 到 2011.06.28，则可通过  和  进行上翻和下翻，通过  和  进行翻到最前和最后。

如果没有符合查询条件的数据，会在查询结果中间显示："没有找到符合条件的结果"。

5.5.3 如何设置详细分析条件

在"延时分析"界面，点击 

按钮右侧的下拉三角按钮，即可在下方弹出详细查询条件设置菜单。

注：当鼠标移动到相应查询条件时，在"说明"对话框对相应查询条件进行详细说明。

如果要重新选择全部条件，可以点击"重置条件"按钮进行全部条件的重新设置。

5.6 统计分析

统计分析分为 SQL 操作类型统计、事件类型统计和流量统计三种统计方式。

5.6.1 SQL 操作类型统计

SQL 操作类型统计主要是对各个审计服务器审计到的数据，按照 SQL 的操作类型进行分类统计。通过查看统计到的 SQL 操作类型协助用户分析服务器在所选时间内进行的 SQL 操作。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏中的"统计分析->SQL 操作类型统计"菜单，进入 SQL 操作类型统计界面（默认为全部服务器的"今天"的所有操作类型的统计）。

5.6.1.1如何进行统计分析

系统默认的服务器选择为：全选，点击服务器下拉按钮可打开所配置全部可选服务器，进行服务器的选择。

系统默认的时间范围查询条件为：今天，点击下拉按钮可打开并选择其余时间查询条件。

时间范围的查询条件有：今天、昨天、最近 7 天、最近 30 天、自定义。

用户可以通过单击  按钮更改日期和时间。

5.6.1.2如何查看分析结果

设置好查询条件后，点击 

按钮，统计结果即显示在下方。

统计的结果分为"SQL 操作类型统计分析趋势图"和"SQL 操作类型排名"两种方式展示。

1、 SQL 操作类型统计分析趋势图用来展示所选条件的 SQL 操作类型按时间的统计趋势，当鼠标放在趋势图节点时，会展示该节点所在时间的统计信息，如下图所示：

2、 SQL 操作类型排名用来展示所统计的各个操作类型的排名、操作类型、百分比、总数。并且在各个操作类型后面有 查看详细 链接，可用来查看所选操作类型的详细的信息。

3、 SQL 操作类型统计分析趋势图和 SQL 操作类型排名均有对比操作，如下图所示，若点击对比昨天：

SQL操作类型排名(2012年02月21日)　　2012年02月21日　　2012年02月20日

排名	操作类型	百分比(近似值)	总数	百分比(近似值)	总数	查看
	所有操作类型		477039		70769	
1	INSERT	30.45%	145246	94.96%	67202	查看详细
2	LOGIN	23.55%	112359	0.01%	6	查看详细
3	OTHER	22.92%	109356	0.04%	31	查看详细
4	CREATE	22.92%	109325	0.03%	19	查看详细

SQL 操作类型统计分析趋势图中有所选时间和要对比时间的曲线图，其中较深颜色的曲线为所选时间统计曲线，较浅颜色曲线为要对比时间的统计曲线；SQL 操作类型排名中有百分比和总数的对比情况，且在数据前方有上升或者下降箭头提示，其中黑色数据为所选时间的操作类型，灰色为要对比时间的相应的操作类型，且在上方有日期提示。

5.6.2 事件类型统计

事件类型统计主要是对各个审计服务器审计到的数据，按照事件的类型进行分类统计。通过查看统计到的事件类型协助用户分析服务器在所选时间内进行的操作事件。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏中的"统计分析->事件类型统计"菜单，进入事件类型统计界面（默认为全部服务器的"今天"的所有事件类型的统计）。

5.6.2.1如何进行统计分析

此项设置方法同 SQL 操作类型统计中设置方法相同。

5.6.2.2如何查看分析结果

设置好查询条件后，点击 

按钮，统计结果即显示在下方。

统计的结果分为 "事件类型统计分析趋势图"和"事件类型排名" 两种方式展示。

1、 事件类型统计分析趋势图用来展示所选条件的事件类型按时间的统计趋势，当鼠标放在趋势图节点时，会展示该节点所在时间的统计信息，如下图所示：

2、 事件类型排名用来展示所统计的各个事件类型的排名、事件类型、百分比、总数。并且在各个事件类型后面有查看详细链接，可用来查看所选事件类型的详细的信息。

3、 事件类型统计分析趋势图和事件类型排名均有对比操作，如下图所示，若点击对比昨天：

事件类型排名(2012年02月21日)　　2012年02月21日　　2012年02月20日

排名	事件类型	百分比(近似值)	总数	百分比(近似值)	总数	查看
	所有事件类型		477039		70769	
1	db_数据变更事件	30.47%	145331	95.1%	67303	查看详细
2	db_用户事件	23.55%	112362	0.02%	17	查看详细
3	未知事件	23.06%	110003	1.89%	1341	查看详细

事件类型统计分析趋势图中有所选时间和要对比时间的曲线图，其中较深颜色的曲线为所选时间统计曲线，较浅颜色曲线为要对比时间的统计曲线；事件类型排名中有百分比和总数的对比情况，且在数据前方有上升或者下降箭头提示，其中黑色数据为所选时间的事件类型，灰色为要对比时间的相应的事件类型，且在上方有日期提示。

5.6.3 流量统计

流量统计主要是对各个审计服务器审计到的数据的流量，按照流量的类型进行分类统计。通过查看统计到的流量类型协助用户分析服务器在所选时间内进行的数据流量。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏中的"统计分析->流量统计"菜单，进入流量统计界面（默认为全部服务器的"今天"的所有流量的比特数统计）。

5.6.3.1如何进行统计分析

此项设置方法同 SQL 操作类型统计中设置方法相同。

5.6.3.2如何查看分析结果

设置好查询条件后，点击 

按钮，统计结果即显示在下方。

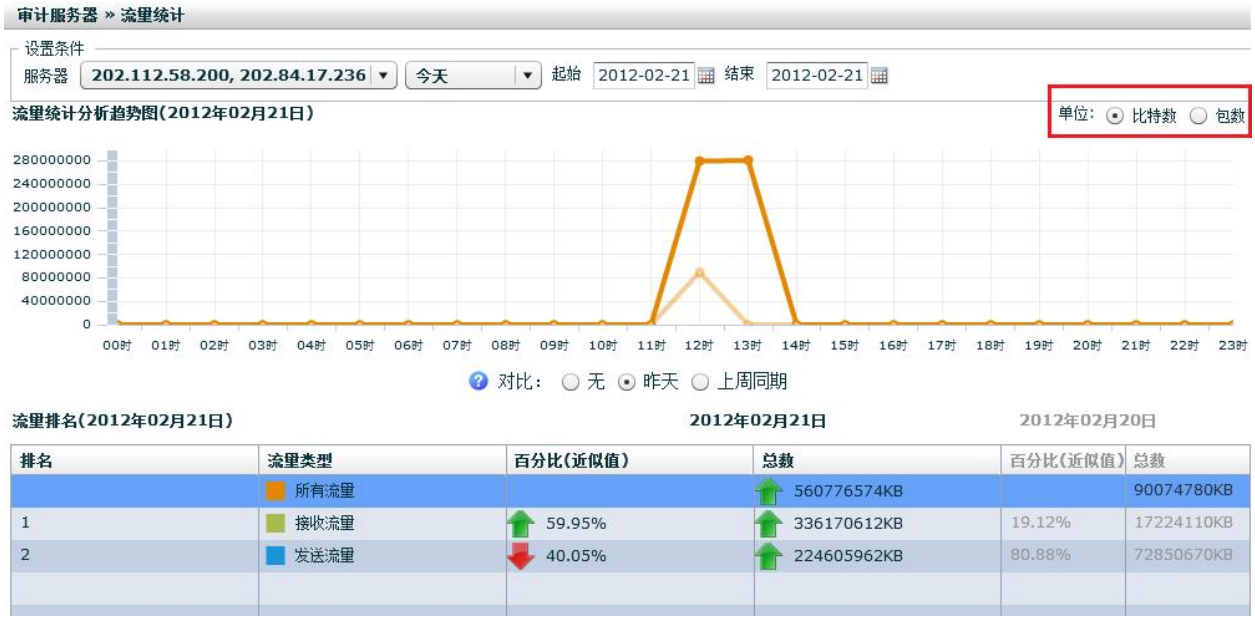
统计的结果分为"流量统计分析趋势图"和"流量排名"两种方式展示。

1、 流量统计分析趋势图用来展示所选条件的流量按时间的统计趋势，当鼠标放在趋势图节点时，会展示该节点所在时间的统计信息，如下图所示：

2、 流量排名用来展示所统计的各个流量类型的排名、流量类型、百分比、总

数。

3、 流量统计分析趋势图和流量排名均有对比操作，而且按单位分为比特数和包数两种对比情况。如下图所示，若点击对比昨天：



流量统计分析趋势图中有所选时间和要对比时间的曲线图，其中较深颜色的曲线为所选时间统计曲线，较浅颜色曲线为要对比时间的统计曲线；流量排名中有百分比和总数的对比情况，且在数据前方有上升或者下降箭头提示，其中黑色数据为所选时间的流量统计，灰色为要对比时间的相应的流量统计，且在上方有日期提示。

5.7 策略中心

5.7.1 策略配置

以拥有"策略配置"功能权限的用户登录系统，鼠标点击左侧导航栏"策略中心—>策略配置"，即可打开"策略配置"界面。

左侧显示事件类型列表，即基于事件类型将所有策略进行分组。系统内置"未知事件"的事件类型。

当一条操作行为被策略命中生成事件后，这条事件的事件类型就是这个策略所在分组的事件类型名称。

5.7.1.1如何设置事件类型

在添加审计策略前需要先添加事件类型。

点击“添加事件类型”按钮，右侧上方显示可编辑事件类型信息。

其中“响应方式”处可选择一个行为匹配了该事件类型下对应的策略后是“记录”还是“不记录”；勾选“SNMP”可设置一个行为匹配了该事件类型下对应的策略后发送一个 SNMP 日志给指定的目的地，配置方式为 IP:端口；勾选“日志”可设置一个行为匹配了该事件类型下对应的策略后发送一个 syslog 日志给指定的目的地，配置方式为 IP:端口。

注意：

1、 内置的“未知事件”用于匹配所有被用户自定义策略遗漏的事件；

2、 内置的“未知事件”不允许删除，只允许更改响应方式，并且不允许在“未知事件类型”下添加策略。

在事件类型列表处，选中一条记录，即可显示“编辑”、“删除”按钮。点击“删除”，弹出如下提示：

点击"转移"，弹出策略转移对话框，如下所示：

用户可选择将其下策略转移到其他的事件类型，以避免删除该条事件类型时将其下策略也一并删除的情况。当该条事件类型记录下不包含策略时，"转移"按钮将处于不可用状态。

5.7.1.2如何设置策略

用户自定义事件类型后，即可添加策略。

点击"新建策略"进入策略信息界面：

"来源设置"处可配置策略中应用的来源规则，如下图所示：

1.选择“任意”，即为不对来源规则进行限制；

2.选择“自定来源”，即应用当前系统中存在的来源规则，可多选。点击“配置”按钮可以打开“来源规则”界面；

3.勾选“所选来源规则外”，即应用当前系统中存在的在自定来源之外的来源规则。

“时间规则”、“内容规则”配置和“动作规则”配置同上。其中“动作规则”中的“异常串”处可匹配 SQL 操作的返回信息中出现的关键字，不区分大小写，输入多个时以英文逗号分隔；“内容规则”处可根据需求选择匹配的内容规则。

策略的应用对象有三种方式，如下图所示：

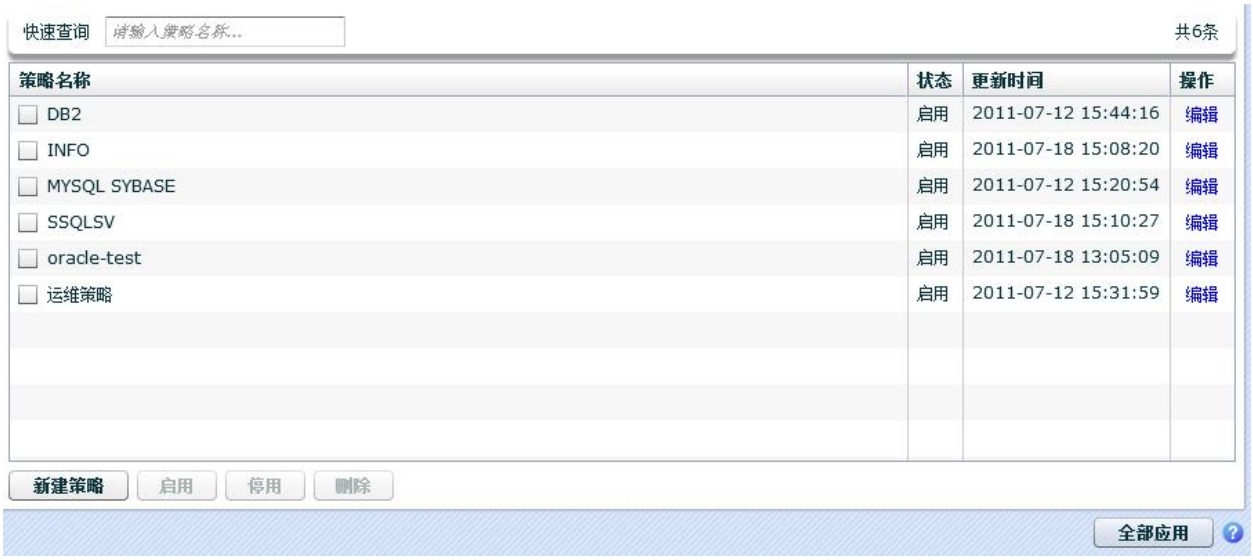
1.数据库服务器组：策略将应用于当前勾选的服务器组，匹配其下的数据库服务器。可点击右下角的“配置数据库服务器”跳转到数据库服务器界面；

2.资产组：点选“资产组”，下方的资产组下拉列表变为可用，列出了当前勾选的服务器组下的所有资产组，支持选择多个，策略将匹配资产组下的资产。可以点击右下角的“配置资产”跳转到资产界面；

3.未知资产组：策略将应用于系统内置的资产组，匹配被用户自定义遗漏的资产。

保存策略后，即可在事件类型下方的策略列表处查看各策略名称。

勾选某个策略，列表下方的“启用”“停用”“删除”按钮变为可用状态。



注意：设置策略完成后，需要点击右下角的“全部应用”按钮，使策略生效。

5.7.2 资产配置

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏“策略中心->资产配置”，即可进入资产配置界面。

通过资产配置界面可对审计数据库服务器下的资产进行配置，包括添加自定义资产，添加自定义资产到逻辑资产组。

资产配置界面左侧列出已有的审计数据库服务器，界面右侧列出服务器所属的资产组列表。

点击界面左侧下方的“添加数据库服务器”按钮可添加审计数据库服务器。

点击界面右侧下方的“新建资产组”按钮可添加资产组。

点击资产组右侧的“编辑”可编辑资产组。

点击界面右侧下方的“复制”按钮可复制资产组。

点击资产组右侧的“删除”或点击界面右侧下方的“删除”按钮可删除资产组。

排序： 点击资产组名称和资产数可进行升、倒序排列。

快速查询： 输入资产组名称的部分或全部可快速查询到资产组。

全部应用： 点击全部应用，界面上所有的配置都将被应用并生效。

5.7.2.1添加/编辑资产组

选中资产配置左侧的审计数据库服务器后，右边列出该数据库服务器下已有的资产组，点击“新建资产组”按钮或点击资产组列表中的“编辑”，进入到资产组配置页面。

在资产组配置页面，可输入资产组名称，资产组说明，通过点击“添加资产”按钮对资产组添加资产。

排序： 点击资产名称可进行升、倒序排列。

快速查询： 输入资产名称的部分或全部可快速查询到资产。

5.7.2.2添加/编辑/删除资产

1．添加资产

在资产配置页面上点击“添加资产”按钮，弹出“添加资产”页面。

在添加资产页面上，有两种方式添加资产：

“已存在资产”列表上列出同一个服务器下其它资产组已添加的自定义资产，通过打勾可添加同一服务器下其它资产组下的自定义资产到新的资产组。

也可以通过在“手动添加”处输入新的资产名。

下图是添加资产示例：

2．导入内置资产

点击“导入内置资产”，系统展示内置到服务器组下的资产组列表，对内置到服务器组下的资产组打勾，然后点击“导入”按钮，内置资产组下的资产被添加到资产组。

3．编辑资产

点击资产列表中的已添加的资产“编辑”，可进入到编辑资产页面，编辑资产页面示例如下：

4．删除资产

点击资产列表中的“删除”，弹出确认删除资产页面，确认删除后点击“保存”回到资产组列表处。

5.7.2.3复制资产组

在资产配置页面上选中已有资产组，点击“复制”按钮，弹出复制资产组页面。

复制资产组功能对选定资产组复制为另一个资产组， 包括资产组下的资产也被复制。复制资产组需要输入新的资产组名称。

下图是复制资产组示例：

5.7.2.4删除资产组

在资产配置界面，点击资产组列表中右侧的“删除”或界面右侧下方的“删除”按钮，弹出确认删除对话框。

在确认删除对话框中，选择确定删除资产组后，资产组和资产组下的自定义资产均被删除。

5.7.3 来源规则

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏“策略中心->来源规则”，即可进入来源规则页面。

来源规则可用于配置审计数据的来源。

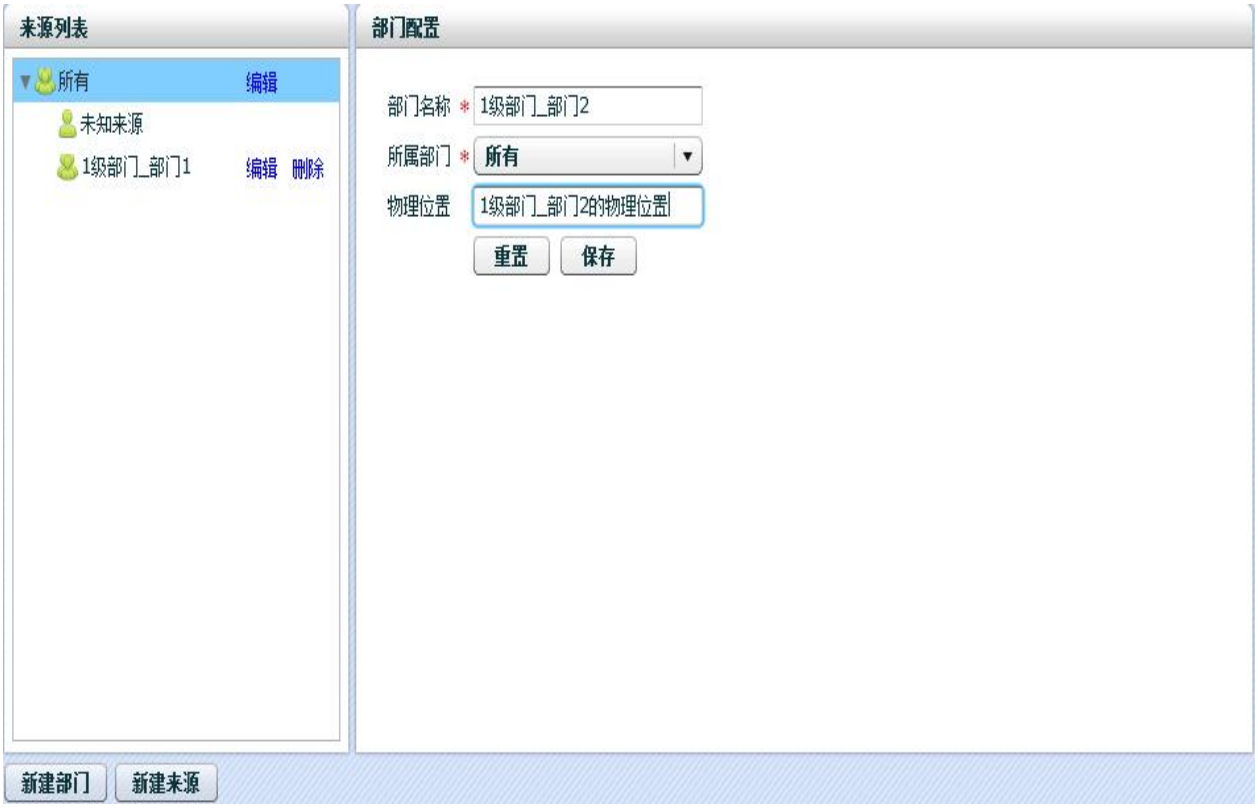
通过点击“新建部门”和“新建来源”按钮，添加不同的部门和来源。部门之间是树状结构，每个

部门下都可以添加来源。

5.7.3.1新建/编辑/删除部门

1．新建部门

在来源规则页面，点击“新建部门”按钮后，可进入新建部门页面，如下图添加部门示例：



2．编辑部门

在来源列表中点击部门右侧的“编辑”，即可对部门重新进行配置，同点击“添加部门”。

3．删除部门

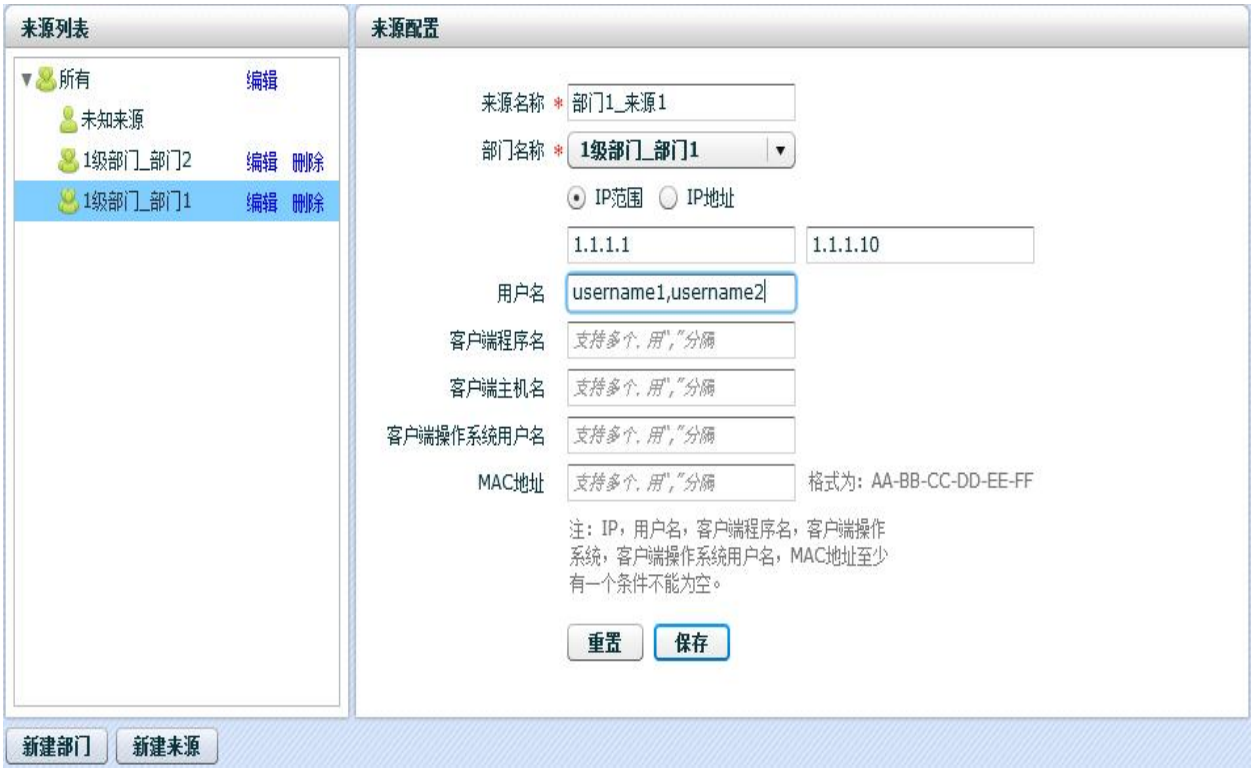
在来源列表中点击部门右侧的“删除”，即可对选中部门及隶属这个部门的子部门和来源一起删除。

5.7.3.2新建/编辑/删除来源

1．新建来源

在来源规则页面，选中需要添加来源的部门，再点击“新建来源”按钮后，可进入新建部门页面。

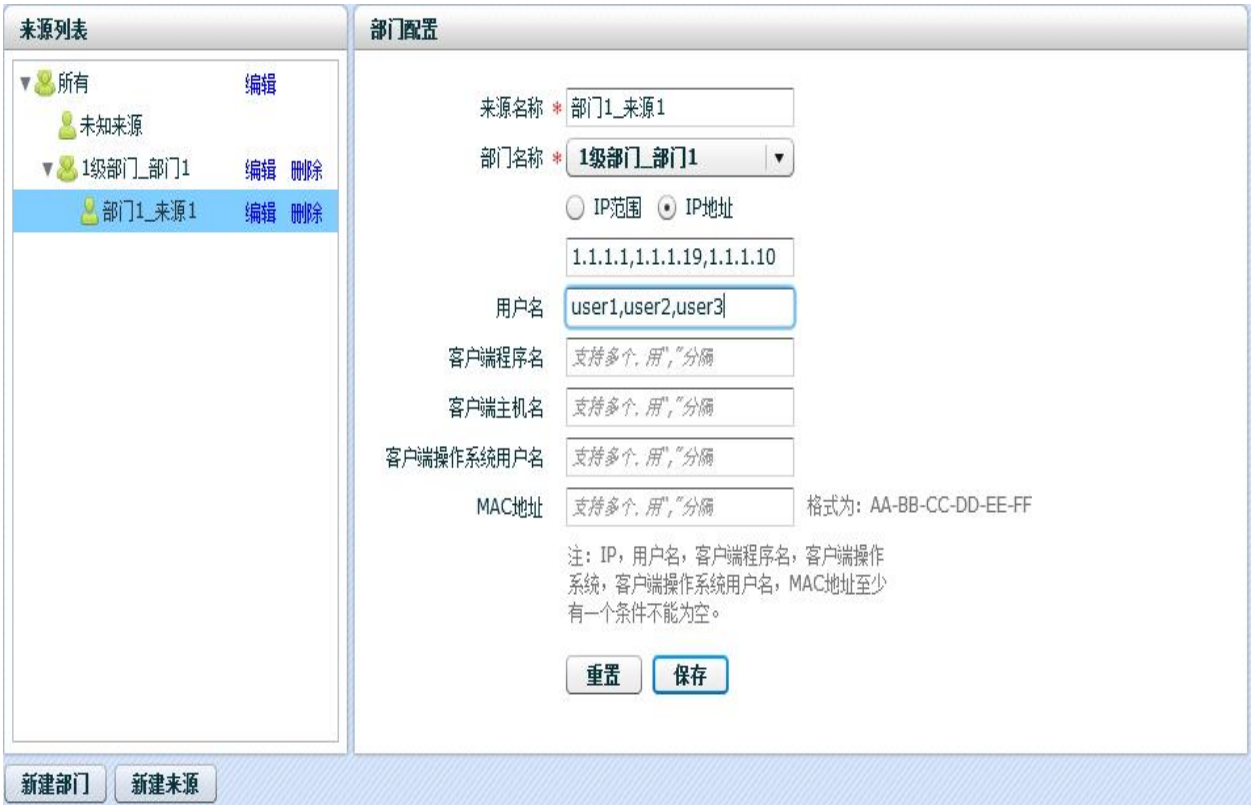
如下图是对“1 级部门_部门 1”部门添加来源示例：



2．编辑来源

点击来源列表中来源名称右侧的“编辑”，可对来源进行编辑。

下图是对“部门 1_来源 1”来源的编辑示例：



3．删除来源

点击来源列表中来源名称右侧的"删除"，可删除选定来源组。

5.7.4 时间规则

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏"策略中心->时间规则"，即可进入时间规则页面。

时间规则可用于配置审计数据的周日历或时间段。

通过点击"新建"按钮，添加不同的时间规则。

5.7.4.1新建时间规则

在时间规则页面，点击"新建"按钮后，可进入新建时间页面。时间规则可选择周日历或时间段两种格式。

如下图是设置周日历时间为每周的周一到周五的 9：00：00-18：30：00 的时间规则示例：

如下图是设置时间段从 2011/06/06 00：00：00 到 2011/06/16 23：59：59 的时间规则示例：

5.7.4.2编辑时间规则

在时间规则页面，点击时间规则列表上的时间规则右侧的“编辑”，可对时间规则进行编辑。

5.7.4.3删除时间规则

在时间规则页面，点击时间规则列表上的时间规则右侧的“删除”，可删除时间规则。

5.7.5 内容规则

以系统管理员 sysadmin 登录系统， 鼠标点击左侧导航栏“策略中心->内容规则”，即可进入内容规则页面。

内容规则可用于配置审计数据的 sql 语句中的关键字匹配。

下图是没有添加任何时间规则的示例：

5.7.5.1新建内容规则

在内容规则页面，点击“新建内容规则”按钮后，可进入新建内容规则页面。内容规则规则类型可选关键字或者正则表达式进行匹配，并在下面的空白区域配置要匹配的关键字或正则表达式。

5.7.5.2编辑内容规则

在内容规则页面，点击内容规则列表上的内容规则右侧的“编辑”，可对内容规则进行编辑。

5.7.5.3复制内容规则

在内容规则页面上选中已有内容规则，点击“复制”按钮，弹出复制内容规则页面。

复制内容规则功能对选定内容规则复制为另一个内容规则， 包括内容规则下的配置也被复制。复制内容规则需要输入新的内容规则名称。

下图是复制内容规则示例：

5.7.5.4删除内容规则

在内容规则页面，点击内容规则列表上的内容规则右侧的“删除”，可删除内容规则。

5.8 报表中心

系统为用户提供报表，以各种方式统计审计数据，方便用户查看。

5.8.1 如何预览报表

以拥有“历史报表管理”功能权限的用户登录系统，鼠标点击左侧导航栏“报表中心->历史报表管理”界面，即可进入历史报表管理界面。

左侧“报表模板”区域显示系统默认提供的模板，用户可点击某个模板右侧的“手动报表”，然后配置好该报表需要的各项参数：

各种报表模板的参数主要有以下几种：

报表名称：报表生成后的文件命名

时间范围开始时间：报表统计数据的开始时间，默认为昨天的 00:00:00；

时间范围结束时间：报表统计数据的结束时间，默认为昨天的 23:59:59；

审计数据库服务器：报表统计的指定服务器 ip 地址；

生成格式：报表下载后的文本格式 docx、html、pdf、pptx 及 xlsx；

用户设置各项参数后，选择 html 的生成格式，点击"预览"按钮，浏览器打开新界面，在新界面中可预览生成的报表。

5.8.2 如何手动生成报表

以拥有"历史报表管理"功能权限的用户登录系统，鼠标点击左侧导航栏"报表中心->历史报表管理"界面，即可进入历史报表管理界面。

左侧"报表模板"区域显示系统默认提供的模板，用户可点击某个模板右侧的"手动报表"，然后配置好该报表需要的各项参数：

各种报表模板的参数主要有以下几种：

报表名称：报表生成后的文件命名

时间范围开始时间：报表统计数据的开始时间，默认为昨天的 00:00:00；

时间范围结束时间：报表统计数据的结束时间，默认为昨天的 23:59:59；

审计数据库服务器：报表统计的指定服务器 ip 地址；

生成格式：报表下载后的文本格式 docx、html、pdf、pptx 及 xlsx；

用户设置各项参数后，点击手动报表对话框中的"下载"按钮，浏览器打开新界面，然后弹出文件下载对话框，此时可以选择相应操作，执行打开或保存下载功能。

注意：如果下载报表时选择"html"格式，导出文件为压缩包，需解压。

5.8.3 如何使用自动报表

以拥有"报表模板管理"功能权限的用户登录系统，鼠标点击"报表中心->报表模板管理"，进入报表模板管理界面。

根据用户实际需要，系统内置几种不同的报表模板，用户可以根据系统内置的报表模板添加报表，并可以对其进行编辑或删除等操作。

5.8.3.1如何添加报表

选中某一个报表模板，点击页面右下角的"添加报表"按钮，即可根据该报表模板添加报表。

报表配置包括：报表信息、报表参数以及报表任务。其中报表信息包括：所选模板（不可编辑）、报表名称（不允许为空）、报表描述以及标签。报表参数根据报表模板不同，有时需要选择审计数据库服务器。报表任务包括： 接收人、输出格式以及时间。编辑各项信息后，点击界面右下方的"保存"按钮，报表成功保存，回到报表模板管理界面。

5.8.3.1.1 如何使用报表标签

报表配置报表信息中有一个标签输入框，用户可以为自己添加的报表添加标签，标签用于在报表模板界面或历史报表管理界面根据标签名快速过滤报表。

5.8.3.1.2 如何配置报表任务

在报表配置页面的报表任务信息栏中，用户可以对自动报表进行任务设置。

报表接收人：指定自动报表的收件人，需输入完整的 email 地址，多个收件人之间以“,”分开；

输出格式包括：docx、html、pdf、pptx 和 xlsx

任务时间包括：

每日：每天将系统所在天前一天的数据以事先设定的报表格式发送给报表接收人；

每周：每周将系统所在周前一周的数据以事先设定的报表格式发送给报表接收人；

每月：每月将系统所在月前一月的数据以事先设定的报表格式发送给报表接收人。

注意：

1． 对三种时间的自动报表任务，系统触发时间有所不同。每日任务的触发时间是次日凌晨 1:00，统计前一日的数据；每周任务的触发时间是每周 1 凌晨 2:00，统计前一周的数据；每月任务的触发时间是每月 1 号凌晨 3:00，统计前一月的数据。

2． 自动报表的邮件服务器在“系统管理—工作参数”的“邮件 SMTP 服务器”中配置，具体可参见“5.8.4.2 如何进行邮件服务器配置”。

5.8.3.2如何编辑、删除报表

在报表任务列表处，点击某个报表任务右侧的“编辑”按钮，即可打开该报表配置界面，用户可对其进行编辑。修改了相应参数后，“保存”按钮变为可用状态，点击“保存”后，系统回到报表列表界面。

注意：不允许添加名称相同的报表，会给出提示：报表名称已存在。

点击某个报表任务右侧的“删除”按钮，弹出删除确认提示。确认后该报表即被删除。

5.8.4 如何使用历史报表

历史报表处是对已经自动生成的报表任务进行管理。

以拥有“历史报表管理”功能权限的用户登录系统，鼠标点击左侧导航栏“报表中心->历史报表管理”界面，即可进入历史报表管理界面。

历史报表管理界面的左侧“报表模板”下面有一个下拉按钮，可以根据系统设定的分类标准对报表模板进行快速过滤。当用户选中某一个报表模板后，界面右侧显示其对应的历史报表生成记录。历史报表信息包括：报表名称、报表模板、生成时间、接收人、生成格式、标签以及状态。

用户可以选中某条生成记录或者几条生成记录，点击右下角“删除”按钮，可将该条生成记录删除；点击“导出”按钮，界面弹出导出对话框，点击“导出”按钮，选择目标地址保存后，即可导出历史报表文件。

注意：

1.导出历史报表会把选中的所有报表压缩成一个名为“报表.zip”包，需要解压。

2.若报表自动生成时失败，该条记录会显示为红色，点击状态列的“重新生成”可以将报表重新生成，并可按照需要将其导出。

5.9 系统配置

系统配置，包括审计数据库服务器、审计 WEB 中间件、知识库、IP 采集条件、工作参数、角色管理、补丁管理、授权管理、备份/还原、重启/关机等十个子菜单，以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏“系统配置”选择相应菜单，即可进入相应界面。

5.9.1 审计数据库服务器

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏“系统配置->审计数据库服务器”，即可进入审计数据库服务器界面。

点击“添加”按钮，进入“审计数据库设置”界面，用户可自定义配置审计服务器组名称、数据库类型、版本以及该组下的多个审计数据库服务器的详细信息。

例如，可选择服务器组审计对象为 DB2 类型的数据库，下方的数据库列表处列出多个 db2 类型的审计服务器的信息。

其中，端口显示为数据库的默认端口，如 DB2 默认为 50000，oracle 为 1521 等。

当需要审计某个服务器上发生的网络行为时，则需要正确勾选相应的 FTP、TELNET、SSH 端口并配置正确的服务端口。

同时，该设置也将作为攻击检测中的审计对象被实时监控。

注意：勾选"数据过滤"可以配置过滤条件，此处可以对指定的 SQL 操作类型和来源进行过滤。符合条件的数据将在审计过程中直接被丢弃不被审计。

如上图所示，该审计服务器上发生的 INSERT、SELECT、UPDATE 操作将不会被审计。

注意：配置数据库服务器信息后（包括添加、编辑、删除），在门户界面的右上角红色气泡处生成消息，提醒同步，如下图所示：

需要点击"同步"，并看到"同步成功"的提示后，配置才能生效

5.9.2 审计 WEB 中间件

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏"系统配置->审计 WEB 中间件"，即可进入中间件配置界面。

点击"添加"按钮，用户可自定义配置 WEB 中间件的名称、IP、端口以及关联关系的审计。

如上图，系统将审计 IP 为 192.168.0.100 且端口为 80 的 WEB 中间件行为。

如需关联审计，则需要添加关联关系。方法如下：

勾选“中间件关联”，点击“添加关联关系”按钮，如下图所示：

系统默认中间件服务器即为中间件作为客户端访问数据库的 IP，“数据库服务器”的下拉列表处显示了当前系统已存在的所有数据库服务器的 IP 地址，“中间件访问 URL”处可配置 URL 关键字。

设置完成后，点击“保存”即可返回中间件审计列表处，且看到系统中已添加的中间件的各项信息。如下图所示：

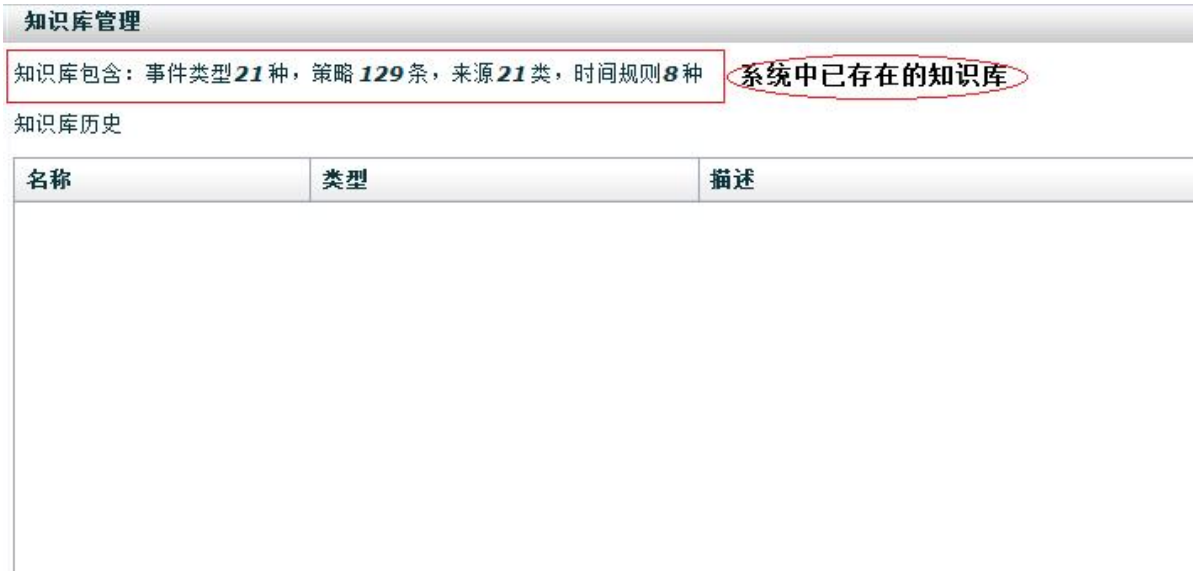
注意：配置 WEB 服务器信息后，在门户界面的右上角红色气泡处生成消息，提醒同步，如下图所示：

需要点击"同步"，并看到"同步成功"的提示后，配置才能生效。

5.9.3 知识库

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏"系统配置->知识库"，即可进入知识库配置界面。

知识库是用来配置数据库审计系统的内置事件类型、策略、来源、时间规则。如下图所示：



点击右下方的 

按钮，可导入由数据库审计系统公司根据用户需求制作的内置文件安装包，导入/修改知识库。如下图所示：

5.9.4 IP 采集条件

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏"系统配置->IP 采集条件"，即可进入采集配置界面。

默认 IP 采集功能处于开启状态。

系统会自动获取到当前已添加的审计库服务器的 IP 并将其填入"采集 IP 地址"列表处。用户还可以手动输入 IP 地址，将其添加为采集或者是不采集。

在审计过程中，系统会首先检查在"不采集 IP 地址"列表处的 IP，将其数据包丢弃不被采集；然后检查在"采集 IP 地址"列表处的地址，将其数据包进行采集；最后按照界面下方的'不在以上 IP 地址范围内数据'的处理方式来确定剩下的数据包是采集或是采集。

注意：

1. 系统默认"不在以上 IP 地址范围内数据"的处理方式为"不采集"，即列表范围外的 IP 数据包将被丢弃不采集。

2. 保存 IP 采集条件配置后，需要点击右下角的"同步"按钮配置才能生效；或在门户界面的消息提醒处点击策略"同步"并看到"同步成功"的提示后配置生效。

5.9.5 工作参数

在工作参数设置界面，可以设置时间、邮件 SMTP 服务器、磁盘预警、授权预警、数据处理、户登陆安全性和页面超时。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏"系统配置->工作参数"，即可进入到工作参数设置界面。

5.9.5.1如何进行时间设置

时间设置，即用户可以设置系统的日期和时间，也可以将其与某个主机或 IP 地址的计算机时间进行同步设置。

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的"系统配置->工作参数"，进入工作参数界面，在"工作参数设置"界面左上角有"时间设置"栏，默认是系统当前日期和当前时间。如下图所示：

用户可以通过单击按钮更改日期和时间。

用户可以单击时间按钮，在下拉菜单中选取时间，也可以进行手动输入，如图所示：

若将时间设置与输入的主机名或者 IP 的时间进行同步。对时间设置的"时间服务器"进行设置，如下图所示：

按照提示输入主机名或者 IP 后，"同步"按钮变为可用，例如：输入 IP 为 192.168.56.3，如下图所示：

可点击"同步"将当前系统时间与该处的时间服务器同步。

点击"保存"按钮，将弹出如下提示：

点击"确定"按钮，进入登录界面。

5.9.5.2如何设置邮件 SMTP 服务器

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的"系统配置->工作参数"，进入工作参数界面，在"工作参数设置"界面左下角有"邮件 SMTP 服务器"设置一栏，在此栏可以输入姓名、邮件地址、SMTP 服务器、端口、服务器测试，可以选择是否加密，还可以通过身份认证输入用户名和密码。如下图所示：

姓名、邮件地址、SMTP 服务器，可以按照提示信息输入。

输入邮件地址时，若输入正确，方框显示为蓝色，如下图所示：

若输入有误，方框变为红色框，并且会标注错误提示，如下图所示：

“加密”项，可以通过后面的下拉菜单选择是或否，当选择“否”时，默认端口是 25，可以通过上下键改变端口；当选择“是”时，默认端口是 465，可以通过上下键改变端口。

当“身份认证”被勾选的时候，需要“输入用户名和密码”，如图所示：

如果要更改用户名和密码，点击“重置”按钮即可。

服务器测试一栏，当输入接收者邮件地址的时候，其后的"测试"按钮变为可用。若邮件地址输入正确，方框显示为蓝色框，如图所示：

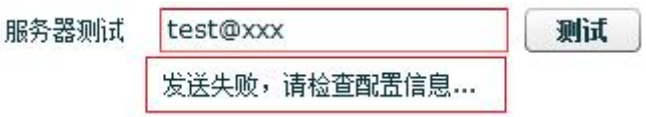
若邮件邮件输入有误时，方框变为红色框，并且会标注错误提示，如图所示：

按照要求，每一项都正确填写后，点击"测试"按钮，对当前所填写内容进行测试。若测试成功，将在服务器测试下面将显示"发送成功"。

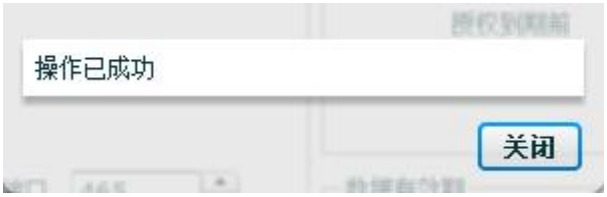
并且，在所填写的邮件地址中会收到一封邮件，内容为："恭喜您，当您 收到该邮件时，您的邮件服务器测试已通过！"

若测试失败，将弹出错误告警提示，如下图所示：

同时在服务器测试方框下面，给出如下发送失败提示：



所有信息都输入完成，单击"保存"按钮保存当前输入信息，并弹出如下提示：



点击“关闭”按钮，返回到工作参数设置界面。

5.9.5.3如何设置磁盘预警

磁盘预警功能，即系统硬盘的磁盘空间预警功能。支持检测系统的磁盘占用率功能，提供预警的配置界面，支持磁盘占用率的预警阀值设置。

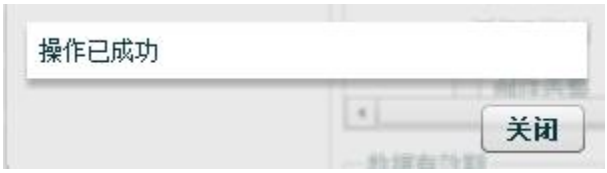
以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的“系统配置->工作参数”，进入工作参数界面，右上有“磁盘预警”一栏，如下图所示：

预警阀值（磁盘使用率%）：审计中心设备磁盘的审计数据存储区使用率预警阀值，**默认预警阀值为 80%，可配范围 50-89%。**当审计中心设备磁盘的审计数据存储区占用率达到预设的预警阀值时，向配置的邮件地址发送磁盘空间预警邮件，每天一封，直至审计中心设备磁盘的审计数据使用区使用率低于所配置的报警阀值；

保护阀值（磁盘使用率%）：审计中心设备磁盘的审计数据存储区使用率保护阀值，**默认保护阀值为 90%，可配范围 50-98%。**当审计中心设备磁盘的审计数据存储区使用率达到预设的保护阀值时，系统会根据"处理方式"中的选项采取数据保护措施；

处理方式：当审计中心设备磁盘的审计数据存储区使用率达到保护阀值时，系统采取的数据保护措施。审计中心系统**默认选择"数据停止记录"保护策略**，即当审计中心设备磁盘的审计数据存储区使用率达到保护阀值时，系统将自动停止审计，不再增加新的审计数据；选择"覆盖"保护策略，当审计中心设备磁盘的审计数据存储区使用率达到保护阀值时，系统将覆盖之前的审计数据，直到磁盘使用率低于所配置的保护阀值。

通过点击  ，可以改变预警阀值和保护阀值，设置好后，点击"保存"按钮，弹出如下提示：



点击"关闭"按钮，返回到工作参数设置界面。

5.9.5.4如何设置授权预警

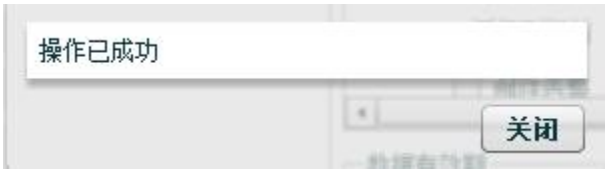
授权预警，即系统的授权使用时间预警。

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的"系统配置->工作参数"，进入工作参数界面，右中有"授权预警"一栏，如下图所示：

通过点击，设置授权天数提示。当审计中心的授权距离授权到期时间小于或等于此处配置的发送时间时，系统将每天向所配置的邮件地址发送一封授权到期提醒邮件。

默认时间授权到期前 30 天邮件告警提示，可配范围 1-100 天。

设置好后，点击"保存"按钮，弹出如下提示：



点击"关闭"按钮，返回到工作参数设置界面。

5.9.5.5如何设置数据处理

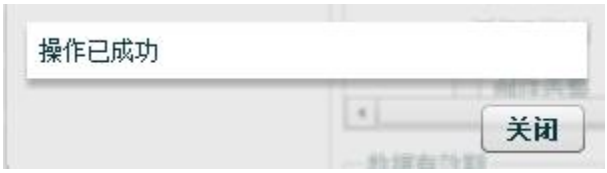
数据处理，即对审计系统的数据进行审计数据保留时间设置（只保留有效期内的数据）以及缓存表数据超过多少条后提示的设置。

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的"系统配置->工作参数"，进入工作参数界面，右中有"数据处理"一栏：

对审计数据保留天数进行设置。保留设置天数内的审计数据，超过设定天数，将删除审计数据。

系统默认设置审计数据保留 30 天后删除，可配保存范围为 0-365 天。

通过点击，可以改变审计数据保留时间，设置好后，点击"保存"按钮，弹出如下提示：



点击"关闭"按钮，返回到工作参数设置界面。

对缓存表数据超过多少条后提示设置。缓存表数据超过设定值后会在首页给出气泡提示。默认设置为 600000。可配范围为 1- 99999999。

通过点击  ，可以改变缓存表数据设置，设置好后，点击"保存"按钮，弹出"操作已成功"的窗口。点击"关闭"按钮，返回到工作参数设置界面。

5.9.5.6如何设置用户登陆安全性

用户登陆安全性，即限定用户安全登录次数，连续登录失败超过设定次数，系统将自动锁定。在锁定时间内，不可以再次登录。只有超过锁定时间，用户再次刷新登录界面后，重新输入用户名和密码进行登录。

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的"系统配置->工作参数"，进入工作参数界面，右下角有"用户登陆安全性"一栏，如下图所示:

（1）最大连接登录失败 n（0-20 以内的任意整数）次后系统锁定

通过点击  ，改变次数。

（2）锁定时间

通过点击  ，改变锁定时间。

系统默认最大连续登录失败 5 次后系统锁定，可配次数范围 0-20 次。

系统默认锁定时间为 5 分钟，可配锁定时间范围为 1-9999 分钟。

当设置最大连续登录失败 0 次后系统锁定时，锁定时间不可设定。

设置好后，点击"保存"按钮，提示操作已成功，即对当前设定进行保存。

例如：设置用户最大连接登录失败五次，超过五次系统将锁定登录界面，并在登录界面给出如下提示：

设置锁定时间为五分钟，当超过锁定时间后，刷新方可进入初始登录界面。

5.9.5.7页面超时

页面超时默认为 10 分钟，即登录系统后 10 分钟无操作就会提示超时登录，用户需要重新登录系统。

在此处配置超时时间为 0 时，表示界面永不超时。

5.9.6 角色管理

"角色管理"显示当前系统的所有角色列表，展示列包括：角色名、描述、更新时间和所含用户。

用户自定义添加的用户必须要隶属于相应的角色，以限制其对该审计系统的管理、查看的权限。

系统默认的角色有：报表使用者、统计分析员、报表管理者、外审计员、安全观察员、性能监控员、策略管理员、内审计员、系统管理员以及安全管理员。

注意：只有系统管理员 sysadmin 才能有权限进行角色管理，其余用户均没有此权限。

以系统管理员 sysadmin 登录系统，鼠标点击左侧导航栏"系统配置->角色管理"，即可进入到角色管理界面。

5.9.6.1如何添加角色

如果要添加新角色，点击角色管理界面左下角的 

按钮，进入到角色设置界面。

（1）角色名称和描述

"角色名"是必填项且具有唯一性的，不允许重复，否则会给出提示：角色名已存在。如下图所示：

在描述栏内，对将要添加的角色进行描述。

（2）权限分配

初始添加角色后默认该角色没有被分配任何权限。

功能权限的左侧列出可以分配的全部功能权限（包括：首页、审计中心、攻击监测、性能分析、统计分析、策略中心、报表中心、系统配置），用户可以勾选某个或全部功能，将功能权限分配给将要添加的角色。选中某个权限后"保存"按钮变为可用。点击"保存"，完成角色添加；点击"重置"，此时权限状态变为用户上一次保存时的状态；点击"取消"，取消角色添加。

如果权限设置设定有误，点击 重置 按钮，清楚勾选项，更改权限设置；如果确认无误，点击 保存 按钮，对当前新添加角色进行保存，并且，将新添加角色显示到角色列表中；如果取消添加，点击 取消 按钮，返回到角色管理界面。

5.9.6.2如何编辑角色

用户可以对角色重新编辑，包括角色名称、角色描述以及角色权限设置。在"角色管理"界面，选择要修改角色项，如"admin"，点击 编辑 按钮进入编辑角色界面。

如果权限设置有误，点击 重置 按钮，重新更改权限设置；如果确认无误，点击 保存 按钮，对当前编辑角色进行保存，并显示到角色列表中；如果取消编辑，点击 取消 按钮，返回到角色管理界面。

5.9.6.3如何删除角色

在"角色管理"界面，选择要删除角色，如 admin1，点击 删除 按钮，弹出提示，如下图所示：

点击 删除 按钮，所选角色被删除。点击 取消 按钮，所选角色不删除，并关闭对话框返回到角色管理界面。

5.9.7 补丁管理

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的"系统配置->补丁管理"，进入"补丁管理"界面。

补丁管理界面包括设备名和操作，设备名分为：审计中心和探针，可以对审计中心和探针进行上传或升级操作。

注：审计中心和探针的补丁设备名处显示了当前软件版本信息。

升级补丁成功后，该补丁会同时显示在审计中心和探针处。

5.9.7.1如何进行补丁上传

（1） 鼠标左键点击列表中一个审计中心或探针后面的 上传 按钮，系统将弹出文件选择对话框，

正确选择要上传的补丁包文件并点击"打开"，即可进行补丁包上传。在上传时，会提示上传进度对话框，如下图所示：

点击进度条窗口的 × 按钮将其关闭，返回到补丁管理界面。

5.9.7.2如何进行补丁升级

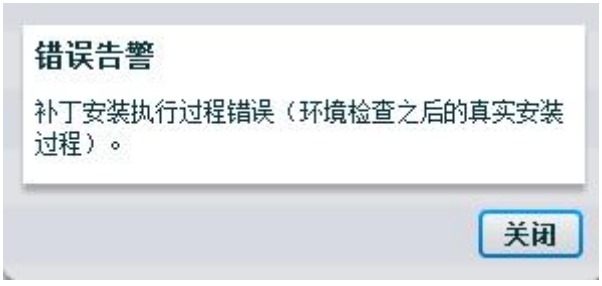
（1）升级成功

在补丁包上传后，点击 升级 进行审计中心或探针的升级，若升级成功，弹出如下提示对话框：

点击“确定”按钮，返回到补丁管理界面，原“升级”按钮变为不可用状态。

（2）升级失败

在补丁包上传后，点击 升级 进行审计中心或探针的升级，如果升级过程没有正确完成，系统将弹出提示：



点击“关闭”按钮，返回到补丁管理界面。

5.9.7.3如何查看已上传补丁及进行补丁卸载

（1）查看已上传补丁

注：只有将文件“上传”并成功“升级”后，才能在界面显示已上传的补丁文件。

将文件上传并成功升级后，补丁安装成功，此时，审计中心或者探针前面出现  按钮，点击它，由  变成  ，在审计中心或者探针下面才会显示出已成功安装的补丁。

（2）补丁卸载

如果安装的补丁包是在另个一补丁包目录下，此时，若卸载补丁包，需要逐级卸载。

5.9.8 授权管理

5.9.8.1如何进行授权

以系统管理员 sysadmin 登录系统，鼠标左键点击左侧导航栏中的“系统配置->授权管理”，进入“授权管理”界面。

授权管理分为两个部分：授权信息和授权状态。首次登录系统时，左侧授权信息的授权状态显示为“未授权”，如要授权，点击 

按钮，弹出如下对话框：

（1）创建授权文件

注：“ * ”表示为必填项，同时在选中“ * ”后面的方框时，会有如下提示对话框：

填好相应信息后，方框的颜色有红色变为蓝色，如下图所示：

将信息全部填写完成后，点击下方的 创建授权文件 按钮，系统会弹出保存文件对话框，选择保存目录，点击“保存”，保存生成的“license_request**.zip”文件，返回到“授权”界面，点击右下角的 确定 按钮，返回到“授权管理”界面。

（2）导入授权文件

将保存后的“license_request**.zip”文件发送给相关授权人员，相关授权人员将会返回相应的授权文件，在授权管理界面，点击“授权”，重新进入授权界面，然后点击 导入 按钮，导入授权文件，此时，导入按钮后面的 授权 按钮变为可用。

（3）授权

点击 授权 按钮，如果授权失败，在导入授权文件下面以红色字体显示“授权失败”的提示，

如下图所示：

如果授权成功，在导入授权文件下面以红色字体显示“授权成功”，如下图所示：

并且，弹出如下对话框：

点击“确定”按钮，界面将重新返回到用户登陆界面。

注：有了授权文件，每次重新安装审计中心和探针后，直接导入并授权即可。

5.9.8.2如何查看授权信息

点击左侧导航栏中的“系统配置->授权管理”，左侧为用户的授权信息，右侧为授权状态。

授权成功后，单位名称、系统使用部门、联系人姓名、联系人电话以及联系人邮箱将与创建时一致，此时授权状态为“已授权”，并且显示了授权到期的天数。

用户还可以点击“备份授权文件”，选择目标地址后，将以 license_backup.zip 文件格式备份授权文件。

注意：

审计服务器数量：指该审计中心可审计的最大审计服务器数，当”策略配置->规则配置->审计服务器”中所配置的审计服务器数达到此审计服务器数时，该审计中心将不能再配置更多的审计服务器数；

探针数量：审计中心被注册的探针数；

授权服务：指该审计中心可审计的服务类型，一台审计中心只能对已授权的服务类型进行审计，没有授权的报务类型则不能审计。

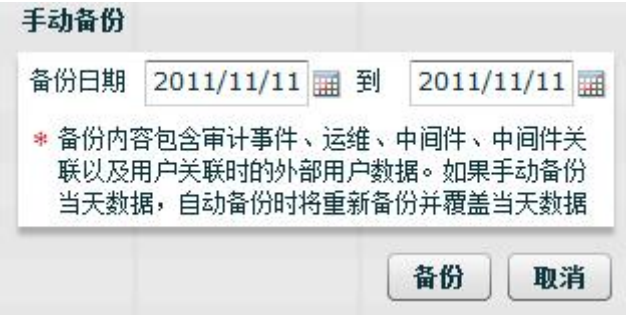
5.9.9 备份/还原

“备份/还原”，就是对审计事件进行备份和还原。

鼠标点击左侧导航栏中的“系统配置->备份/还原”，进入界面。

5.9.9.1如何手动备份

点击“手动备份”，进入如下界面：

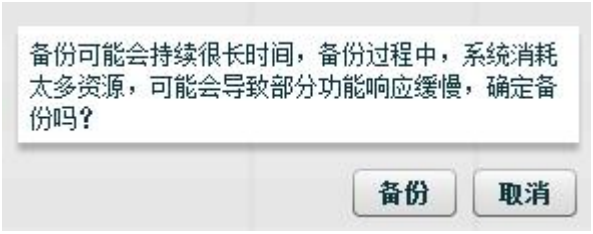


手动备份默认包含审计事件、运维、中间件、中间件关联以及用户关联时的外部用户数据。

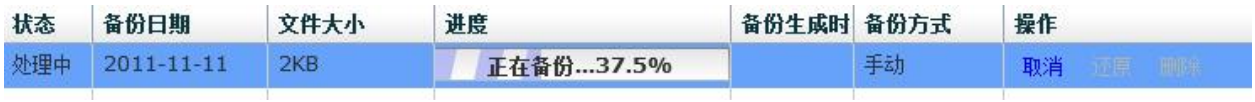
手动备份的日期可以选择 1 天或一个起始终止时间段。

手动备份单天数据示例：

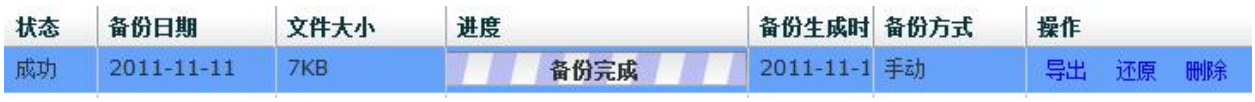
在备份日期里选择 2011/11/11 到 2011/11/11 的备份过程示例：



点击“备份”，进行下一步：



2011/11/11 的数据备份完成后，界面如下显示：



取消备份

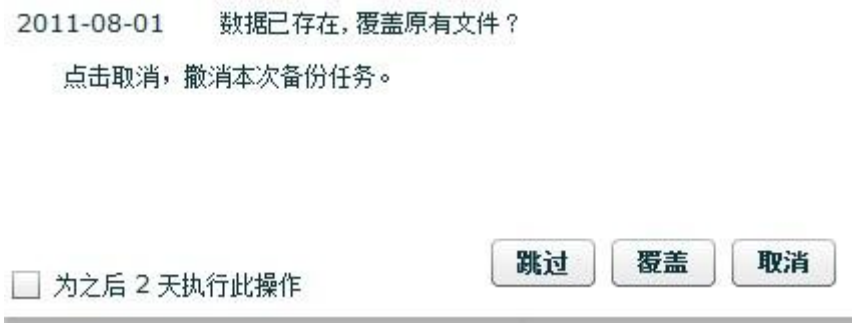
在备份过程中，点击“取消”可取消备份。

导出、删除备份

选中状态为“成功”的备份，点击“导出”可导出备份后数据的打包文件，点击“还原”可导出备份后数据的打包文件，点击“删除”可删除备份。

备份时间段时的覆盖和跳过

备份列表中已成功备份 2011/08/01 到 2011/08/03 的备份，手动备份重新选择 2011/08/01 到 2011/08/03 进行备份，确定备份后，页面上弹出如下对话框：



点击“跳过”表示忽略重新备份 2011/08/01 的备份任务。

点击“覆盖”表示重新备份 2011/08/01 的数据。

点击“取消”表示撤消本次备份任务 。

打勾“为之后 x 天执行此操作”，按选择“跳过”或“覆盖”的方式同样处理接下来的 2011/08/02 和 2011/08/03 的备份任务。

5.9.9.2如何自动备份

自动备份开启后，在每日的 00:00:00 开始自动备份前一天的数据，备份审计事件。

点击自动备份旁边的"开"或"关"，并确认"开"或"关"，系统将开启/停止每日自动备份。

5.9.9.3备份转储

点击"备份转储"，进入如下界面：

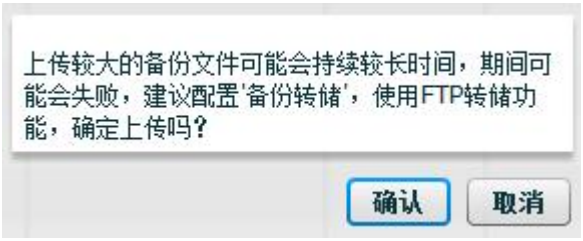
填写 FTP 的 IP 及端口，用户名，密码，以及备份文件要转储到 FTP 的路径。

如下图所示， 是将备份文件转储到 ftp://192.168.0.3/backup 文件夹下。其中 FTP 端口为 21，访问 FTP 的用户名为 user，同时还需要填写 FTP 用户的密码。

填写 FTP 设置后，点击“测试连接”，连接成功后弹出“测试成功”的提示框后，“保存”可用，点击“保存”FTP 设置，系统会自动将本地备份文件转储到 FTP 上，同时，系统也会在每天的 5:00 把本地备份文件同步到 FTP 上。

5.9.9.4上传备份文件

点击“上传备份文件”后如下图所示：



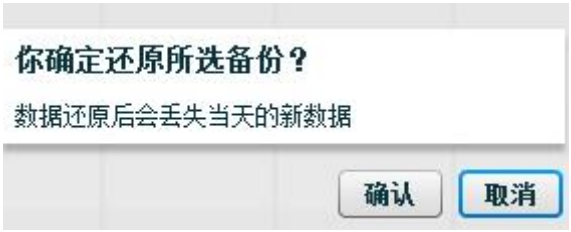
点击“确认”，弹出文件上传框，点击“浏览”，选中备份文件后，点击“上传”。

上传成功后，在备份列表中生成备份任务，如下图所示：

状态	备份日期	文件大小	进度	备份生成时间	备份方式	操作
成功	2011-11-10	8KB	备份完成	2011-11-11 16:51:19	上传	导出 还原 删除

5.9.9.5还原

当备份列表中有任务时，可通过点击"还原"对备份日期的数据进行还原，也可以通过上传备份文件生成备份任务后点击"还原"。点击 "还原"后如下图所示：



还原过程中如下图：

状态	备份日期	文件大小	进度	备份生成时间	备份方式	操作
处理中	2011-11-11	7KB	正在还原...85%	2011-11-11 16:24:24	手动	导出 取消 删除

还原完成并成功后，如下图：

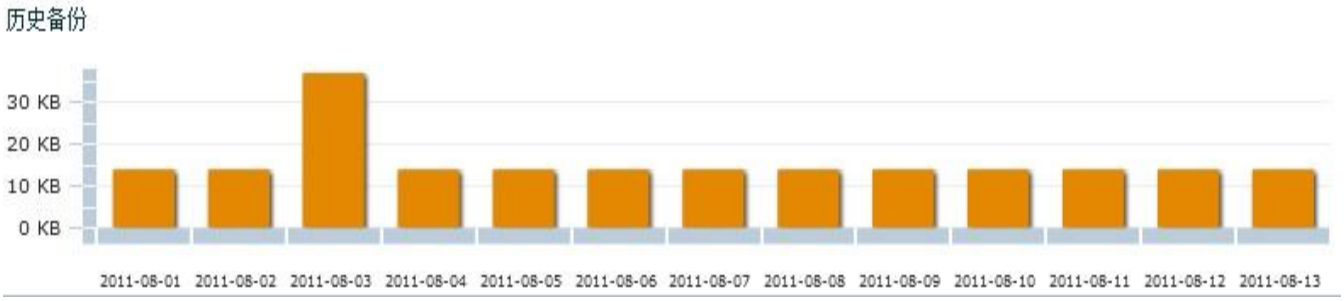
状态	备份日期	文件大小	进度	备份生成时间	备份方式	操作
成功	2011-11-11	7KB	还原完成	2011-11-11 16:24:24	手动	导出 还原 删除

取消还原

在还原过程中，点击"取消"可取消还原。

5.9.9.6如何查看历史备份图

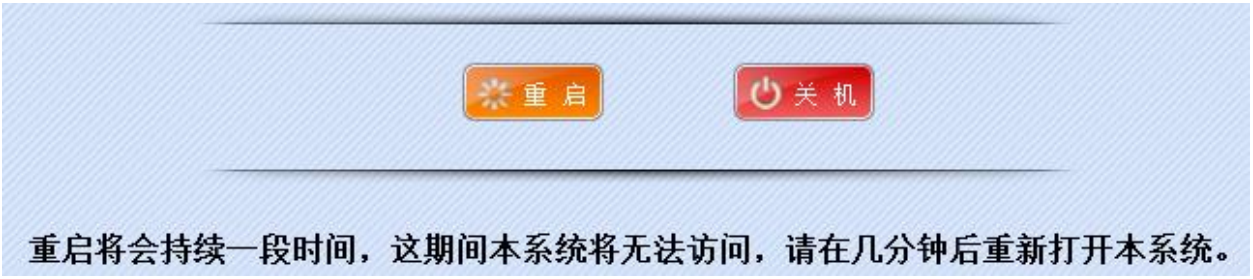
历史备份图以二维坐标直观表示历史备份的日期以及备份数据大小。横坐标为备份任务时间，纵坐标为备份数据大小（KB 为单位)。



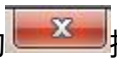
5.9.10 重启/关机

“重启/关机”功能，就是重新启动系统或者关闭系统。

鼠标点击左侧导航栏中的“系统配置->重启/关机”，进入如下界面：



（1）重启

点击“重启”按钮，给出确认提示， 若确定要重新启动系统，那么点击“确定”；否则点击“取消”或右上角的  按钮，返回到“重启/关机”界面。

（2）关机

点击“关机”按钮，给出确认提示， 若确定要关闭系统，那么点击“确定”即可；否则点击“取消”或右上角的  按钮，返回到“重启/关机”界面。

5.10用户管理

注意：仅有用户管理员 useradmin 可以进行用户的创建和删除。

以用户管理员 userdmin 登录系统，即可进入“用户管理”界面。

界面显示系统所有的自定义用户列表，展示列包括：用户账号、状态、描述、电子邮箱、最后登录时间、更新时间。点击属性列的名字可以对列表中的数据进行升序或降序排列。点击“刷新”按钮，对用户列表进行更新。

5.10.1 如何添加用户

点击右下角 

按钮，管理员添加用户配置信息如下：

用户账号：必填，填写用户登录名称。长度最小 5 个字符，最大 32 个字符，且必须为字母或数字。该账号添加以后不可以修改，只允许删除；

对应角色：自定义用户所属的角色，如果不选择某个角色，该用户将没有对应的权限；

密码：必填，为用户初始密码，长度最小为 8 个字符，最大 32 个字符，且必须为字母、数字和特殊字符的组合；

电子邮箱：必填，填写用户邮箱地址；

状态（启用）：该自定义用户处于可使用状态，允许该用户登录系统；

状态（禁用）：该自定义用户处于禁用状态，使用该用户登录系统时会提示该用户已禁用登录失败；

全名：用户登录系统后的显示名称；

描述：用户自定义描述，最长输入 1024 个字符

填写完以上信息后，点击“保存”，该用户被创建成功，并返回到用户管理主界面；点击“取消”，取消对用户的创建，并返回到用户管理主界面。

注意：用户账号、密码、确认密码和邮箱为必填项，不得为空；新建普通用户在选择对应角色添加权限前，只拥有修改个人资料的权限，其他权限需有了归属角色后才可拥有。

5.10.2 如何编辑用户

在用户管理界面，选中要修改的用户，点击右下角 编辑 按钮，进入用户编辑界面。

在用户编辑界面，可以修改对应角色权限、电子邮箱、状态，还可以添加全名、电话以及描述。

如果修改密码，勾选修改密码，界面新增新密码输入框，如下图所示：

输入相应信息后，点击“ 保存 ”按钮，则修改项被保存。点击 取消 ，则取消对密码的修改。

5.10.3 如何删除用户

在用户管理界面，选中要删除的用户名称，如选中 admin 点击右下角 删除 按钮，界面将弹出确认提示，点击 删除 按钮，该用户被删除。点击 取消 按钮，该用户保留。

5.11 系统日志管理

以日志管理员 auditadmin 登录系统，进入系统日志界面，系统日志主要记录了用户在系统下的所有操作行为的时间、日志类型、级别、状态、用户名及内容，界面。

点击属性列的名字可以对列表中的数据进行升序或降序排列。

5.11.1 如何进行日志查询

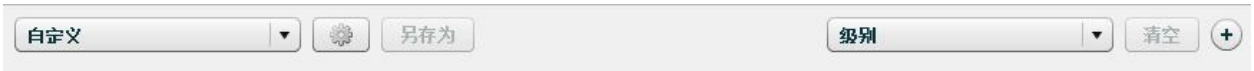
5.11.1.1 如何设置时间范围的日志查询

进入日志界面后，点击“快速选项”下拉按钮，可以通过快速选项进行时间选取。

用户也可以通过点击日期 和时间 按钮选取日期和时间，或手动输入自定义的值。

5.11.1.2 如何自定义条件进行日志查询

进入界面后，点击“查询”下拉按钮，弹出如下对话框：

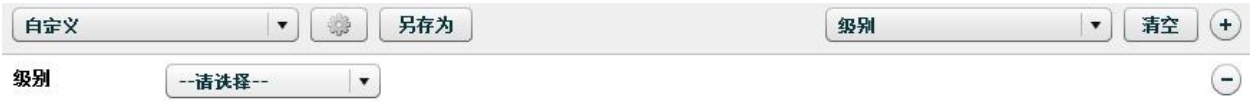


右侧是查询属性下拉菜单，可以选择不同的属性条件进行日志查询。默认属性条件是级别。属性条件菜单如下图所示：

点击属性条件下拉菜单后面的，有一个以上查询条件时，“清空”按钮变为可用。单击“清空”，清空当前所有查询条件，重新设置查询条件。

左侧是“自定义”下拉按钮，未选择查询条件时，右侧“另存为”按钮不可操作。

当选择某个属性查询条件，然后单击，并且，查询条件有一个以上时，“自定义”后的“另存为”按钮变为可用。例如：查询属性选择“级别”，单击，弹出如下对话框：

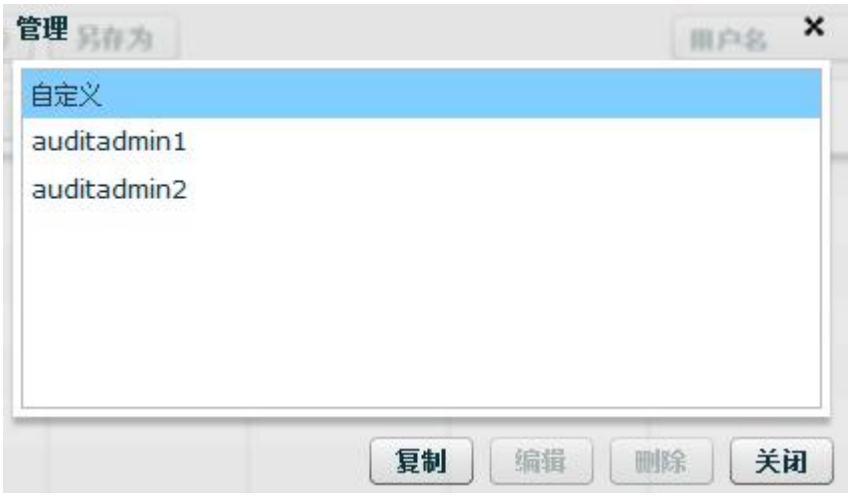


选择某一级别属性后，点击“另存为”，输入名称后，“确认”按钮变为可用，点击“确认”自定义查询条件保存成功，该界面关闭；点击“关闭”，不保存该自定义的查询条件，该界面关闭。

点击“自定义”下拉按钮，将弹出已保存的的查询条件，然后可以进行快速自定义查询。

当选择已保存的查询条件，点击右侧，弹出“管理”对话框：

选中“自定义”时，只有“复制”按钮变为可用，如图所示：



点击“复制”，可复制该查询条件。

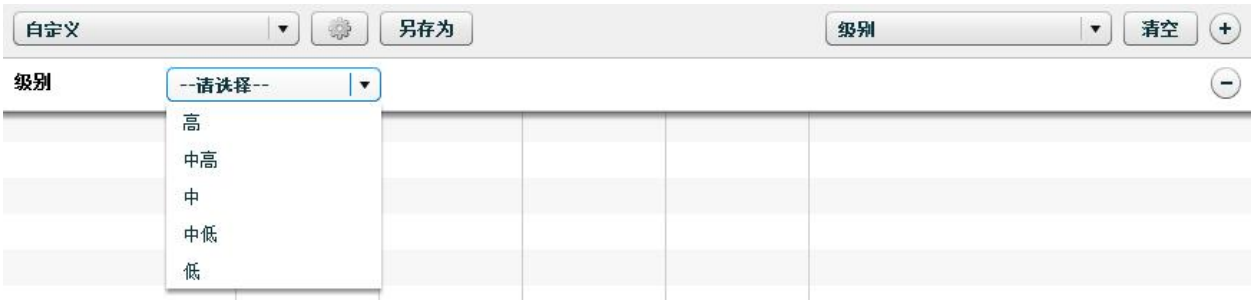
选中“自定义”以外的其他选项，可以对其进行复制、编辑、删除等操作。如图所示：

在“自定义”下拉菜单中，选择其他已保存查询条件，对其进行修改后，“自定义”下拉框后的“保存”变为可用，如图所示：

点击“保存”弹出“保存”对话框，和“另存为”对话框一样。

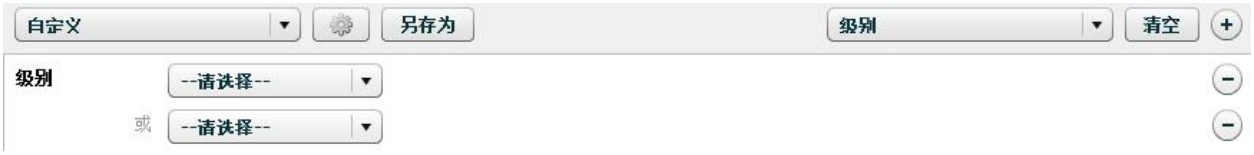
5.11.1.2.1 按“级别”属性进行日志查询

单击“查询”下拉键，弹出自定义栏，在属性类型菜单选择“级别”项，然后单击  ，  增减条件，如图所示：



级别选项分为：高、中高、中、中低、低，选择某个条件后，可对其进行“另存为”操作。

单击，还可以同时选择多个条件（最多可以选择十个条件）进行查询，多个条件之间是“或”的关系。如图所示：



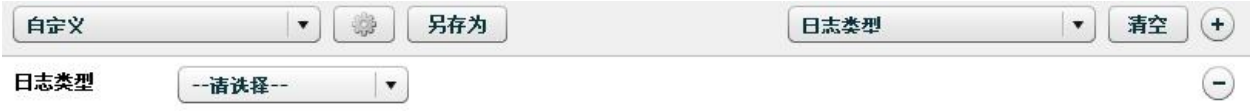
5.11.1.2.2 按“状态”属性进行日志查询

单击“查询”下拉键，弹出自定义栏，在属性类型菜单选择“状态”项，然后单击，增减条件，如图所示：

状态分为成功、失败。选择其中一个条件后，可以对其进行“另存为”操作。

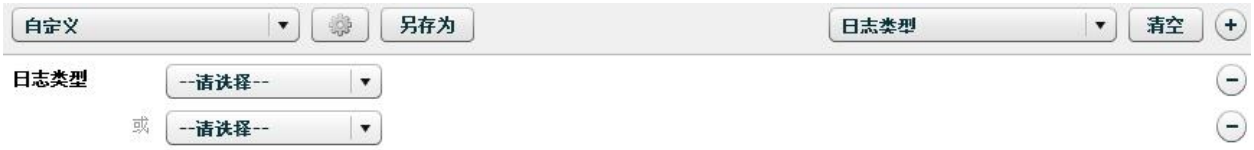
5.11.1.2.3 按“日志类型”属性进行日志查询

单击“查询”下拉键，弹出自定义栏，在属性类型菜单选择“日志类型”项，然后单击，增减条件，如图所示：



选择某个条件后，可对其进行“另存为”操作。

单击，还可以同时选择多个条件（最多可以选择十个条件）进行查询，多个条件之间是"或"的关系。如图所示：

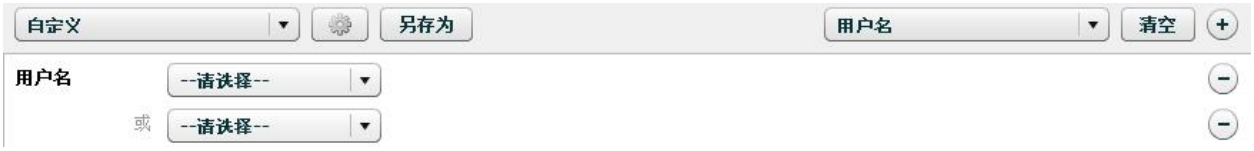


5.11.1.2.4 按“用户名”属性进行日志查询

单击"查询"下拉键，弹出自定义栏，在属性类型菜单选择"用户名"项，然后单击，增减条件，如图所示：

用户名选择条件分为：系统管理用户名（sysadmin）、用户管理用户名（useradmin）、系统日志管理用户名（auditadmin）。选择某些条件后，可对其进行"另存为"操作。

单击，还可以同时选择多个条件（最多可以选择十个条件）进行查询，多个条件之间是"或"的关系。如图所示：



5.11.1.2.5 按“内容”属性进行日志查询

单击“查询”下拉键，弹出自定义栏，在属性类型菜单选择“内容”项，然后单击  ，  增减条件，如图所示：

在内容后面的方框内，输入要查询的关键词，进行查询。还可对其进行“另存为”操作。

并且，同时可以输入多个关键词（最多可以输入十个）进行查询，多个条件之间是“或”的关系。如图所示：

5.11.2 如何查看日志的详细信息

在日志界面内，鼠标双击一条日记记录，日志详细内容会显示在日志列表下方。用户也可以通过单击右下角的“详细信息”按钮，关闭或者打开日志详情。

5.11.3 如何进行日志删除

在日志界面右下角，用户单击“删除所有日志”按钮，系统弹出删除所有日志确认对话框。用户单击取消可以取消删除操作，单击确定就会删除所有日志。

5.11.4 如何导出系统日志

5.11.5 如何导出全部日志列表

在日志界面右下角，用户单击“导出日志”按钮，系统弹出导出设置选项卡。用户可以设置以 WORD 或者 HTML 格式导出。

5.11.6 如何调整日志展示列

在日志界面内，用户单击日志列标题，可以按标题内容重新排列日志记录。用户也可以使用鼠标拖拽功能，调整日志内容显示的纵向顺序。