中国移动云市场
dbAudit 产品
使用手册

目 录

1.关于本手册

1.1. 本手册适合的对象

此手册使用对象为：数据库管理员、系统管理员，它假定您已具备下列知识与经验：

- 了解计算机、操作系统，以及操作系统指令等基础知识。
- 有数据库的实务经验，或对数据库概念有一定程度的认识。
- 具有 SQL 与 Web 应用程序开发经验或知识。

1.2. 本手册使用的惯例

惯例	说明
粗体	系统预设值、环境变数、文件、路径，以及系统界面上的各种标题等都以**粗体**显示。
斜体	*斜体*字型为范例值，须以用户环境/系统中定义或配置的正确值取代。
【】	系统界面上的菜单选项、按钮等都标记在此符号中。
>	菜单项目的路径符号。例如：【仪表盘】>【系统性能】，表示先点击【仪表盘】，再点击【系统性能】。

2.系统概述

dbAudit 为星瑞格数据库安全审计系统，主要功能特色为：

- 记录用户对数据库进行的访问活动与访问的数据
- 记录 web 应用系统进行的数据访问活动
- 提供数据库访问活动与 web 应用系统活动的完整分析信息，清楚呈现活动事件的人、事、时、地、物
- 通过人性化操作界面与下钻式 (Drill-Down) 查询，审计人员可轻松地进行数据分析
- 支持各种信息安全与审计法规
- 通过主动审计管理机制定义数据库访问审计策略与告警机制
- 7x24 实时监控、随时掌握访问状况，并提早主动告警异常行为

对合法授权者的非法或可疑访问活动，以及外部通过 web 应用系统进行的数据窃取等行为进行预防和监控并实时告警。

此系统的部署与运作，完全无需启用数据库本身的审计记录日志(Audit Trail)功能或仰赖数据库本身的日志记录。

本文档是xxx系统产品在中国移动公众服务云SAAS平台操作手册。

2.1. 系统运行架构

dbAudit 系统运作架构包括 SecuCenter、SecuEyes、SecuAgent 及 SecuLog。在环境配置上，SecuCenter、SecuEyes 和 SecuLog 必须是安装在单独的专用计算机上，不与其他软件共享同一台计算机，以保护审计数据的安全性与完整性，且每个 SecuEyes 可用于监控一个以上的网络段；而 SecuAgent 则是外挂在被监控的服务器上，可以监控位于同一台计算机上的多个目标数据库实例。

- **SecuEyes** 主要负责采集与解析 Web 应用系统服务器的访问活动与数据库服务器的访问活动，并将收集的数据传输到 SecuCenter。

- **SecuAgent** 用于采集经由 TCP 联机方式对 Web 服务器或数据库服务器进行的访问活动，及在数据库服务器本机执行的 SQL 活动，并将采集的信息传送到 SecuEyes 进行解析后传送到 SecuCenter。

- **SecuCenter** 采集与处理从 SecuEyes 传送过来的数据，并将处理过的数据存储到 dbAudit 数据库中，作为分析与统计使用。并且提供用户通过网页界面来管理 dbAudit 设备、监控目标、审计报表、审计策略、告警和用户帐号等等，以及查阅审计记录，同时完整记录用户对 dbAudit 系统的访问行为。

- **SecuLog** 主要是定期备份 SecuCenter 的历史审计数据、报表和图表模板等备份数据，并提供用户通过其系统网页界面还原和查阅某一指定日期区间的备份数据，以避免对 SecuCenter 造成负担，确保在线审计的效能与实时性。

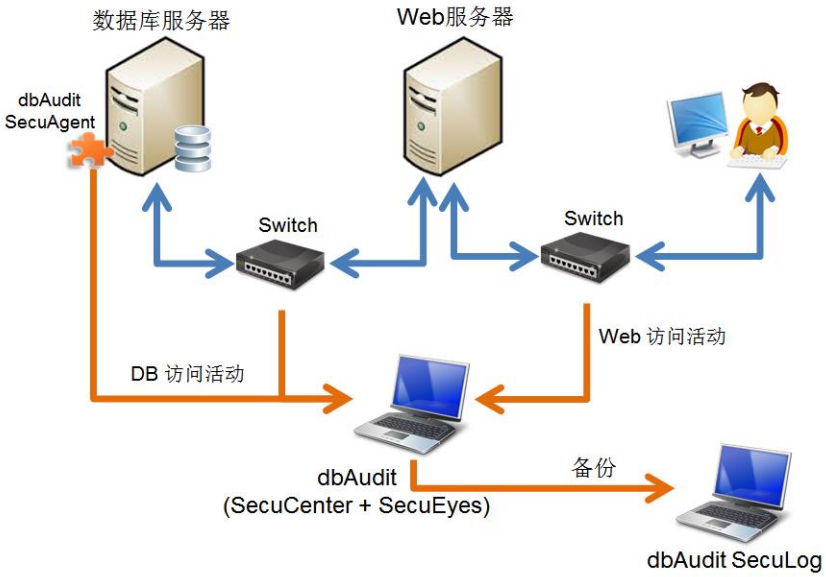


图 2-1 系统运行架构示意图

2.2. 审计数据保护机制

为了确保审计数据的安全性、完整性与不可否定性，dbAudit 在审计数据的传输、保存与使用都有相应的保护机制，以防止审计数据遭到窃取、窜改或删除。

在 SecuEyes、SecuAgent、SecuLog 和 SecuCenter 间的数据传输，是采用加密通讯通道来进行数据传输，以确保传输数据的安全与完整。

用户只能够通过使用 SSL 传输协议的 dbAudit 网页界面来管理 dbAudit 系统和查看审计记录。而 dbAudit 网页界面也仅提供用户查阅审计记录的功能，没有提供用户对审计记录进行手动添加、修改或删除的功能，同时对显示的敏感性数据进行掩码处理。

通过 dbAudit 系统提供的系统管理员、安控管理员、审计人员、一般人员等用户角色，可以限制用户在网页界面上可操作的功能与动作；而用户帐户的审计权限配置则限制用户可查阅的审计数据范围。

对于 dbAudit 系统经由备份程序生成的备份文件，则是经过密码密钥加密与数位签名处理后，才传送到备份存储介质上保存，以确保数据的完整与不可否定性。

在 dbAudit 本机仅提供 CLI (Command Line Interface)模式让系统默认的特定帐号登录进行系统管理。而 dbAudit 本机上不允许用户执行 CLI 以外的程序或命令，也不接受任何 CLI 以外的命令。CLI 清单上并不提供任何涉及变更和查阅审计数据的命令。CLI 清单提供密码变更命令，让系统管理员可以变更系统默认帐号的默认密码。

2.3. 系统需求

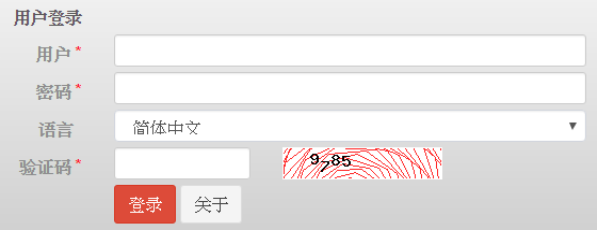
浏览器 (版本)	IE 11 以上 FireFox 40 以上 Chrome 40 以上 (建议)
建议的屏幕解析度	1024 x 768 以上
RAM（内存）	1G 以上

3.登录

1. 请输入 dbAudit 的 URL，例：http://192.168.123.180:8080。

   如登录 SecuCenter，URL 中的 IP 地址为 SecuCenter 的 IP 地址；如登录 SecuLog，URL 的 IP 为 SecuLog 的 IP 地址。默认端口为 8080。

   如果不清楚 dbAudit 系统入口网址，请洽询系统管理者。



2. 从**语言**下拉菜单选择登录后页面的显示语言。

3. 在用户和密码字段输入用户帐号和密码。

   对于不是使用单一帐号(LDAP 帐号)登录 dbAudit 的用户，请使用 dbAudit 发送给您的临时密码登录。于首次登录时，系统会强制您变更密码。如果未收到临时密码通知信函，请洽询系统管理员。如果您在临时密码过期前都未登录系统开通帐户，则必须请系统管理员重新设置一个临时密码，dbAudit 系统会重新发送一个临时密码通知函给您。

   如果您是使用单一帐号(LDAP 帐号)登录 dbAudit 的用户，于首次登录前，务必请系统管理员帮您于 dbAudit 系统中设置使用 LDAP 帐号的帐户。

   仅 SecuCenter 上的有效账号才可登录 SecuCenter 和 SecuLog。

   有关密码变更的密码强度颜色与相应复杂度的说明，请参阅 5.1.1 密码强度颜色与相应复杂度。

4. 在**验证码**文本框内输入文本框旁的图形验证码后，单击【登录】。如果登录页面放置过久，请点击**验证码**文本框旁的图形验证码以生成新的图形验证码。

4.接口界面、角色与权限

4.1. 接口界面

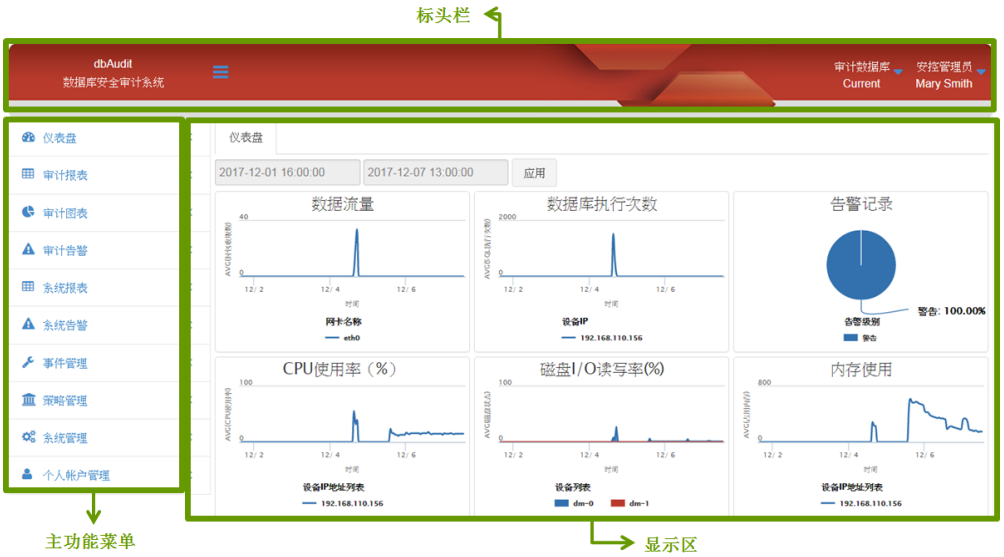


图 4-1 dbAudit 系统网页界面概观

注：在操作使用上，请勿使用浏览器本身的上一页与下一页功能，以免造成页面信息错误。

系统界面分成三个部分：

标题栏　　包括以下项目：

用于显示/隐藏主功能菜单。右图虚线框部分为主功能菜单的隐藏形式；当鼠标移到其上时立即显示出原本主功能菜单，鼠标离开时立即变成隐藏形式。

此处显示您目前正在查看的数据库，并提供下拉菜单让您选择查看其他的数据库。下拉菜单中列出所有您可查看的数据库包括 **Current** 和其他还原回来的历史数据库。**Current** 为系统运行中使用的数据库，用于保存已处理的采集数据，以及 dbAudit 本身的访问活动记录。历史数据库名称格式为*起始日期_结束日期*，标示该历史数据库是哪一个时间区间的数据。

例：20170201_20170228，表示该历史数据库的数据为 2017/2/1~2017/2/28 期间的数据。

显示目前登录用户名称与角色，并提供下拉菜单让您可以签退系统、修改您的帐户信息和界面喜好，以及查看 dbAudit 版本号。

主功能菜单　显示用户可以使用的功能项目。系统依据用户角色和登录对象（SecuCenter 或 SecuLog）的不同，来显示用户可操作的主功能项目与各主功能项下的子功能选项。

显示区　依据用户选择的功能项目显示相应操作画面，供用户进行项目设置与数据查询的操作，以及显示查询结果等。

4.2. 界面上的主功能项

- 仪表盘　以图表方式显示告警事件分布、SecuCenter 的系统资源使用曲线、各 dbAudit 设备捕捉的 SQL 活动数量曲线、被监控目标上登录失败/数据访问失败的次数曲线等等，并显示各 dbAudit 设备的目前运行状态。

- 审计报表　用户可以通过报表来审计被监控目标（应用系统、数据库服务器、Web 服务器）上的访问活动，和曾被查阅过的数据。并提供用户自定义审计报表、设置报表排程，和导出/打印报表结果。

- 审计图表　以图表方式提供被监控目标（应用系统、数据库服务器、Web 服务器）上访问活动的统计信息，并允许用户自定义审计图表。

- 审计告警　用户可以通过告警通知监控被监控目标（应用系统、数据库服务器、Web 服务器）上的访问活动及曾被查阅过的数据等，以及时发现异常访问活动。并允许用户自定义告警事件。

- 系统报表　用户可以通过报表来审计 dbAudit 用户在 dbAudit 系统上的访问活动和操作。并提供用户自定义审计报表、设置报表排程，和导出/打印报表结果。

- 系统告警　用户可以通过告警通知实时监控 dbAudit 系统上的访问活动和操作，以及时发现异常访问活动和操作。并允许用户自定义告警事件。

- 事件管理　主要分为四部分：
  - 提供用户处理收到的告警事件与待审核的告警事件
  - 提供事件侦查引擎的侦查记录，以及告警通知发送记录查询
  - 提供系统管理员查询 dbAudit 异常日志与管理异常状况是否已排除
  - 对于排程报表任务，提供一个方便与集中式的查看界面

- 策略管理　　提供用户管理法规、法规下的法条、法条的审计条件、事件的审核阶层，以及 SQL 活动的捕捉策略。通过审计条件关联的审计报表和告警通知，用户审计数据访问活动是否遵循法条要求，和监控是否有不符合法条要求的数据访问活动发生。

- 系统管理　　提供系统管理员进行 dbAudit 系统配置与管理，例：监控目标的管理、dbAudit 设备配置、用户帐号管理、消息传递通道配置等。

- 个人帐户管理　　提供登录用户维护自己的帐户信息包括用户名、密码、email 等信息的维护。

4.3. 数据时间段设置

在报表和告警的清单页面，以及报表/告警排程设置、报表导出和打印等窗口都可看到类似下面的时间段显示。

2017-05-08 00:00:00 ~ 2017-05-08 14:00:00

当在时间段上点击时开启如下时间段变更窗口。时间段的设置分为：相对时间和固定时间。

图 4-2 相对/绝对时间区段设置窗口

相对时间框，用于设置一个相对于运行当下时间的时间段。例：当下时间为 2017-3-14（周二），那么上周末就是指 2017-03-11 00:00:00 ~ 2017-03-13 00:00:00。完成时间段设置后，单击【应用】将相对于当下时间的时间段返回页面上，例：2017-03-11 00:00:00 ~ 2017-03-13 00:00:00（上周末）。

点击红框内的一个默认时间段，在**起始时间**和**结束时间**文字框内就会显示出该时间段的起迄表示式。例：-1m@m，m 为月的时间符，-1m 表示往回一个月，@m 表示以月启始点（也就是当月一号）开始计算；所以 -1m@m 表示上个月。因此，如果默认时间段没有您需要的时间段，您可以手动方式直接在**起始时间**和**结束时间**文字框内以时间表示式输入时间段的起迄时间。

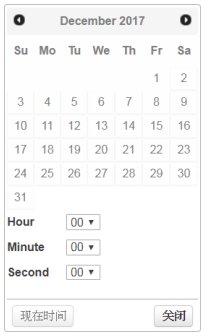
表示式中可用的时间符：d（天）、w（周）、m（月）、i（分）、h（时）。

图 4-3 相对时间区段设置框

固定时间框，用于设置一个特定的时间段（例：2017-03-01 00:00:00 ~ 2017-03-15 00:00:00）。

图 4-4 固定时间区段设置框

当点击**起始时间**文本框或**结束时间**文本框时，将弹出如右的对话框。选择的日期与时会立即出现在相应的文本框内，完成后点击【关闭】关闭对话框。完成时间段设置后，单击【应用】将指定的时间段返回页面上。



4.4. 角色权限

dbAudit 提供四种用户角色：系统管理员、安控管理员、审计人员、报表查阅人员。

系统管理员：　负责管理 dbAudit 系统设置和环境配置，以及监控系统运行状况。

安控管理员：　主要负责审计相关项目的管理与设置，包括报表、图表、告警、法规/法条/审计条件，和事件审核阶层等，并可对收到的事件通知进行处理与签核。

审计人员：　主要执行审计任务，其可操作的主要对象包括：报表、图表，并可对收到的事件通知进行处理与签核。

报表查阅人员：　主要将事件通知处理结果呈报给上级主管，其主要操作对象为事件通知。

以下为各角色可操作的功能项目对照表，“✓”表示该角色用户可以完全操作：

表 4-1 角色与可操作主功能项对照表

	系统管理员	安控管理员	审计人员	报表查阅人员
仪表盘	✓	✓	模块状态监控除外	模块状态监控除外
审计报表		✓	✓	
审计图表		✓	✓	
审计告警		✓	仅可查阅	
系统报表	✓	系统访问活动相关项目	系统访问活动相关项目	
系统告警	✓	系统访问活动相关项目	系统访问活动相关项目	
事件管理	✓	系统异常相关项目除外	系统异常相关项目除外	仅事件审核
策略管理	仅用户阶层管理	✓	仅可查阅	
系统管理	✓	仅可查看： • 设置的监控目标 • 已还原历史数据库信息		

5.个人信息/接口配置

【个人帐户管理】的【帐户设置】和【界面喜好设置】分别提供个人帐户信息设置，和个人的接口喜好设置。

5.1. 帐户信息

每个用户都有一个唯一的登录帐号用于标识该用户，因此登录帐号一旦创建后就不允许变更。在【帐户设置】页面上，除了**登录帐号**不允许变更外，其余字段：用户名称、用户部门、LDAP 验证、密码、邮件地址、电话、用户注释等都可以变更。修改完毕，单击【保存】保存变更。

用户仅可在 SecuCenter 上进行帐户信息变更，SecuLog 上不提供用户对帐户信息、密码等进行修改的功能。

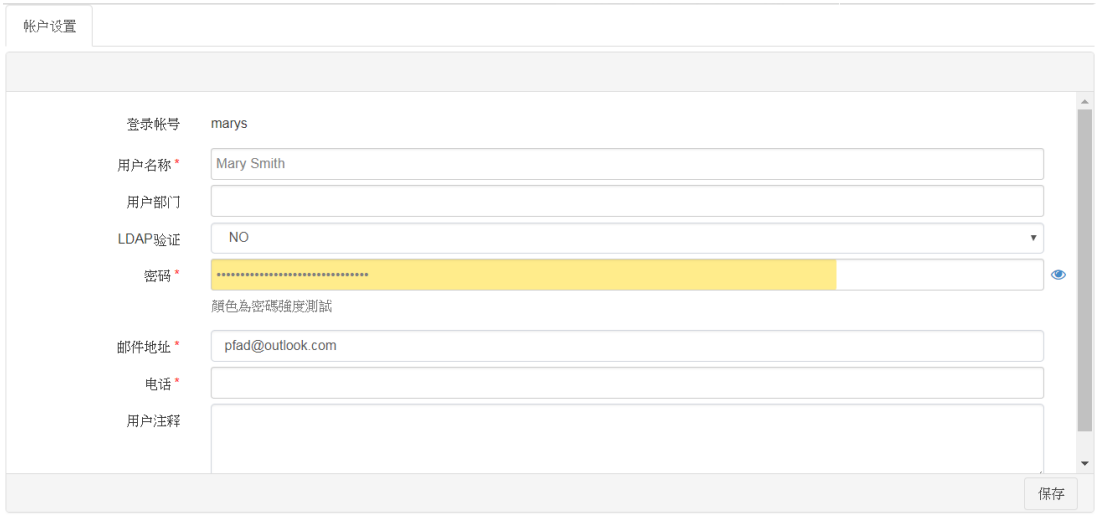


图 5-1 个人帐户信息编辑

表 5-1 个人帐户信息字段说明

字段	说明
用户名称	用户的全称。
用户部门	用户所属部门单位。
LDAP 验证	选择 “YES”，表示用户是使用单一帐号(LDAP 帐号)/密码来登录 dbAudit 系统。帐号的登录认证与密码管理都是由 LDAP 负责。 选择 “NO”，表示由 dbAudit 负责该帐号的登录验证与密码管理，那么就必须输入**密码**字段。

字段	说明
密码	用户登录密码。依据您的输入将以颜色显示密码的强度。建议密码为大小写英文字母、数字和特殊字符等的混合。有关密码强度颜色与相应的复杂度，请参阅 5.1.1 密码强度颜色与相应复杂度。 如 **LDAP 认证**设置为 “YES”，就不会看到此字段。
邮件地址	用户的电子邮箱地址，用于接收系统发送的排程报表、告警通知、帐户变更通知等。
电话	用户的联络电话。

5.1.1. 密码强度颜色与相应复杂度

dbAudit 使用以下 6 个条件来检验密码的强度。当您变更密码时，新密码字符组合符合的条件数越多，则密码的强度和复杂度也就越高，相对地，您的帐号安全性也就越高。

- 字串长度 > 8
- 字串长度 > 10
- 包含大写字母
- 包含小写字母
- 包含数字
- 包含特殊字符（例如：@、#）

表 5-2 密码强度颜色说明

符合的条件数	密码强度颜色说明
1~2	密码强度颜色为红色。表示密码字符的组合为最弱的。
3	密码强度颜色为橙色。
4	密码强度颜色为黄色。
5~6	密码强度颜色为青绿色。表示密码字符的组合为最强的。

5.2. 接口配置

用户可通过登录页面的语言下拉菜单来设置 dbAudit 接口页面的显示语言配置。

对于界面上查询结果每页显示的笔数缺省为 10 笔，如果想变更每页显示笔数，您可以通过【个人帐户管理】>【界面设置】的**默认笔数**字段来进行变更。

6.综合监控仪表盘

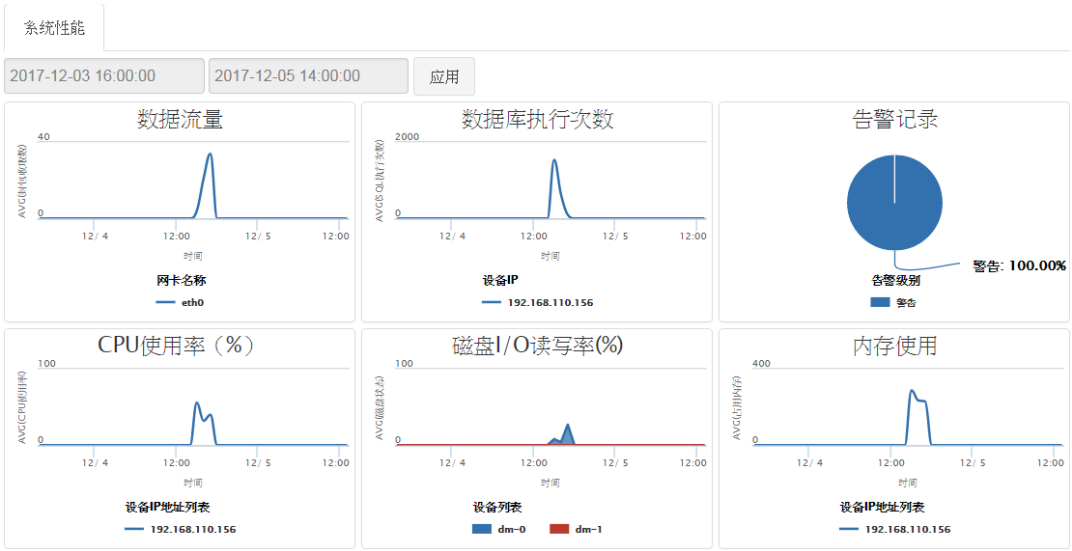
安控人员/审计人员可以通过【仪表盘】的各种分析图来监视监控目标上登录失败与 SQL 执行失败的次数曲线，并可监视 SecuCenter 的资源使用状况和查看各 dbAudit 设备的运行状态。

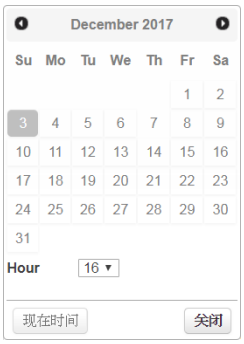
同时，还可通过【审计图表】和【审计报表】来查看监控目标上的数据访问活动的各种统计与详细信息；通过【审计告警】配置相关告警来监控是否有关注的重要事件发生。并可通过【系统报表】来查看 dbAudit 的用户访问活动，和通过【系统警示】配置相关告警来监控是否有关注的重要事件发生。有关图表、报表和告警的操作说明，请分别参阅 7 图表、8 报表和 9 告警。

◆ 系统性能

通过【仪表盘】>【系统性能】提供的图表，您可以监控 SecuCenter 的性能包括 CPU、I/O、网络、内存、执行的 SQL 语句数等等。

如图表上有很多条曲线，您可以点击某一个曲线相应的图例将该曲线暂时隐藏起来；当再次点击该图例时就会重新显示该图例相应的曲线。





图表上方有两个时间框，用于分别设置要查看的时间段的开始时间与结束时间。点击输入框时将开启如左的日历对话框，设置 了日期与时间后单击【关闭】以将指定的日期时间带回输入框。完成起始和结束日期设置后单击【应用】以重新整理页面信息。

当您将鼠标移动到曲线上时会出现类似右上图的提示框，显示该点的数据。

在该点上右击鼠标会出现类似右下图可下钻查看的右键菜单。点击右键菜单中项目后，将开启一个新标签页显示其信息。例：点击右键菜单的【设备IP】开启类似下面的标签页，显示该指定时间区间内各 dbAudit 设备捕捉的平均 SQL 活动量曲线图。有关图表与报表的使用操作说明，请参阅 7 图表和 8 报表。

◆ 审计监控

【仪表盘】>【审计监控】以图表方式显示监控目标上关注的访问活动的数量曲线，包括对于不同对象的登录失败次数和 SQL 执行失败次数曲线，和不同级别告警的发生次数分布等。

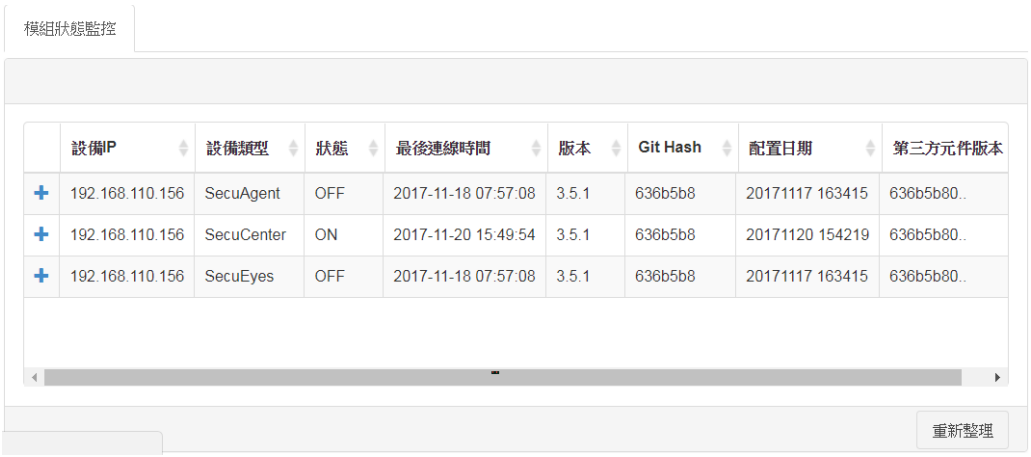
其操作方式与【系统性能】相同。您可以指定要查看的时间区间后单击【应用】以重新整理页面信息。也可以将鼠标移动到曲线上查看该点数据并通过右键菜单的项目下钻到相关图表与报表以查看其他信息。也可以通过点击图例的方式来显示与隐藏其相应的曲线。

◆ 模块状态监控

通过【仪表盘】>【模块状态监控】您可以查看目前 dbAudit 系统已设置的 dbAudit 设备的 IP、运行状态、使用的软件版本、安装（配置）日期，以及所使用的第三方组件版本

等信息。

在 SecuLog 上不提供【模块状态监控】查看各 dbAudit 模块的运行状态。



7.图表

【审计图表】是以图表方式呈现目标应用系统与数据库数据访问活动的统计信息，让用户可以从统计信息的角度来审计数据访问活动，并通过下钻式查询功能来查看更多相关信息。

左侧菜单的不同图表主题提供不同内容属性的审计图表。例如：【审计图表】>【SQL 活动追踪】仅提供与 SQL 活动有关的图表内容和配置字段。

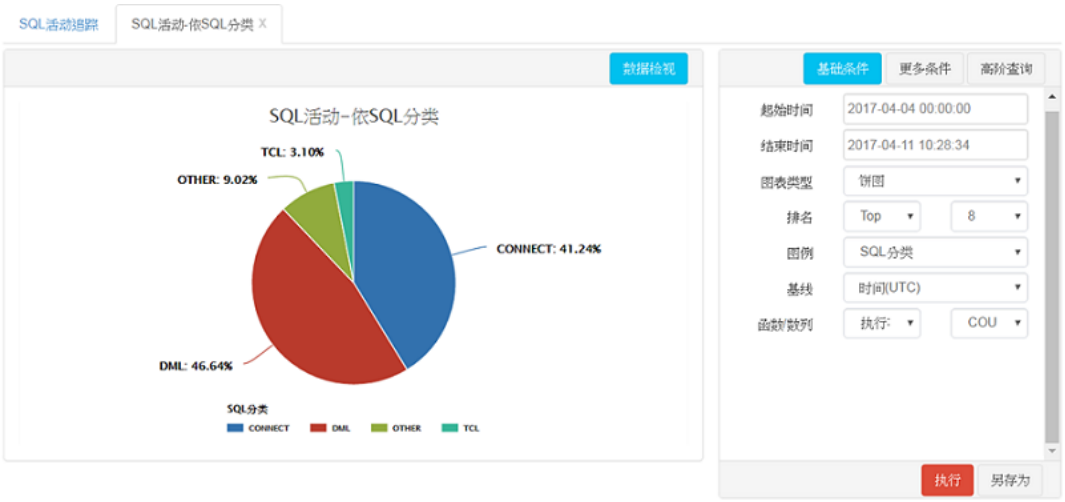
点击【审计图表】下某一图表主题后，开启该主题的图表管理与操作页面。例如：【审计图表】>【SQL 活动追踪】开启类似以下的图表管理与操作页面。您可通过**分类**下拉菜单选择列出哪个分类下的 SQL 活动追踪图表，并对其中的图表进行添加、修改与删除。分类主要包括各种法规、异常管理和一般审计追踪，让您能够将图表储存于适当类别，之后可依据类别迅速找到需要调整或查看的图表。

系统默认列显示勾号的项目为系统默认图表，是不允许用户修改或删除的。

图 7-1 图表管理（SQL 活动追踪）

7.1. 在线查看

在清单页面选择欲查看的图表（例：SQL 活动-依 SQL 分类）并指定查看的时间段后，单击【钻取】，系统将开启新标签页并绘制该指定时间段内的统计数据图表（类似下图所示）。您可以变更该标签页上的时间段，以查看其他时间段的统计图表。有关时间段的设置说明，请参阅 4.3 数据时间段设置。

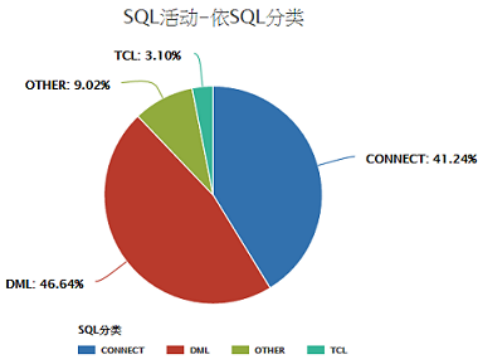


图表右侧的基础条件：

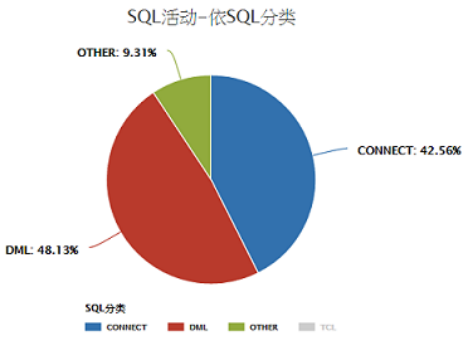
- 起始时间和结束时间：指定使用哪一个时间范围的数据来绘制图表。
- 图表类型：指定使用哪一种图表类型来绘制图表。
- 图例：用于在图表上标识所选类别中各数据列对象。

- 排名：对于数据列对象过多而难以检视的图表，您可以选择 Top 或 Bottom，并指定显示的数据列对象数目，以使图表仅显示最前面或最后面的 n 项数据列对象。

  也可透过点击图表上图例以隐藏图例相应的曲线/区块；反之，再次点击图例，则重新显示图例相应的曲线/区块。



图例 TCL 隐藏前

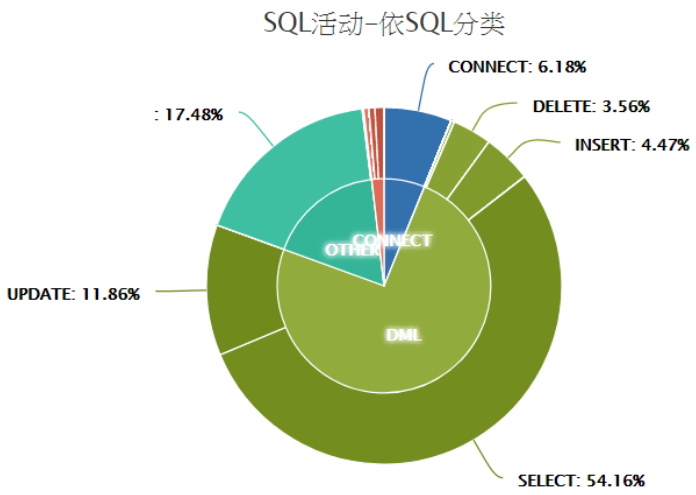


图例 TCL 隐藏后

- 函数/数列：指定数据列的统计对象（例：执行次数）。

- 基线：用于设置统计基线，一般为时间。如果统计基线为时间，系统将基于时间对指定时间段内每一数据列对象的数据进行统计运算。如果选择其他字段作为统计基线，系统将基于指定时间段内该字段出现的值对指定时间段内的每一数据列对象的数据进行统计运算。

  以上面的图表为示例，当**基线**设为“SQL 操作指令”时，系统将基于指定时间段内“SQL 操作指令”出现的值（SELECT、INSERT、DELETE、UPDATE、COPY、CONNECT 等等）对指定时间段内每一 SQL 分类（CONNECT、DML、OTHER、TCL 等）进行执行次数比率计算。下图显示指定时间段内每一数据列对象基于“SQL 操作指令”的统计数据。



您可以在图表曲线任一点或任一区块上右击鼠标，从右键菜单中选择要查看的其他相关信息，系统会将鼠标所在位置的相关数据带入所选的选项作为捞取相关详细信息的条件值。

【更多条件】或【高阶查询】将在基础条件下显示更多其他适用于该图表主题的筛选条件项目。各筛选条件间是使用 AND 逻辑运算符关连。【更多条件】只允许您对于每一筛选条件设置单一条件值；【高阶查询】允许您通过运算符（IN、LIKE、NOT LIKE、>、<、IN SET 等等）对筛选条件设置多个条件值。通过筛选条件的设置，您可以从图表使用的数据范围内筛选出特定的数据集来绘制图表。

例：要从 “SQL 活动-依 SQL 分类” 图表使用的数据范围筛选出特定的数据库服务器来绘制图表。请先从列表中选择该图表后单击【钻取】，然后在**起始时间**框和**结束时间**框设置使用哪个时间区间的数据。接着，从【更多条件】的**数据库服务器**下拉菜单中选取要查看的数据库服务器后，系统立即依据所给条件重新绘制图表。

有关运算符（IN、LIKE、NOT LIKE、>、<、IN SET 等等）与条件值的关系说明，请参阅 8.5.2.1 运算符与条件值组件。

7.2. 添加/修改/删除

对图表的添加、修改和删除操作，请在 SecuCenter 的 **Current** 数据库上进行。如在 SecuLog 的数据库或 SecuCenter 的其他历史数据库上执行这些操作，其生成的结果都是暂时性的。因为当 SecuCenter 运行定期备份时，会将本身的 **Current** 数据库同步到 SecuLog 的 **Current** 数据库，并覆盖掉 SecuLog 的 **Current** 数据库内容；而 SecuLog 或 SecuCenter 的其他历史数据库，在被移除时该历史数据库内的所有变更也会一并被移除。

图 7-2 图表编辑

◆ **从空白开始创建新图表**

先从清单页面（类似图 7-1 所示）的**分类**下拉菜单选择新图表所属的图表分类，然后单击【添加】开启类似图 7-2 的添加页面。

页面右侧项目为图表设置项目，详细操作方式请参阅前一节。**起始时间**和**结束时间**为变动性必备项目，由用户于运行图表时指定，因此图表配置文件并不会保存任何特定时间区间值。

编辑完后，单击【保存】，输入图表名称后，单击【提交】完成新图表的创建，并将新图表加入所选的分类中。

如果在清单页面没有看到新添加的图表，请单击【刷新页面】以重新刷新页面。

- **以现有图表为样板创建新图表**

先从清单页面（类似图 7-1 所示）的**分类**下拉菜单中选择样本图表所属的图表分类，再选择作为样板的图表，然后单击【钻取】开启类似图 7-2 的页面。

页面右侧项目为图表设置项目，详细操作方式请参阅前一节。**起始时间**和**结束时间**为变动性必备项目，由用户于运行图表时指定，因此图表配置文件并不会保存任何特定时间区间值。

编辑完后，请单击【另存为】，输入图表名称后，单击【提交】完成新图表的创建，并将新图表加入与样板图表相同的分类中。如单击【保存】将会覆盖样板图表的原配置。

如果在清单页面没有看到新添加的图表，请单击【刷新页面】以重新刷新页面。

- **修改图表**

系统不允许您修改系统默认图表，仅允许您修改自定义的图表。

先从清单页面(类似图 7-1 所示)的**分类**下拉菜单选择要修改的图表所属的图表分类后，选择要修改的图表，然后单击【钻取】开启类似图 7-2 的页面。

页面右侧项目为图表设置项目，详细操作方式请参阅前一节。**起始时间**和**结束时间**为变动性必备项目，由用户于运行图表时指定，因此图表配置文件并不会保存任何特定时间区间值。编辑完后，单击【保存】以保存变更。

- **删除图表**

系统不允许您删除系统默认图表，仅允许您删除自定义的图表。

先从清单页面(类似图 7-1 所示)的**分类**下拉菜单选择要删除的图表所属的图表分类后，选择要删除的图表，然后单击【删除】再单击【确定】。

8.报表

基于法规与数据安全策略对于数据访问的保护、追踪及控管等的实施方法是从 5W：人（Who）、事（What）、时（When）、地（Where）、物（onWhat）的角度来实现，因此，【审计报表】提供的报表也是从 5W（人、事、时、地、物）的角度来完整呈现数据访问活动记录，让您可以轻松的审计与追踪数据库的每一个数据访问活动。并且，您可以通过报表提供的右键菜单项目向下钻取更多相关信息。同样地，您可以通过【系统报表】提供的报表来审计用户在 dbAudit 上的数据访问活动，以及系统资源使用量与性能等数据。

除了默认报表外，您可以依据企业需求，在【审计报表】和【系统报表】的各报表主题中自定义报表。

左侧菜单所列的报表主题分别提供不同内容属性的审计报表。例如：【审计报表】>【SQL 活动追踪】仅提供与 SQL 活动有关的报表内容和配置字段。

点击【审计报表】或【系统报表】下某一报表主题后，开启该主题的报表管理与操作页面。例如：【审计报表】>【SQL 活动追踪】开启类似以下的报表管理与操作页面。您可通过**分类**下拉菜单选择列出哪个分类下的 SQL 活动追踪报表，并对其中的报表进行添加、修改与删除。分类主要包括各种法规、异常管理和一般审计追踪，让您能够将报表储存于适当类别，之后可依据类别迅速找到需要调整或执行的报表。

系统默认列显示勾号的项目为系统默认报表，是不允许用户修改或删除的，仅允许直接运行或作为报表创建的样板。有关审计报表和系统报表的查阅和创建等操作，请参阅以下章节。

图 8-1 报表管理（SQL 活动追踪）

8.1. 在线查看

在清单页面（类似图 8-1 所示）选择欲查看的报表（例：数据库活动）并指定查看的时间段后，单击【钻取】，系统将开启新标签页来显示指定时间段内的报表结果（类似下图所示）。您可以变更该报表标签页上的时间段，以查看其他时间段的数据。有关时间段的设置说明，请参阅 4.3 数据时间段设置。

图 8-2 指定时间段内的报表查阅结果

点击某一列头（例如，点击上图的“SQL 语句”列头），则页面上的显示结果将以该字段的升序进行排序，再次点击时，将以该字段的降序进行排序。

如果想要查看更多字段或移除某些不想查看的字段，可单击【编辑钻取条件】进入编辑页面，完成后单击编辑页面上的【预览】来检视依据修改后的配置所重新生成的结果。在编辑页面上的变更为暂时性的，除非您在编辑页面上单击【保存】或【另存为】来保存变更。有关编辑页面的操作说明，请参阅 8.5 添加/修改/删除。

如要导出或打印该报表结果，请单击报表结果下方的【导出报表】或【打印报表】。有关导出和打印的操作说明，请参阅 8.2 导出/打印。

您可以在报表结果的任一行上右击鼠标，从右键菜单中选择要查看的其他相关信息，系统会将该行的相关数据带入所选的选项作为捞取相关详细信息的条件值，并开启新标签页显示钻取的信息。您可以在新开启的标签页上重复同样的操作继续钻取相关信息。

除了在线查看外，您还可以设置报表定期运行并将结果发送给相关人员。有关报表定期运行设置的说明，请参阅 8.3 报表定时发送配置。

8.2. 导出/打印

◆ **导出**

您可以在类似图 8-1 的报表清单页面，选择一个报表后单击清单下方的【导出报表】开启以下类似窗口；或者在类似图 8-2 报表结果页面上单击【导出报表】开启以下类似窗口，以导出指定报表的结果。

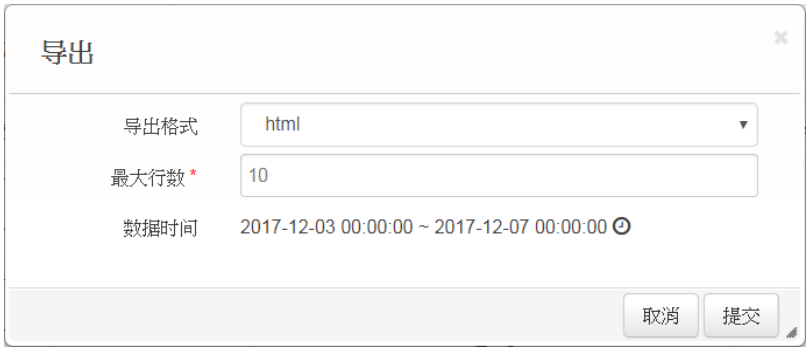


图 8-3 报表导出

表 8-1 报表导出字段说明

字段	说明
导出格式	报表结果的导出格式。目前提供 csv、html、pdf、xls、xml 等格式。
最大行数	指定最大导出笔数。
数据时间	指定使用哪个时间范围的数据来生成报表结果。 如果是从类似图 8-1 的页面开启导出窗口，该字段的默认值为清单上方的时间段；如果是从类似图 8-2 的页面开启导出窗口，该字段的默认值为报表结果上方的时间段。 有关数据时间的设置说明，请参阅 4.3 数据时间段设置。

在指定了想要的导出格式、导出的笔数与使用的数据时间段后，单击【提交】，系统将依据指定的格式、笔数和数据范围生成文档，并开启保存窗口询问您保存位置。默认文档名为：*报表名称-报表生成时间.选择的导出格式*，例如：数据库活动-2017_04_13_14_29_52.html。

◆ **打印**

您可以在类似图 8-1 的报表清单页面，选择一个报表后单击清单下方的【打印报表】开启以下类似窗口；或者在类似图 8-2 报表结果页面上单击【打印报表】开启以下类似窗口，以打印出指定报表的结果。

图 8-4 报表打印

表 8-2 报表打印字段说明

字段	说明
最大行数	指定最大打印笔数。
数据时间	指定使用哪个时间范围的数据来生成报表结果。 如果是从类似图 8-1 的页面开启打印窗口，该字段的默认值为清单上方的时间段；如果是从类似图 8-2 的页面开启打印窗口，该字段的默认值为报表结果上方的时间段。 有关数据时间的设置说明，请参阅 4.3 数据时间段设置。

在指定了想要打印笔数与使用的数据时间范围，单击【提交】后系统将开启一个新标签页显示打印内容，并开启系统的打印设置窗口以便您指定从哪一个打印机打印出来。

8.3. 报表定时发送配置

通过排程设置，您可以指定报表结果的生成周期，并指定报表结果的发送对象与需要走的签核流程。定期报表发送使您不仅不再需要周期性地以手动方式指定查询时间段来查看每一份报表结果，也可通过签核流程方式确认相关人员收到并审计了报表内容。除了周期性报表外，您也可以将单一次涵盖较大数据范围的报表查询以排程方式送到后台运行，以免除在线查看方式占住前台界面的操作。

先从类似图 8-1 的报表清单选择要添加或修改排程配置的报表后，单击【定时发送报表】开启类似以下的报表排程设置窗口。

图 8-5 报表定时发送配置

表 8-3 报表定时发送配置字段说明

字段	说明
通知对象	定期报表发送对象。
签核流程	定期报表套用的签核流程。有关签核流程设置的说明，请参阅 11.1 签核流程配置。
导出格式	报表内容的导出格式。目前提供 csv、html、pdf、xls、xml 等格式。
最大行数	报表结果包含的最大数据笔数。
重复发送	YES 表示报表将定期运行。 NO 表示报表在运行一次之后，就会将报表排程变成停用状态。通过这种方式，您可将报表送到后台运行，无需因为在线等待报表结果生成而无法进行其他操作动作。
启用	是否启动排程设置。
数据时间	指定使用哪个时间段的数据来生成报表结果。如果是使用相对时间区间，那么系统将以指定的相对时间间隔，作为运行周期间隔。例如：选择**每 15 分钟**，那么系统将每 15 分钟运行一次报表。 有关数据时间段的设置说明，请参阅 4.3 数据时间段设置。

通知对象和**签核流程**两个字段必须设置一个，两个都设置也可以。如果指定了签核流程，系统会将定期报表结果发送给该签核流程的第一层人员。有关签核流程的运行与操作说明，请参阅 11 事件签核流程。

设置完毕后单击【提交】保存报表的排程设置并返回清单页面。如果**启用**为“YES”，其清单上**定时发送报表**将显示 ON 表示报表排程为启用状态；如果为“NO”，将显示 OFF 表示报表排程为停用状态。您可以单击清单上**定时发送报表**内的图标变更报表排程的启用或停用状态。同时，系统依据**数据时间**设置预估运行报表的时间点并显示在清单的**预计报表发送时间**。

当提交**启用**为“YES”的排程配置时：

- 如**数据时间**为绝对时间，则无论**重复发送**为“YES”或“NO”，系统会立即于报表运行队列中放入该报表，并在执行一次之后自动将报表排程变成停用状态。

- 如**数据时间**为相对时间且**重复发送**为“YES”，系统会立即于报表运行队列中放入该报表，待此次运行结束后依据**数据时间**的周期间隔预估下一次的运行时间并更新清单的**预计报表发送时间**。如果**重复发送**为“NO”，系统会立即于报表运行队列中放入该报表，并在执行一次之后自动将报表排程变成停用状态。

对于单次的报表排程，您可以通过清单页面的【刷新页面】来查看报表运行是否已经结束。

8.4. 移除报表定期发送配置

如果您不是要暂时停止报表的定期发送，而是要完全移除定期发送配置，请依以下步骤执行移除：

1. 先从清单页面（类似图 8-1 所示）的**分类**下拉菜单选择报表分类，再选择要移除定时发送设置的报表。

2. 单击【定时发送报表】开启排程设置窗口。

3. 单击【移除发送设置】再单击【确定】后，系统就会删除掉该报表的排程设置。

8.5. 添加/修改/删除

对报表的添加、修改和删除，请在 SecuCenter 的 **Current** 数据库上进行。如在 SecuLog 的数据库或 SecuCenter 的其他历史数据库上执行这些操作，其结果都是暂时性的。因为当 SecuCenter 运行定期备份时，会将本身的 **Current** 数据库同步到 SecuLog 的 **Current** 数据库，并覆盖掉 SecuLog 的 **Current** 数据库内容；而 SecuLog 或 SecuCenter 的其他历史数据库，在被移除时该历史数据库内的所有变更也会一并被移除。

图 8-6 报表编辑

◆ **从空白开始创建新报表**

先从清单页面（类似图 8-1 所示）的**分类**下拉菜单选择新报表的所属分类后，单击【添加】开启类似图 8-6 的添加页面。有关报表字段与条件的设置说明，请参阅 8.5.1 字段设置和 8.5.2 条件设置。

在编辑过程中，您随时可以单击【预览】来查看报表生成结果是否符合您所想要的样貌；再单击【编辑钻取条件】就可回到编辑页面。

编辑完后，单击【保存】，输入报表名称后，单击【提交】完成新报表的创建，并将新报表加入所选的分类中。

如果在清单页面没有看到新添加的报表，请单击【刷新页面】以重新刷新页面。

◆ **以现有报表为样板创建新报表**

先从清单页面（类似图 8-1 所示）的**分类**下拉菜单选择样板报表所属的报表分类，再选择作为样板的报表，然后单击【编辑钻取条件】开启类似图 8-6 的页面。有关报表字段与条件的设置说明，请参阅 8.5.1 字段设置和 8.5.2 条件设置。

在编辑过程中，您随时可以单击【预览】来查看报表生成结果是否符合您所想要的样貌；再单击【编辑钻取条件】就可以回到编辑页面。

编辑完后，单击【另存为】，输入报表名称后，单击【提交】完成新报表的创建，并将新报表加入与样板报表相同的的分类中。如单击【保存】将覆盖样板报表的原配置。

如果在清单页面没有看到新添加的报表，请单击【刷新页面】以重新刷新页面。

◆ **修改报表**

系统不允许您修改系统默认报表，仅允许您修改自定义的报表。

先从清单页面(类似图 8-1 所示)的**分类**下拉菜单选择要修改的报表所属的报表分类后，选择要修改的报表，然后单击【编辑钻取条件】开启类似图 8-6 的页面。有关报表字段与条件的设置说明，请参阅 8.5.1 字段设置和 8.5.2 条件设置。

在编辑过程中，您随时可以单击【预览】来查看报表生成结果是否符合您所想要的样貌；再单击【编辑钻取条件】就可以回到编辑页面。编辑完后，单击【保存】储存变更。

◆ **删除报表**

系统不允许您删除系统默认报表，仅允许您删除自定义的报表。

先从清单页面(类似图 8-1 所示)的**分类**下拉菜单选择要删除的报表所属的报表分类后，选择要删除的报表，然后单击【删除】再单击【确定】。

8.5.1. 字段设置

编辑页面的【选择字段】标签页用于设置报表上显示的字段、字段的显示顺序，及字段值的统计。

该报表主题（例，【审计报表】>【SQL 活动追踪】）下所有可选择的字段，分别列在**选择字段**框中的人、事、时、地、物、统计等类别下。已选择到报表的字段则罗列在**已选字段**框中，其从上至下的顺序相应于报表上从左至右的显示顺序。

图 8-7 报表字段设置

◆ **选择字段**

直接点击**选择字段**框中的一个字段，例如：“人”分类下的“OS 用户”字段，就可把“OS 用户”字段添加到**已选字段**框中，并且自动加到已选字段的最后面。

在“统计”分类下的“执行次数”是统计查询结果中相同数据行的笔数。相同数据行是指两笔或两笔以上的数据行中未套用任何 MAX、MIN、AVG、SUM 函数的各字段的内容完全相同。

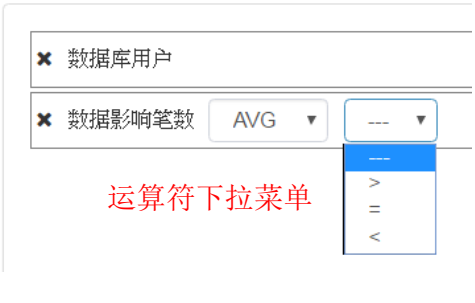
如要从**已选字段**框中移除某一个字段，您只需点击该字段前的叉号（X），就可以把该字段移除。

◆ **设置字段显示顺序**

已选字段框中字段从上到下的顺序相应于报表上从左到右的显示顺序，也就是说，最上面的字段是报表的第一列，依此类推。您可以直接使用拖放方式调整字段位置；也就是说，将鼠标移到要移动的字段上，按下鼠标左键将字段拖到指定位置后放开鼠标左键。

◆ **设置字段统计运算**

已选字段框中可计算的字段，其后面会出现函数下拉菜单（如下左图所示）。如果选择“---”就可把套用在该字段的统计运算函数移除。

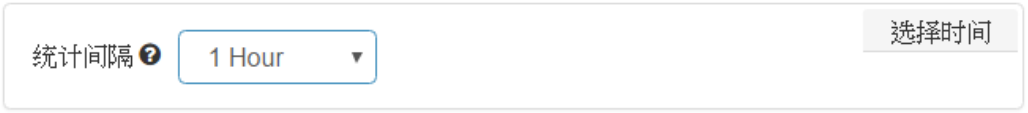


在查询结果中，系统会对相同数据行的该字段执行指定的统计函数运算。相同数据行是指两笔或两笔以上的数据行内未套用任何 MAX、MIN、AVG、SUM 函数的各字段的内容完全相同。

如果需要筛选出运算结果符合阈值（Threshold Value）的数据行，请在运算符下拉菜单（如上右图所示）选取运算符（>、=、<），并在最后面的文本框输入阈值。

◆ **设置字段统计时间间隔**

如果**已选字段**框包含了时间字段（例如：SQL 运行时间）和套用了函数（MAX、MIN、AVG、SUM）的字段（例如：数据影响笔数），那么在**选择时间**框内会出现时间间隔设置项如下所示，用以设置统计的时间间隔。当运行报表时，系统会依据指定的统计时间间隔和时间字段找出每个统计时间间隔内发生的数据访问活动，然后对于每个间隔内的数据行进行统计运算（例如：计算“数据影响笔数”的平均值）。

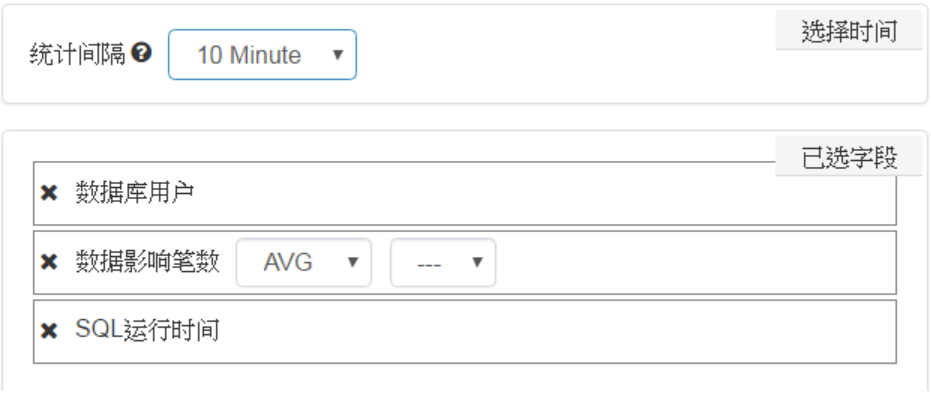


示例：计算每 10 分钟内各数据库用户的 SQL 访问活动平均影响的数据笔数。操作步骤如下：

1. 依序将“数据库用户”、“数据影响笔数”、“SQL 运行时间”等字段加入**已选字段**框。

2. 从“数据影响笔数”字段的函数下拉菜单选择 AVG 函数来计算平均每个数据库用户访问活动影响的数据笔数。

3. **统计间隔**的时间间隔设置为 **10 Minute**。系统通过指定的时间间隔和“SQL 运行时间”的时间值，将指定时间范围内的数据分成每 10 分钟一个区隔的数据集。



设置完成后，系统先依据 SQL 活动的运行时间找出每 10 分钟内发生的 SQL 访问活动，然后再以数据库用户为对象，计算每 10 分钟内每个数据库用户的 SQL 活动平均影响的数据笔数。

8.5.2. 条件设置

编辑页面的【选择条件】标签页用于设置报表筛选条件。

图 8-8 报表条件设置

从左侧**选择条件**框选择筛选字段，通过**设置条件**框来设置筛选字段的条件值，然后添加到**已选条件**框内的 AND 或 OR 运算框（通过 AND 和 OR 生成）中。

运算框上标识了该框使用的运算符，即为该框内筛选条件间使用的运算符。例如：运算框上标识为 AND 运算符，那么该运算框内条件间的运算符为 AND。

系统基于**设置条件**框中筛选字段的数据型态提供相应可选的运算符清单，并依据所选的运算符提供相应可使用的条件值组件。有关运算符与条件值组件的说明，请参阅 8.5.2.1 运算符与条件值组件。

当点选**选择条件**框中带有 "(D)" 前缀或 "(R)" 前缀的项目时，该项目会直接加入**已选条件**框内灰色标识的运算框中。"(D)" 前缀标识项目为已定义的条件。"(R)" 前缀标识项目为法条，此类项目是列在**法条**分类下，且仅已套用了审计条件且属于所选主题的法条才会显示在**法条**分类下。有关 "(D)" 和 "(R)" 前缀的项目的详细说明，请参阅 10 审计策略。

如果添加筛选条件时，**已选条件**框内尚无任何运算框，则系统会自动配置 AND 运算框并把筛选条件加入。

已选条件框中使用灰色来标识目前活跃的 AND/OR 运算框。筛选条件仅可添加到目前活跃的运算框中。单击某个运算框的 图标，把该运算框变为目前活跃的运算框。

如要编辑**已选条件**框中某个筛选条件的条件值，请点击该条件的 图标；如要移除某个条件，请点击该条件的 图标。如要移除**已选条件**框某个 AND/OR 运算框，请点击该运算框

的 ✖ 图标；运算框被移除时，运算框内的筛选条件，以及内层运算框会一并被移除。

示例： 以【审计报表】>【SQL 活动追踪】主题下的报表来说明如何设置报表的筛选条件。

假设欲加入的筛选条件如下：

(数据库用户 = *david* 或 *sa*) AND (数据库客户端 IP = *192.168.125.111*) ➡ A 条件组

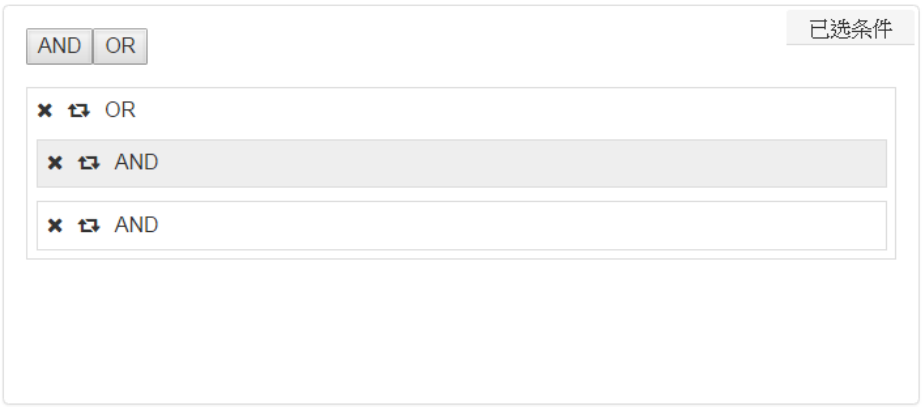
OR

(数据库用户 = *frank* 或 *jack*) AND (数据库客户端 IP = *192.168.125.220*) ➡ B 条件组

以下为设置步骤：

1. 每一个红色标识的运算符对应一个运算框。需从最外层开始添加每个运算符相应的运算框。

   a.) 点击 OR 添加最外层的 OR 运算框。也就是 A 条件组和 B 条件组间的 OR 运算符。
   b.) 点击 AND 在 OR 运算框内添加第一个 AND 运算框，也就是 A 条件组内两个条件间的 AND 运算符。
   c.) 点击 OR 运算框的 🔁，使其成为目前活跃的运算框（即以灰色标识）。
   d.) 点击 AND 在 OR 运算框内添加第二个 AND 运算框，也就是 B 条件组内两个条件间的 AND 运算符。



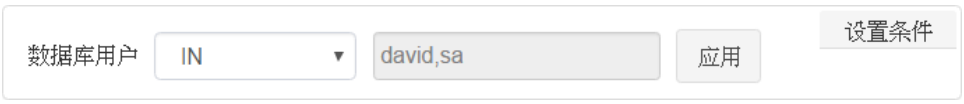
2. 单击第一个 AND 运算框的 🔁，其成为目前活跃的运算框。

3. 从**选择条件**框中点选【人】>【数据库用户】。

4. 到**设置条件**框中，设置条件字段“数据库用户”的运算符和条件值。

   a.) 从运算符下拉菜单中选择 **IN** 运算符。
   b.) 点击条件值输入框，开启如下多选窗口。多选窗口左侧清单为可选择的条件值，右侧清单为已选择的条件值。有关多选窗口的操作说明，请参阅 8.5.2.2 多选窗口。

此示例中的用户帐号 *david* 和 *sa* 不在清单内，您必须直接在文本框输入 *david*，然后单击【添加】，把该帐号加入右边清单内。重复同样动作把示例的 *sa* 加入。单击【提交】把条件值带回**设置条件**框中的文本框内。

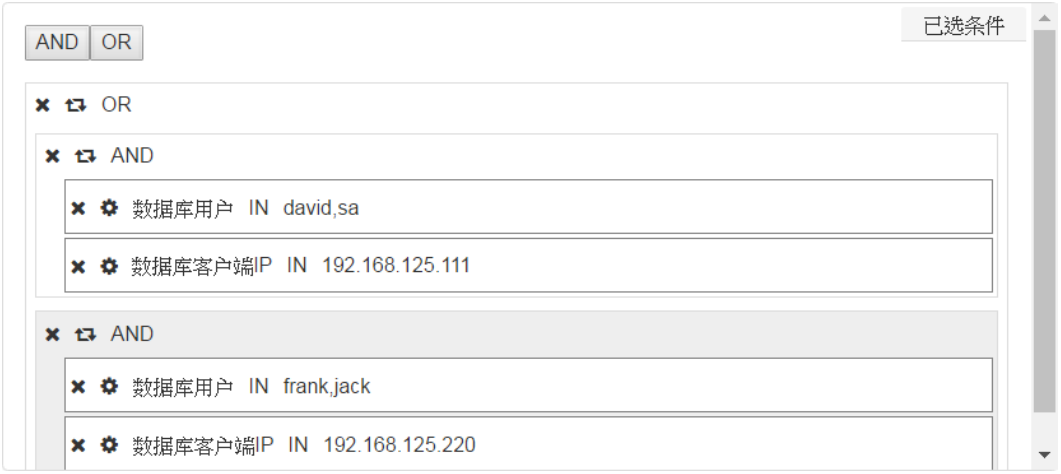


c.) 单击**设置条件**框的【应用】，把筛选条件加入**已选条件**框中的第一个 AND 运算框内。

5. 在**选择条件**框中点选【地】>【数据库客户端 IP】。然后参照第 4 步骤的方式，设置条件字段“数据库客户端 IP”的运算符和条件值，并添加到**已选条件**框中的第一个 AND 运算框内。

6. 单击第二个 AND 运算框的 ，其成为目前活跃的运算框。

7. 重复上面的 2~5 步骤把 B 条件组中的筛选条件加入**已选条件**框中的第二个 AND 运算框内。



8.5.2.1. 运算符与条件值组件

系统会依据筛选字段的数据型态提供相应可选的运算符清单，并依据所选的运算符提供相应可使用的条件值组件。

表 8-4 运算符和相应条件值组件的操作与运行说明

运算符	条件值组件	筛选操作与运行说明
=、>=、<= <>、>、< LIKE NOT LIKE LIKE_BEGIN LIKE_END	文字文本框	文字文本框只允许输入一个数值或字串。字串可以包括文字、数字，及符号，例：“，”、“：”。 LIKE，筛选出筛选字段值中含有指定字串的数据行。 NOT LIKE，筛选出筛选字段值中不含有指定字串的数据行。 LIKE_BEGIN，筛选出筛选字段值的起始字串与指定字串相同的数据行。 LIKE_END，筛选出筛选字段值的结尾字串与指定字串相同的数据行。
NULL NOT NULL		用于筛选出筛选字段值为 NULL 或非 NULL 的数据行。
IN SET NOT IN SET	下拉菜单	菜单中选项为已定义的数据集。有关数据集的创建与设置说明，请参阅 10 审计策略的 10.1 数据集和确认名单。 IN SET，筛选出筛选字段值与数据集中任一值相同的数据行。 NOT IN SET，筛选出筛选字段值与数据集中任一值都不相同的数据行。
IN NOT IN	多选窗口 (类似图 8-9)	通过多选窗口，您可以指定多个条件值。有关该多选窗口的操作说明，请参阅 8.5.2.2 多选窗口。 IN，筛选出筛选字段值与任一指定条件值相同的数据行。 NOT IN，筛选出筛选字段值与任一指定条件值都不相同的数据行。
MULTI_IN NOT MULTI_IN MULTI_LIKE NOT MULTI_LIKE	多选窗口 (类似图 8-9)	通过多选窗口，您可以指定多个条件值。有关该多选窗口的操作说明，请参阅 8.5.2.2 多选窗口。 这些运算符仅适用于字段值是一个值组，也就是包含

运算符	条件值组件	筛选操作与运行说明
		多个值，且值之间是以逗号为分隔符号。例如：“表清单”字段的值为“customer,order,payment”。筛选是将字段中逗号分隔的每个值与条件值做比较。 MULTI_IN，筛选出筛选字段值组中包含了任一个指定条件值的数据行。例如：条件值为“customer,order”，则字段值组为“customer,payment”、“order,payment,customer”等等的数据行都符合筛选条件；而字段值组为“payment,bill”的数据行就不符合筛选条件。 NOT MULTI_IN，筛选出筛选字段值组中不含有任一个指定条件值的数据行。例如：条件值为“customer,order”，则字段值组为“customer,payment”、“order,payment,customer”等等的数据行都不符合筛选条件；而字段值组为“payment,bill”的数据行就符合筛选条件。 MULTI_LIKE 是将逗号分隔的每个值视为一个字串来做筛选，用于筛选出筛选字段值组中具有任一个指定字串的数据行。例如：条件值为“cust,ord”，则字段值组为“custsum,payment”、“order,payment,CN_customer”等等的数据行都符合筛选条件；而字段值组为“payment,bill_cus”的数据行就不符合筛选条件。 NOT MULTI_LIKE 是将逗号分隔的每个值视为一个字串来做筛选，用于筛选出筛选字段值组中没有任一个指定字串的数据行。

8.5.2.2. 多选窗口

图 8-9 多选窗口

窗口左侧清单是从捕捉的数据访问活动中汇整出来的数据集合，右侧清单为您已选择的条件值。当点击左侧清单项目，该项目会自动从左侧清单移到右侧清单中；当点击右侧清单项目，该项目会自动从右侧清单移到左侧清单中。

如在文本框输入字串后点击【搜索】，左边清单将列出以该字串为开头的项目，并在清单显示符合的项目数。如清除文本框内容后点击【搜索】，左边清单将重新列出原本的清单项目。

如要设置的条件值不在清单上，您可直接在文本框输入该条件值后，单击【添加】把条件值添加到右侧清单内。所有手动添加到右侧清单的项目，因为原本就不是从数据访问活动中汇整出来的，当从右侧清单移除时并不会出现在左侧清单内。

9. 告警

SecuLog 不提供告警通知设置与变更功能，也不提供数据访问活动告警发送功能，如使用 SecuLog 网页接口，请忽略此章。

除了报表外，您还可以通过告警通知及时得知发生了某项关注的数据访问活动，以及 dbAudit 的系统资源使用和系统性能等等告警信息。

【审计告警】是针对受监控的数据库服务器/Web 服务器上的访问活动提供告警配置，而【系统告警】是针对 dbAudit 系统上的访问活动和系统资源使用状况等提供告警配置。

除了默认告警外，您可以依据企业需求，在【审计告警】或【系统告警】的各告警主题中自定义告警。

左侧【审计告警】或【系统告警】菜单中的不同告警主题对不同监控对象提供告警配置。例如:【审计告警】>【SQL 活动追踪】内的告警用于监控目标数据库访问活动，因此仅提供与 SQL 活动有关的配置字段。

点击【审计告警】或【系统告警】下某一告警主题后，开启该主题的告警管理与操作页面。例如:【审计告警】>【SQL 活动追踪】开启类似以下的告警管理与操作页面。您可使用**分类**下拉菜单选择列出哪个分类下的 SQL 活动追踪相关的告警，并对其中的告警进行添加、修改与删除。分类主要包括各种法规、异常管理和一般审计追踪，让您能够将告警储存于适当类别，之后可依据类别迅速找到需要调整或检视的告警。

系统默认列显示勾号的项目为系统默认告警，是不允许用户修改或删除的，仅允许直接运行或作为告警创建的样板。有关告警的启用/停用和创建等操作，请参阅以下章节。

图 9-1 告警管理（SQL 活动追踪）

9.1. 在线查看

除了事件发生时通过告警通知通知相关人员外，您也可以随时从告警清单上直接查看任一告警事件在某个时间段发生的事件。

请先从清单页面（类似图 9-1 所示）选择欲查看的告警事件（例：数据库登录）并指定查看的时间段后，单击【检验】，系统将开启新标签页来显示该指定时间段内发生的告警事件（类似下图所示）。您可以变更该标签页上的时间段，以查看其他时间段的数据。有关时间段的设置说明，请参阅 4.3 数据时间段设置。

图 9-2 指定时间段内发生的告警事件

点击列头（例如，点击上图的“数据库用户”列头），则页面上的显示结果将以该字段的升序进行排序，再次点击时，将以该字段的降序进行排序。

如果想要查看更多字段或移除某些不想查看的字段，可单击【编辑检验条件】进入编辑页面；在编辑过程中可单击【检验】来检视依据修改后配置所重新生成的结果。在编辑页面上的变更为暂时性的，除非您在编辑页面上单击【保存】或【另存为】来保存变更。有关编辑页面的操作说明，请参阅 9.4 添加/修改/删除。

除了在线查看外，您可以设置事件的告警通知，自动检验是否有事件发生，一旦有事件发生时就会发送告警通知给指定的人员。有关告警通知设置的说明，请参阅 9.2 告警通知设置。

9.2. 告警通知设置

通过告警通知设置，系统会自动依照事件检验条件来检验是否有事件发生；当有事件发生时，系统会依照您指定的通知对象与签核流程发送告警通知给相关人员。并且您可以通过签核流程的方式来追踪与掌握告警事件是否已经获得适当处理。

请先从类似图 9-1 的清单选择要添加或修改告警通知配置的告警事件后，单击【定时发送告警】开启类似以下的设置窗口。

图 9-3 告警定时发送配置

表 9-1 警定时发送配置字段说明

字段	说明
通知对象	告警通知发送对象。
签核流程	告警通知套用的签核流程。有关签核流程设置的说明，请参阅 11.1 签核流程配置。
导出格式	告警通知的附件内容格式。目前提供 csv、html、pdf、xls、xml 等格式。
最大行数	告警通知内容包含的最大数据笔数。
启用	是否启动告警通知设置。
数据时间	指定检验哪个时间段的数据。如果是使用相对时间区间，那么系统将以指定的相对时间间隔，作为运行周期间隔。例如：选择**每 15 分钟**，那么系统将每 15 分钟运行一次告警事件检验。 有关数据时间段的设置说明，请参阅 4.3 数据时间段设置。

通知对象和**签核流程**两个字段必须设置一个，两个都设置也可以。如果指定了签核流程，系统会将告警通知发送给该签核流程的第一层人员。有关签核流程的运行与操作说明，请参阅 11 事件签核流程。

设置完毕后单击【提交】保存告警通知设置并返回清单页面。如果**启用**为“YES”，其清单上**定时发送报表**将显示 ON 表示告警通知为启用状态；如果为“NO”，将显示 OFF 表示告警通知为停用状态。您可以单击清单上**定时发送报表**内的图标变更告警通知的启用或停用状态。同时，系统依据**数据时间**设置预估运行告警事件检验的时间点并显示在清单的**预计报表发送时间**。

9.3. 移除告警通知设置

如果您不是要暂时停止事件的告警通知，而是要完全移除告警通知的设置，请依以下步骤执行移除：

1. 先从清单页面（类似图 9-1 所示）的**分类**下拉菜单选择告警分类，再选择要移除发送设置的告警事件。

2. 单击【定时发送告警】开启告警通知设置窗口。

3. 单击【移除发送设置】再单击【确定】后，系统就会删除掉该告警事件的告警通知设置。

9.4. 添加/修改/删除

图 9-4 告警编辑页面

◆ **从空白开始创建新告警**

先从清单页面（类似图 9-1 所示）的**分类**下拉菜单选择新告警所属的告警分类后，单击【添加】开启类似图 9-4 的添加页面。告警通知字段与条件的设置操作与报表的相同，相关说明请参阅 8.5.1 字段设置和 8.5.2 条件设置。

在编辑过程中，您随时可以单击【检验】来查看告警的事件信息样貌是否符合您想要；

再单击【编辑检验条件】就可回到编辑页面。

编辑完后，单击【保存】，输入告警名称和设置告警级别后，单击【提交】完成新告警的创建，并将新告警加入所选的分类中。告警级别用于标识告警事件的严重度，其分为信息、警告、错误、严重错误。

如果在清单页面没有看到新添加的告警，请单击【刷新页面】以重新刷新页面。

- **以现有告警为样板创建新告警**

先从清单页面（类似图 9-1 所示）的**分类**下拉菜单选择样板告警所属的告警分类，再选择作为样板的告警，然后单击【编辑检验条件】开启类似图 9-4 的页面。告警通知字段与条件的设置操作与报表的相同，相关说明请参阅 8.5.1 字段设置和 8.5.2 条件设置。

在编辑过程中，您随时可以单击【检验】来查看告警的事件信息样貌是否符合您想要的；再单击【编辑检验条件】就可回到编辑页面。

编辑完后，单击【另存为】，输入告警名称和设置其告警级别后，单击【提交】完成新告警的创建，并将新告警加入与样板告警相同的的分类中。如单击【保存】将覆盖样板告警的原配置。告警级别用于标识告警事件的严重度，其分为信息、警告、错误、严重错误。

如果在清单页面没有看到新添加的告警，请单击【刷新页面】以重新刷新页面。

- **修改告警**

系统不允许您修改系统默认告警，仅允许您修改自定义的告警。

先从清单页面(类似图 9-1 所示)的**分类**下拉菜单选择要修改的告警所属的告警分类后，选择要修改的告警，然后单击【编辑检验条件】开启类似图 9-4 的页面。告警通知字段与条件的设置操作与报表的相同，相关说明请参阅 8.5.1 字段设置和 8.5.2 条件设置。

在编辑过程中，您随时可以单击【检验】来查看告警的事件信息样貌是否符合您想要的；再单击【编辑检验条件】就可回到编辑页面。编辑完后，单击【保存】储存变更。

- **删除告警**

系统不允许您删除系统默认告警，仅允许您删除自定义的告警。

先從清單頁面（類似图 9-1 所示）的**分類**下拉選單中選擇要刪除的警示所屬的警示分類後，選擇要刪除的警示，然後按【刪除】再按【確認】。

10. 审计策略

每一个数据访问活动必然是由 5W 要项：人（Who，动作执行者）、事（What，执行的动作或操作）、时（When，发生的时间）、地（Where，发生地点）、物（onWhat，拿取了什么东西）等组成，而对于每一活动的审计也是必然从 5W 角度进行。因此，dbAudit 通过【策略管理】的【法条】、【条件】和【数据集】和【未确认名单管理】以 5W 角度帮助您建立各审计法条相应的 5W 条件，以及特定 5W 对象群（例如：外包人员、人事人员、财务人员、可疑用户等等）。

以下章节将从【数据集】和【未确认名单管理】开始说明如何建立数据集（特定 5W 对象群），接着说明如何在【条件】建立 5W 审计条件，然后说明如何通过【法条】组合审计条件以具体化法规和信息安全规范的条文要求。

法条、条件和数据集的添加、修改和删除应在 SecuCenter 的 **Current** 数据库上进行。在 SecuLog 的数据库或 SecuCenter 的其他历史数据库上执行这些操作，其结果都是暂时性的。因为当 SecuCenter 运行定期备份时，会将本身的 **Current** 数据库同步到 SecuLog 的 **Current** 数据库，并覆盖掉 SecuLog 的 **Current** 数据库内容；而 SecuLog 或 SecuCenter 的其他历史数据库，在被移除时该历史数据库内的所有变更也会一并被移除。

10.1.数据集和确认名单

10.1.1. 数据集

dbAudit 自动将采集的每一数据访问活动的数据依照 5W 分类（人、事、时、地、物）与系统默认数据源类别（例如：全域用户、全域端口、全域客户端 IP、全域参数值、全域数据表等等）归整为不同的*基础数据集*。

您可以依据您赋予数据的意义，将*基础数据群*中的数据归类成不同对象群（也就是数据集），例如：依据人员角色将人（Who）分类下的用户帐户数据归类成外包人员、人事人员、财务人员、可疑用户等数据集。数据集，可作为与 IN SET 和 NOT IN SET 运算符搭配的条件值选项。有关筛选条件运算符和条件值组件的说明，请参阅 8.5.2.1 运算符与条件值组件。

以数据集作为条件值，可使筛选条件不再因条件值变更而需要调整。也就是说，如果有一个以上的报表/告警使用了同样的筛选条件，您不再需要因为筛选条件使用的条件值变动而需要逐一修改每一报表/告警的筛选条件的条件值，还担心会有遗漏修改的。

例如：筛选条件为：数据库用户 IN (“usera”, “userb”, “userc”)，其中的条件值 usera、userb、userc 为人事人员帐户。一旦多一个人员或移除一个人员，您都需要回来调整这个筛选条件。如果创建一个 “人事人员” 数据集，把 usera、userb、userc 放在这个数据集内，并把该筛选条件改成：数据库用户 IN SET 人事人员。以这样的方式，则无论 “人事人员” 数据集的数

据如何变更，都不需要重新调整筛选条件。

单击【策略管理】>【数据集】将开启类似以下的数据集清单。可通过**分类**下拉菜单与**数据源**下拉菜单选择列出哪一个*基础数据集*中的数据集，并对该*基础数据集*中的数据集进行添加、修改与删除。

分类下拉菜单的选项为 5W 分类。**数据源**下拉菜单的选项为系统默认数据源类别。因此，dbAudit 自动将采集的每一数据访问活动的数据依照**分类**和**数据源**中的选目归整为不同的*基础数据集*。

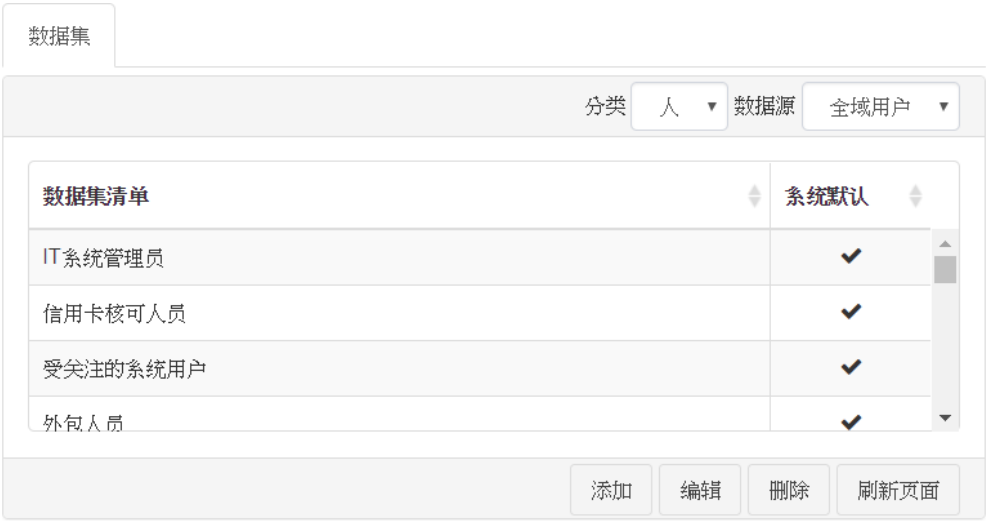


图 10-1 数据集管理

- **添加数据集**

先从清单页面（类似图 10-1 所示）的**分类**和**数据源**下拉菜单选择新数据集所属的分类和数据源后，单击【添加】开启类似图 10-2 的设置窗口。

系统依据**分类**和**数据源**决定使用哪一个*基础数据集*来进行新数据集的创建。添加窗口上的左侧列表是特定*基础数据集*的可用数据，右侧列表为您已选择的条件值。例如：使用**分类**为“人”和**数据源**为“全域用户”的*基础数据集*来创建数据集。有关该对话窗口的操作与多选窗口相同，相关操作说明，请参阅 8.5.2.2 多选窗口。

完成右侧清单设置，并在**名称**字段给予了数据集名称后，单击【提交】创建新数据集。如果在清单上没有看到新数据集，请单击【刷新页面】以重新刷新页面。

- **修改数据集**

先从清单页面（类似图 10-1 所示）的**分类**和**数据源**下拉菜单选择要修改的数据集所属的分类和数据源后，再选择要修改的数据集，然后单击【编辑】开启类似图 10-2 的设置窗口。

分类和**数据源**的选择限制了该数据集的数据是基于那一个*基础数据集*来设置的。修改窗口上的左侧列表是特定*基础数据集*的数据，右侧列表为您已选择的条件值。例如：修改**分类**为“人”且**数据源**为“全域用户”的任一数据集，而数据集仅可使用该特定*基础数据集*的数据。有关该对话窗口的操作与多选对话窗口相同，相关操作说明，请参阅 8.5.2.2 多选窗口。

完成右侧清单设置后，单击【提交】储存。如数据集已经被任一筛选条件引用，系统就不允许您变更该数据集的名称。

图 10-2 数据集设置

◆ **删除数据集**

先从清单页面（类似图 10-1 所示）的**分类**和**数据源**下拉菜单选择要删除的数据集所属的分类和数据源后，再选择要删除的数据集，然后单击【删除】再单击【确定】。

如该数据集已经被任一筛选条件引用，系统就不允许您删除该数据集。

10.1.2. 确认名单

除透过【策略管理】>【数据集】定义数据集外，您还可通过【策略管理】>【未确认名单管理】直接对捕捉的数据活动中特定字段的值进行识别，将其归整为确认名单与未确认名单。

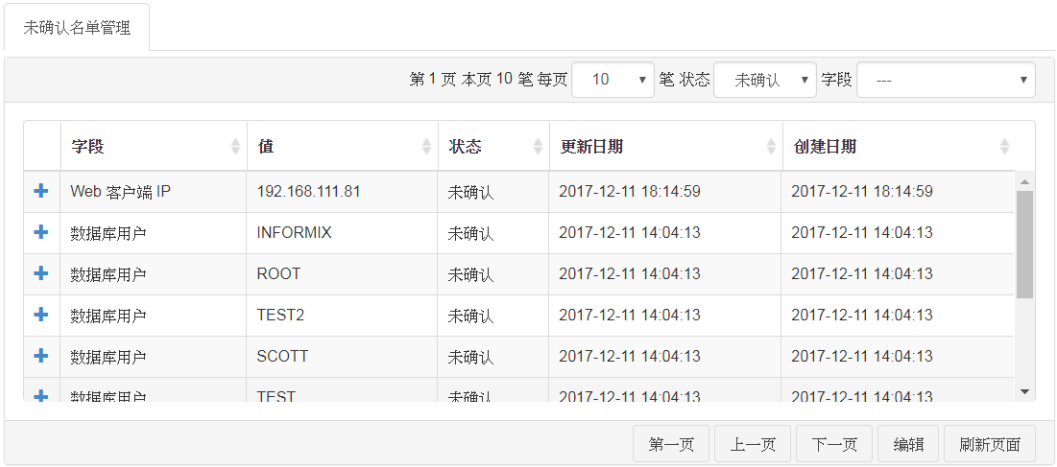


图 10-3 未确认名单管理

【策略管理】>【未确认名单管理】默认显示这些特定字段的所有未确认值。如要查看这些特定字段中已确认的值，请在**状态**下拉菜单选择“已确认”。如要查看某个特定字段中已确认或未确认的值，请先在**字段**下拉菜单选择该字段，然后在**状态**下拉菜单中选择“已确认”或“未确认”以查看该字段中已确认的值或未确认的值。

这些特定字段的值都是来自 dbAudit 捕捉的数据访问活动，其缺省为未确定状态。

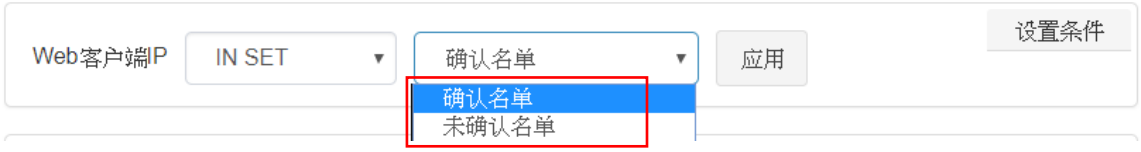
如某特定字段的值为确认知道的，请先选择该笔数据，然后单击【编辑】开启类似以下的编辑窗口，将**状态**字段设置为“已确认”后单击【提交】储存。

如某特定字段的值设置为“已确认”但后来发现其实是不认得的，那么请先选择该笔数据，然后单击【编辑】开启类似以下的编辑窗口，将**状态**字段设置为“未确认”后单击【提交】储存。

图 10-4 修改字段值的确认状态

字段中所有标识为已确认的值，将会自动纳入该字段的确认名单中，而标识为未确认的值将会自动纳入该字段的未确认名单中。

例如：“Web 客户端 IP”这个字段中所有已确认的值将纳入该字段的确认名单中，而该字段中所有未确认的值将纳入该字段的未确认名单中，那么在报表、警示的筛选条件配置页面上使用“Web 客户端 IP”字段并搭配 IN SET 运算符时，将可看到如下图所示该字段相应的确认名单与未确认名单选项。



每个特定字段都有相应的这两个默认数据集：确认名单、未确认名单。如同【策略管理】>【数据集】定义的数据集一样，确认名单和未确认名单可作为筛选条件的条件值（与 IN SET 和 NOT IN SET 运算符搭配），使得筛选条件不再因条件值变更而需要额外的调整操作。

10.2.条件

为了能够从法条角度的 5W 来检验数据访问活动是否符合法条的要求，您必须先通过【策略管理】>【条件】来建立 5W 审计条件，再通过【策略管理】>【法条】将已定义的审计条件套用到法条上以具体化法条的审计要求。

审计条件除了可以被法条引用外，也可以作为报表/告警的筛选条件。在报表/告警的筛选条件设置页面，审计条件是以前缀“(D)”作为标识。有关筛选条件设置页面的操作说明，请参阅 8.5.2 条件设置。

单击【策略管理】>【条件】将开启类似以下的审计条件清单。您可使用**主题**下拉菜单与**分类**下拉菜单选择列出哪个主题的哪个分类下的审计条件，并对其中的条件进行添加、修改与删除。主题下定义的条件，只能提供给相同主题的法条使用。

例如：**主题**选“SQL 活动追踪”、**分类**选“人”，将列出该主题下所有以人为基础定义的条件。

图 10-5 审计条件管理（SQL 活动追踪）

- **从空白开始创建新审计条件**

先从清单页面（类似图 10-5 所示）的**主题**和**分类**下拉菜单选择新条件所属的主题和 5W 分类后，单击【添加】开启类似图 10-6 的添加页面。系统依据**主题**和**分类**的选择决显示新审计条件可用的条件字段。有关条件设置的操作说明，请参阅 8.5.2 条件设置。

设置完后，单击【保存】，输入条件名称后，单击【提交】完成新审计条件的创建，并将新审计条件加入所选的主题与分类中。

如果在清单页面没有看到新添加的审计条件，请单击【刷新页面】以重新刷新页面。

- **以现有条件为样板创建新审计条件**

先从清单页面（类似图 10-5 所示）的**主题**和**分类**下拉菜单选择样板条件所属的主题和 5W 分类，再选择作为样板的审计条件，然后单击【编辑】开启类似图 10-6 的页面。系统依据**主题**和**分类**的选择显示新审计条件可用的条件字段。有关条件设置的操作说明，请参阅 8.5.2 条件设置。

设置完后，单击【另存为】，输入条件名称后，单击【提交】完成新审计条件的创建，并将新审计条件加入与样板条件相同的主题与分类中。如单击【保存】将覆盖样板条件的原配置。

如果在清单页面没有看到新审计条件，请单击【刷新页面】以重新刷新页面。

◆ **修改审计条件**

系统不允许您修改系统默认审计条件，仅允许您修改自定义的审计条件。

先从清单页面（类似图 10-5 所示）的**主题**和**分类**下拉菜单选择要修改的条件所属的主题和 5W 分类后，再选择要修改的审计条件，然后单击【编辑】开启类似图 10-6 的页面。系统依据**主题**和**分类**的选择显示该审计条件可使用的条件字段。有关条件设置的操作说明，请参阅 8.5.2 条件设置。设置完后，单击【保存】储存变更。

图 10-6 审计条件设置

◆ **删除审计条件**

系统不允许您删除系统默认审计条件，仅允许您删除自定义的审计条件。

先从清单页面（类似图 10-5 所示）的**主题**和**分类**下拉菜单选择要删除的条件所属的主题和分类，再选择要删除的审计条件，然后单击【删除】再单击【确定】。

10.3.法条

您可以通过【策略管理】>【法条】来管理与维护各法规的法条，并依据法条的要求引用适当的审计条件以具体实现法条。

已被具体化的法条可以作为报表/告警的筛选条件，用于检验数据访问活动是否符合法条要求。在报表/告警的筛选条件设置页面，已具体化法条是以前缀 “(R)” 作为标识。有关筛选条件设置页面的操作说明，请参阅 8.5.2 条件设置。

单击【策略管理】>【法条】将开启类似以下的法条清单与其具体化对应的 5W 条件。您可通过**主题**下拉菜单与**分类**下拉菜单选择列出哪个法规下与哪个主题相关的法条，并对其中的法条进行添加、修改与删除。

对于**分类**下拉菜单中不适用于您的企业的法规，您可以通过【策略管理】>【法规】将法规关闭而不在出现在下拉菜单中。

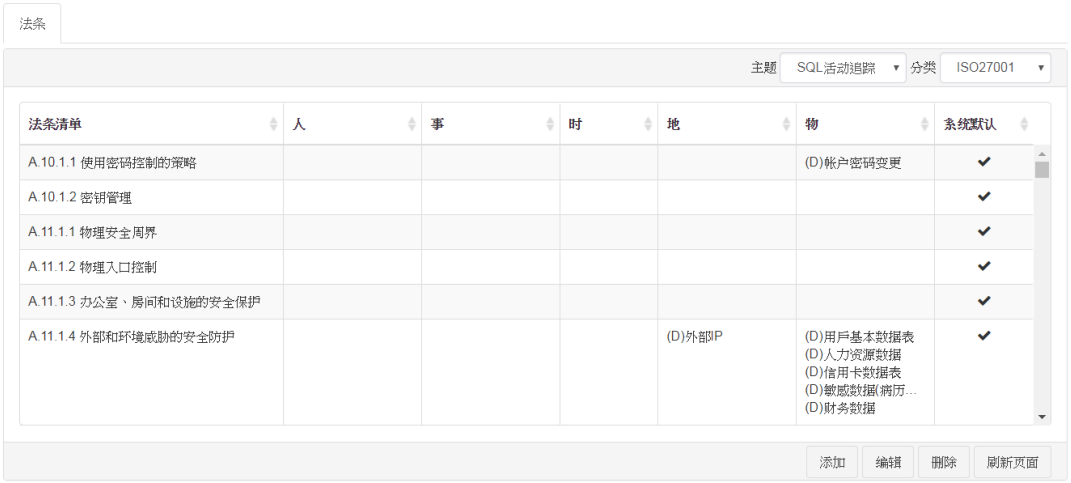


图 10-7 法条管理（SQL 活动追踪）

图 10-8 法条引用条件设置

◆ **从空白开始创建新法条**

先从清单页面（类似图 10-7 所示）的**主题**和**分类**下拉菜单选择新法条所属主题和法规后，单击【添加】开启类似图 10-8 的添加页面。

系统依据**主题**的选择显示新法条可引用的 5W 审计条件。法条只能引用相同主题下定义的审计条件，且法条仅可基于审计条件来配置，如果需要的审计条件不存在，请先参阅 10.2 条件的添加操作说明来建立所需的审计条件。

左侧为 5W 分类中各分类中已定义的审计条件，右侧为已选的审计条件。当点选**选择条件**框中某一分类下的条件时，该条件会自动加入**已选条件**框中同样分类的框中。**已选条件**框中，同一分类的条件间为 OR 关系，而 5W 分类间为 AND 关系。

示例：假设法条要求检验：移动用户与信用卡核可人员的数据异动行为（修改与删除）。下图显示其具体实现的条件配置，其展开的表达式就是：

（“移动用户” OR “信用卡核可人员”）AND （“数据异动 – 修改、删除”）

设置完后，单击【保存】，输入法条名称后，单击【提交】完成新法条的创建，并将新法条加入所选的主题与分类中。

如果在清单页面没有看到新法条，请单击【刷新页面】以重新刷新页面。

◆ **以现有法条为样板创建新法条**

先从清单页面（类似图 10-7 所示）的**主题**和**分类**下拉菜单选择样板发条所属的主题和法规，再选择作为样板的法条，然后单击【编辑】开启类似图 10-8 的页面。

系统依据**主题**的选择显示法条可引用的 5W 审计条件。法条只能引用相同主题下定义的审计条件，且法条仅可基于审计条件来配置，如果需要的审计条件不存在，请先参阅 10.2 条件的添加操作说明来建立所需的审计条件。

左侧为 5W 分类中各分类中已定义的审计条件，右侧为已选的审计条件。当点选**选择条件**框中某一分类下的条件时，该条件会自动加入**已选条件**框中同样分类的框中。**已选条件**框中，同一分类的条件间为 OR 关系，而 5W 分类间为 AND 关系。

示例：假设法条要求检验：移动用户与信用卡核可人员的数据异动行为（修改与删除）。下图显示其具体实现的条件配置，其展开的表达式就是：

（“移动用户” OR “信用卡核可人员”）AND （“数据异动 – 修改、删除”）

设置完后，单击【另存为】，输入法条名称后，单击【提交】完成新法条的创建，并将新法条加入与样板法条相同的主题与分类中。如单击【保存】将覆盖样板法条的原配置。

如果在清单页面没有看到新法条，请单击【刷新页面】以重新刷新页面。

- **修改法条**

系统不允许您修改系统默认法条，仅允许您修改自定义的法条。

先从清单页面（类似图 10-7 所示）的**主题**和**分类**下拉菜单选择要修改的法条所属的主题和法规后，再选择要修改的法条，然后单击【编辑】开启类似图 10-8 的页面。

系统依据**主题**的选择显示该法条可使用的 5W 审计条件。法条只能引用相同主题下定义的审计条件，且法条仅可基于审计条件来配置，如果需要的审计条件不存在，请先参阅 10.2 条件的添加操作说明来建立所需的审计条件。

左侧为 5W 分类中各分类中已定义的审计条件，右侧为已选的审计条件。当点选**选择条件**框中某一分类下的条件时，该条件会自动加入**已选条件**框中同样分类的框中。**已选条件**框中，同一分类的条件间为 OR 关系，而 5W 分类间为 AND 关系。

设置完后，单击【保存】储存变更。

- **删除法条**

系统不允许您删除系统默认法条，仅允许您删除自定义的法条。

先从清单页面（类似图 10-7 所示）的**主题**和**分类**下拉菜单选择要删除的法条所属的主题和法规后，再选择要删除的法条，然后单击【删除】再单击【确定】。

10.4.法规合规检验

通过【策略管理】>【法条施行对照单】您可以清楚看到哪些法条已经被报表或告警引用，以及是否有设置排程报表，并且可从法条角度立即开启相应的报表/告警检验数据访问活动是否符合法条要求与是否有违反的事件发生。

可使用【法条施行对照单】的**分类**下拉菜单选择列出不同法规下的法条施行对照单。对于**分类**下拉菜单中不适用于您企业的法规，您可以通过【政策管理】>【法规】将法规关闭而不出现在下拉选单中。

假设，在【策略管理】>【法条】的审计追踪分类创建了“内部审计规则 A”法条，并应用了适当的审计条件（有关操作说明，请参阅 10.3 法条与 10.2 条件）。然后，在某个报表与告警的筛选条件都引用了该法条，并且设置了该报表的发送排程（有关操作说明，请参阅 8.5.2 条件设置和 8.3 报表定时发送配置）。那么在【策略管理】>【法条施行对照单】的审计追踪分类的法条清单上，“内部审计规则 A”法条对应的各列就会显示如下。

图 10-9 法条施行对照单

报表列表显示的数字，表示在筛选条件中引用相应法条的报表数。当点击该单元格时将开启类似下面的窗口，列出筛选条件中引用该法条的报表。勾选一个或多个报表后单击【提交】，系统将为每个报表开启一个标签页显示报表结果。有关报表在线查看的操作说明，请参阅 8.1 在线查看。

警示列表显示的数字，表示在筛选条件中引用相应法条的告警数。当点击该单元格时会开启类似下面的窗口，列出筛选条件中引用该法条的告警。勾选一个或多个告警后单击【提交】，系统将为每个告警开启一个标签页显示告警事件查验结果。有关告警在线查看的操作说明，请参阅 9.1 在线查看。

排程监控显示勾号，表示引用相应法条的报表中至少有一个配置了定时发送。

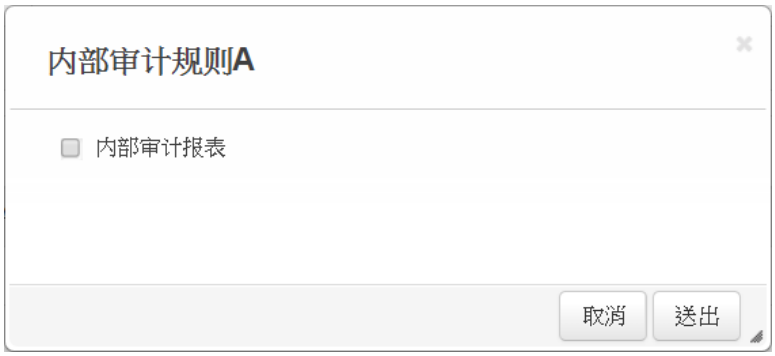


图 10-10 法条对应的报表（或告警）清单

11. 事件签核流程

SecuLog 不提供事件签核与签核记录查阅。如使用 SecuLog 网页接口，请忽略此章。

对于【审计告警】与【系统告警】中已配置签核流程的告警，当告警事件发生时，系统会发送告警通知给指定签核流程中的第一阶人员，同时在第一阶人员的事件审核箱中放入一笔待处理告警通知。

当第一阶人员处理完并通过【事件管理】>【事件审核】提交签核时，系统会依签核流程通知第二阶人员，同时将该笔告警通知移往第二阶人员的事件审核箱中。

当第二阶人员通过【事件管理】>【事件审核】提交时，系统会依签核流程通知第三阶人员，同时将该笔告警通知移往第三阶人员的事件审核箱中；如第二阶人员通过【事件管理】>【事件审核】退回告警通知的处理，系统会依签核流程通知第一阶人员，同时将该笔告警通知退回到第一阶人员的事件审核箱中。

这样的签核过程会持续到该告警通知处理完毕结案。

例如：签核流程配置为 John Smith –> Joy White –> Mary Smith。John Smith 为第一阶人员，Joy White 为第二阶人员，而 Mary Smith 为第三阶人员。

当配置了该签核流程的告警事件发生时，系统会发送告警通知给 John Smith，并在 John Smith 的事件审核箱放入该笔待处理告警通知。当 John Smith 处理完并提交时，系统会通知 Joy White 并将该笔告警通知移往 Joy White 的事件审核箱。当 Joy White 处理完并提交时，系统会通知 Mary Smith 并将该笔告警通知移往 Mary Smith 的事件审核箱。

11.1.签核流程配置

【策略管理】>【用户阶层管理】开启签核流程的管理界面，如下所示。您可依据企业需要创建签核流程并配置流程中各阶层人员。

图 11-1 签核流程管理

如要添加新签核流程，请单击【添加】开启类似下面的添加页面。如要编辑签核流程，请先从**用户流程清单**上选择要修改的流程，然后单击【编辑】开启类似下面的页面。

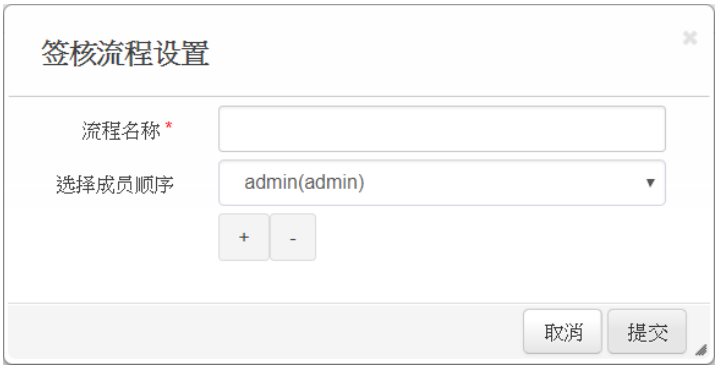


图 11-2 签核流程设置

流程名称为签核流程名称。**选择成员顺序**用于设置流程中的人员以及人员间的签核阶层关系。点击 + 会在**选择成员顺序**的最下方添加一個下拉菜单；点击 - 会将**选择成员顺序**的最后一个下拉菜单移除。一个下拉菜单设置一个阶层人员，从上至下的下拉菜单就是人员间的签核阶层，最上面的下拉菜单就是签核流程的第一阶人员，其下为第二阶人员，依此类推。设置完后，单击【提交】储存配置。

示例：签核流程为 John Smith –> Joy White –> Mary Smith。John Smith 为第一阶人员，Joy White 为第二阶人员，而 Mary Smith 为第三阶人员。下图显示此流程的人员阶层设置。

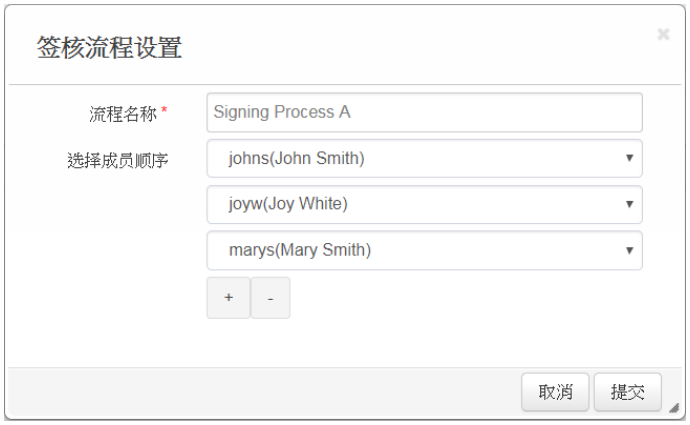


图 11-3 签核流程设置示例

11.2.事件审核

【事件管理】>【事件审核】为您的事件审核箱，其中包含了等待您处理或签核的告警通知，从签核流程的上一阶退回给您重新审核或处理的告警通知，以及由您结案的告警通知。

从【事件管理】>【事件审核】的**事件状态**下拉菜单选择要查看哪一种状态的告警通知。**事件状态**下拉菜单中每种审核状态后面括弧的数字表示您的事件审核箱中有多少笔这种审核状态的告警通知。如果某一事件状态的告警通知太多，您可以使用【搜索】来找出符合特定条件的告警通知。

图 11-4 事件审核列表

点击**内容文档**的【详细数据】将开启新标签页显示相应的告警通知的报表内容，单击**签核记录**的【详细数据】将开启签核记录窗口显示相应的告警通知的整个签核过程与每个过程的处理记录。

表 11-1 事件审核状态说明

事件状态	说明
未处理	签核流程中第一阶人员收到且尚未处理的告警通知的状态。
处理中	对于您正在处理且尚未处理完的告警通知，您可以先将其状态更改为“处理中”。并且在将状态更改为“递交”之前，您可随时进入编辑模式记录处理的过程和结果等信息以及意见。后续将会说明如何进入编辑模式进行记录。
递交	表示为签核流程中前一阶人员（例如，前一章节的签核流程示例中的 John Smith）提交给您审核的告警通知。
退回	表示签核流程中您的后一阶人员（例如，前一章节的签核流程示例中的 Mary Smith）退回给您重新处理的告警通知。
结案	标识由您结案的告警通知。

11.2.1. 签核与签核记录

对于未结案的告警通知，如要进行签核或记录处理过程、审核意见等等，请先从清单中选择该告警通知，然后单击【签核】开启类似下面的签核窗口。

图 11-5 事件签核

您可在**处理记录**里记录任何与该告警通知处理相关的信息，包括处理程序、结果、对于事件的未来防范措施等等。在**事件状态**下拉菜单选择您的签核动作后，单击【提交】。系统会依据**事件状态**下拉菜单的选项和签核流程决定该告警通知接下来该被送给哪一位人员进行处理与签核。

签核窗口上的**事件状态**下拉菜单的可选项，是依据您在签核流程中的阶层位置以及该告警通知的目前状态而决定。其关连如下表所示。

表 11-2 可执行签核操作对照表

您在签核流程中的阶层位置	告警通知目前状态	可执行签核动作
第一阶	未处理 处理中 退回	处理中 递交 结案
中间任一阶	处理中 递交 退回	处理中 递交 退回 结案
最后一阶	处理中 递交	处理中 退回 结案

11.3.事件审核一览表

【事件管理】>【审核一览表】列出已审核结案与待审核的告警通知，以及各告警通知的目前处理状态和负责处理的人员，并可查看每一告警通知的完整签核记录。上级主管通过一览表可以清楚了解有哪些告警通知发生、有哪些告警通知已经放置过久都尚未处理或尚未结案的，以及各告警通知的处理进度与状况。

从【事件管理】>【审核一览表】的**事件状态**下拉菜单选择要查看已结案或未结案的告警通知。并可通过【搜索】来找出符合特定条件的已结案或未结案告警通知。

图 11-6 事件审核一览表

单击**内容文档**的【详细数据】将开启新标签页显示该告警通知的报表内容，单击**签核记录**的【详细数据】将开启签核记录窗口显示该告警通知的整个签核过程与每个过程的处理记录。

12. SQL 安全监控策略

SecuLog 不提供 SQL 活动捕捉策略的设置与变更功能，如使用 SecuLog 网页接口，请忽略此章。

dbAudit 默认为记录所有目标数据库上的所有 SQL 活动，但不记录返回数据。您可以通过【策略管理】>【SQL 安全监控策略】来指定 SQL 的监控（例如：记录哪个数据库用户的 SQL 活动、记录哪个数据表的访问活动、阻断谁对哪个数据表进行的访问活动），以及记录哪些特定格式的返回数据（例如：身分证号、信用卡号）。一旦通过【SQL 安全监控策略】配置了安全监控策略，默认的记录动作就失效了，系统仅会依安全监控策略来记录 SQL 活动或阻断 SQL 活动，不再是记录所有目标数据库上的所有 SQL 活动。

【策略管理】>【SQL 安全监控策略】开启如下的 SQL 安全监控策略的管理页面。该页面列出已配置的监控策略和其捕捉方式（也就是记录方式），以及应用顺序。系统会依照策略应用顺序依序检验捕捉的 SQL 活动与返回数据内容是否符合策略的监控条件。如果捕捉的 SQL 活动与返回数据内容不符合任一监控策略，那么系统将不会保留捕捉的数据或阻断 SQL 活动。如需调整某个策略顺序，请先点选该策略，然后单击【上移】或【下移】以移动该策略在列表上的顺序位置。

另，您可以通过【审计报表】>【SQL 捕获数据】的报表来审计捕捉到的返回数据。

图 12-1 SQL 安全监控策略管理

12.1.SQL 安全监控策略 - 添加/修改/删除

图 12-2 安全监控策略设置

◆ **从空白开始创建新安全监控策略**

单击清单页面（类似图 12-1 所示）的【添加】开启类似图 12-2 的添加页面。策略条件的设置操作与报表的相同，唯一差别在于此页面上的**已选条件**框不提供 AND 和 OR 按钮，相关说明请参阅 8.5.2 条件设置。系统会自动在**已选条件**框中生成 AND 运算框，也就是说，**已选条件**框中的条件间仅可使用 AND 运算符关连。

编辑完后，单击【保存】，并请在**名称**输入安全监控策略名称，在**捕捉方式**设置该策略是用于记录（不记录）符合条件的 SQL 活动，以及是否记录其返回数据，然后单击【提交】完成新策略的创建，并将新策略添加到清单的最后面。

如果在清单页面没有看到新策略，请单击【刷新页面】以重新刷新页面。如需调整新策略的应用顺序，请许先在清单页面选择策略，然后单击【上移】或【下移】以移动该策略在清单上的顺序位置。

表 12-1 **捕捉方式**下拉菜单选项说明

捕捉方式	说明
LOG_ALL	记录符合条件的 SQL 活动与其返回数据。
LOG_SQL	仅记录符合条件的 SQL 活动，不记录其返回数据。
LOG_NONE	符合条件的 SQL 活动与其返回数据都不记录。
LOG_DATA_FILTER	记录符合条件的 SQL 活动，并记录其符合特定格式的返回数据。通过【数据捕捉条件】指定要捕捉的数据格式。

TERMINATE_SESSION	阻断符合条件的 SQL 活动与其相应的会话。依据系统参数 EXCEPTION_LOGGING_POLICY 的设置与【SQL 安全监控策略】中非阻断型策略的捕捉设置来决定是否记录被阻断的 SQL 与其返回数据。有关被阻断 SQL 的 SQL 和返回数据的捕捉，请参阅 12.3 阻断策略的 SQL 与返回数据捕捉。

- **以现有安全监控策略为样板创建新安全监控策略**

先从清单页面(类似图 12-1 所示)选择作为样板的策略后，单击【编辑】开启类似图 12-2 的页面。策略条件的设置操作与报表的相同，唯一差别在于此页面上的**已选条件**框不提供 AND 和 OR 按钮，相关说明请参阅 8.5.2 条件设置。系统会自动在**已选条件**框中生成 AND 运算框，也就是说，**已选条件**框中的条件间仅可使用 AND 运算符关连。

编辑完后，单击【另存为】，并请在**名称**输入策略名称，在**捕捉方式**设置该策略是否捕捉（不捕捉）符合条件的 SQL 活动，以及是否捕捉其返回数据，然后单击【提交】完成新策略的创建，并将新策略加到清单的最后面。如单击【保存】将覆盖样板策略的原配置。有关捕捉方式的选项说明，请参阅表 12-1。

如果在清单页面没有看到新策略，请单击【刷新页面】以重新刷新页面。如需调整新策略的应用顺序，请先在清单页面选择该策略，然后单击【上移】或【下移】以移动该策略在清单上的顺序位置。

- **修改安全监控策略**

先从清单页面（类似图 12-1 所示）选择要修改的策略后，单击【编辑】开启类似图 12-2 的页面。策略条件的设置操作与报表的相同，唯一差别在于此页面上的**已选条件**框不提供 AND 和 OR 按钮，相关说明请参阅 8.5.2 条件设置。系统会自动在**已选条件**框中生成 AND 运算框，也就是说，**已选条件**框中的条件间仅可使用 AND 运算符关连。

编辑完后，单击【保存】以保存变更。如需调整新策略的应用顺序，请在清单页面点选该策略，然后点击【上移】或【下移】以移动该策略在清单上的顺序位置。

- **删除安全监控策略**

先从清单页面（类似图 12-1 所示）选择要删除的策略，然后单击【删除】再单击【确定】。

12.2.数据捕捉条件

单击【数据捕捉条件】开启数据捕捉条件管理页面如下所示。一行是一个捕捉条件，对应一个数据格式。这里设置的数据捕捉条件仅可与捕捉方式为“LOG_DATA_FILTER”的 SQL 安全监控策略一起搭配使用。当该类型策略捕捉到的 SQL 的返回数据的数据格式符合任一数据捕

捉条件时，该返回数据就会被捕捉下来。

图 12-3 数据捕捉条件管理

图 12-4 数据捕捉条件设置

- **添加数据捕捉条件**

单击清单页面的【添加】开启如图 12-4 所示的添加窗口。请在**表达式名称**给予该数据格式正规表示法一个名称（例如：Visa 卡号），在**表达式**放入该数据格式的正规表示法（例如：Visa 卡号的正规表示法为 “/^(4[0-9]{12}(?:[0-9]{3})?)*$/”，符合这样表示法的数据会被视为 Visa 卡号）。完成后，单击【提交】创建新数据捕捉条件。

- **修改数据捕捉条件**

从清单页面选择一个要修改的条件后，单击【编辑】开启类似图 12-4 的窗口。编辑完后，单击【提交】保存变更。

- **删除数据捕捉条件**

先从清单页面选择要删除的条件，然后单击【删除】再单击【确定】。

12.3.阻断策略的 SQL 与返回数据捕捉

如果要设置阻断策略，那么在创建新策略时，须将捕捉方式设为“TERMINATE_SESSION”。有关新策略的设置，请参阅 12.1 SQL 安全监控策略 - 添加/修改/删除的添加部分。

当 dbAudit 系统依据阻断策略阻断 SQL 活动或侦测到含有 SQL 注入攻击的 SQL 活动时，将会比较 EXCEPTION_LOGGING_POLICY 系统参数设置与其他非阻断型 SQL 安全监控策略的捕捉方式，从中选择记录范围涵盖较大的方式来记录 SQL 与返回数据。

示例一：EXCEPTION_LOGGING_POLICY 为 LOG_SQL，而非阻断型 SQL 安全监控策略的捕捉方式之一为 LOG_ALL，那么对于被阻断的 SQL 或含有 SQL 注入攻击的 SQL，dbAudit 将会记录该 SQL 以及其返回的所有数据。

示例二：EXCEPTION_LOGGING_POLICY 为 LOG_SQL，而非阻断型 SQL 安全监控策略的捕捉方式之一为 LOG_DATA_FILTER，那么对于被阻断的 SQL 或含有 SQL 注入攻击的 SQL，dbAudit 将会记录该 SQL 并依据数据捕捉条件记录符合指定格式的返回数据。

EXCEPTION_LOGGING_POLICY 系统参数用于设置被阻断的 SQL 或含有 SQL 注入攻击的 SQL 的 SQL 与返回数据的捕捉方式。有关此参数的说明，请参阅《dbAudit 管理员指南》的系统参数说明。

12.4.场景范例

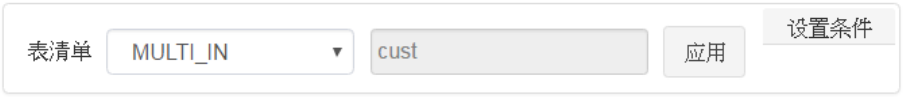
12.4.1. 除特定 SQL 外其余 SQL 皆记录

假设，被监控的目标数据库服务器仅有一台，默认策略是所有 SQL 活动皆记录但不记录返回数据。现在希望仅不记录涉及 cust 表的 SQL，其余 SQL 还是全都记录，但不记录任何返回数据。

1. 单击【添加】先建立不记录访问 cust 表的 SQL 的安全监控策略。

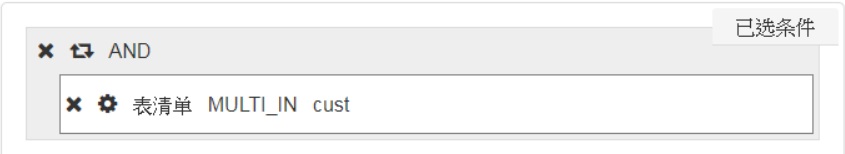
2. 点击【物】>【表清单】。

3. **设置条件**中的运算符下拉菜单选择“MULTI_IN”，并将条件值设置为“cust”。有关运算符与条件值设置的操作说明，请参阅 8.5.2.1 运算符与条件值组件。



由于环境中只有一台被监控目标数据库，所以可以不必设置条件来指定该策略是适用于哪一台数据库服务器。

4. 单击**设置条件**框内的【应用】把条件加入**已选条件**框内后，单击【保存】。



5. 在**名称**输入“cust_excluded”。**捕捉方式**下拉菜单选择“LOG_NONE”，然后单击【提交】创建 SQL 的不记录策略。

6. 单击【添加】来建立记录所有 SQL 的安全监控策略。

7. 不必设置任何条件，直接单击【保存】。

由于环境中只有一台被监控目标数据库，所以可以不必设置条件来指定该策略是适用于哪一台数据库服务器。

8. 在**名称**输入“Capture_All”。**捕捉方式**下拉菜单选择“LOG_SQL”，然后单击【提交】创建记录所有 SQL 但不记录返回数据的策略。

9. 确认清单上“cust_excluded”策略必在“Capture_All”策略之前。在此示例中，这两个策略的顺序很重要，反过来的话，就无法排除访问 cust 表的 SQL 活动。

系统是依策略顺序来检验所捕捉的 SQL 活动符合哪一个安全监控策略，当发现符合的策略时就会停止检验，并依照该策略设置定进行记录或不记录该 SQL 的动作；如果直到最后都没有发现符合的策略，就会丢弃该 SQL 活动。

- “cust_excluded”为第一策略，“Capture_All”为第二策略（正确顺序设置）

  如果捕捉的 SQL 活动没有涉及 cust 表，那么系统在依序检验并发现所捕捉的 SQL 活动与第二策略“Capture_All”的条件相符合后停止检验，并依照该策略设置来记录该 SQL 活动。

  如果捕捉的 SQL 活动涉及 cust 表，那么系统在依序检验并发现所捕捉的 SQL 活动与第一策略“cust_excluded”的条件相符合后停止检验，并依照该策略设置将该 SQL 活动丢弃不记录。

- “Capture_All”为第一策略，“cust_excluded”为第二策略（错误顺序设置）

  如果捕捉的 SQL 活动没有涉及 cust 表，那么系统在依序检验并发现所捕捉的 SQL 活动与第一策略“Capture_All”的条件相符合后停止检验，并依照该策略设置来记录该 SQL 活动。

  如果捕捉的 SQL 活动涉及 cust 表，那么系统在依序检验并发现所捕捉的 SQL 活动与第一策略“Capture_All”的条件相符合后停止检验，并依照该策略设置来记录该 SQL 活动。

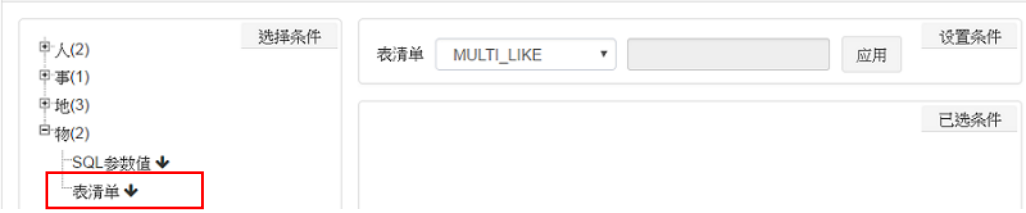
  这样的情况下，第二策略永远也不会检验到，也永远不会满足我们想要的记录需求。

12.4.2. SQL 与数据皆记录，但某一数据库仅记录特定的 SQL

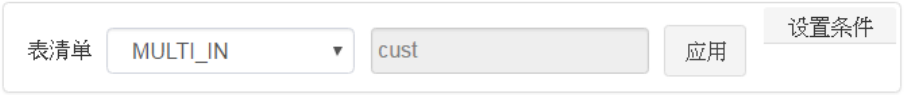
假设，您有 2 台数据库服务器（A 和 B），默认安全监控策略为记录 A 和 B 上的所有 SQL 活动但不记录返回数据。现在您希望依然要记录 B 上的所有 SQL 活动，但仅记录 A 上访问 cust 表的 SQL 活动；同时要记录返回数据中包含 Visa 卡号格式的数据。

1. 单击【添加】先添加 A 服务器的 SQL 安全监控策略。

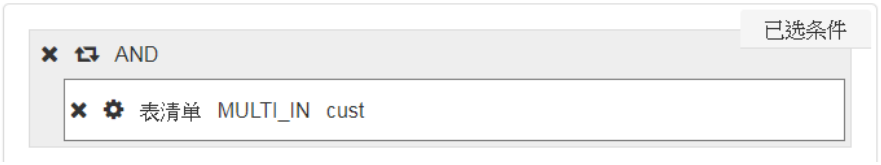
2. 点击【物】>【表清单】。



3. **设置条件**中的运算符下拉菜单选择 “MULTI_IN”，并将条件值设置为 “cust”。有关运算符与条件值设置的操作说明，请参阅 8.5.2.1 运算符与条件值组件。

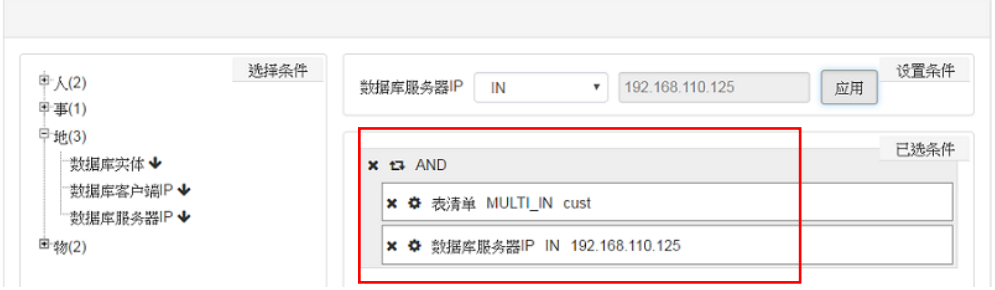


4. 单击**设置条件**框内的【应用】把条件加入**已选条件**框内。



5. 重复步骤 2~4 的操作，把数据库服务器 A 的 IP 条件加入**已选条件**框内，以指定该策略仅适用于特定的数据库服务器。

   点击【物】>【数据库服务器 IP】。在**设置条件**框的运算符下拉菜单选择 “IN”，并将条件值设置为 A 数据库服务器的 IP，例如：192.168.110.125。然后，单击**设置条件**框内的【应用】把条件加入**已选条件**框内。

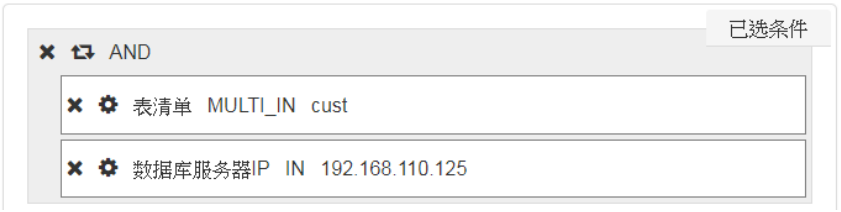


6. 单击【保存】。在**名称**输入“cust_on_A”。**捕捉方式**下拉菜单选择“LOG_DATA_FILTER”，然后单击【提交】创建数据库服务器 A 上的 SQL 安全监控策略。

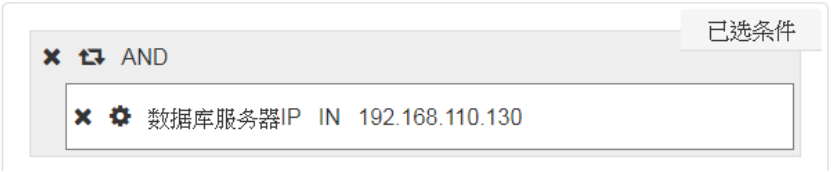
7. 我们使用数据库服务器 A 的安全监控策略来设置数据库服务器 B 的安全监控策略。先从清单上选择“cust_on_A”策略，然后单击【编辑】。

8. 点击“表清单 MULTI_IN cust”条件的 ✖ 图标把该条件移除，并点击“数据库服务器 IP IN 192.168.110.125”条件的 ⚙ 图标修改成数据库服务器 B 的 IP，例如：192.168.110.130，然后单击【应用】。

修改前：



修改后：



9. 单击【另存为】。在**名称**输入“all_on_B”。**捕捉方式**下拉菜单选择“LOG_DATA_FILTER”，然后单击【提交】创建数据库服务器 B 上的 SQL 安全监控策略。

10. 在此示例中，清单上“cust_on_A”与“all_on_B”策略的顺序没有关系，无论哪一个是第一个策略，都可达到我们的记录需求。

系统是依策略顺序来检验 SQL 活动符合哪一个安全监控策略，当发现与某策略条件相符合时就会停止检验，并依照该策略设置执行记录或不记录该 SQL 活动；如果直到最后都没有发现符合的策略，就会丢弃该 SQL 活动。

如果捕捉的 SQL 活动为数据库服务器 A 上的 SQL 活动且涉及 cust 表，那么系统在依序检验并发现所捕捉的 SQL 活动与“cust_on_A”策略的条件相符合后停止检验，并依照该策略设置来记录该 SQL 活动。

如果捕捉的 SQL 活动为数据库服务器 A 上的 SQL 活动且不涉及 cust 表，那么系统在依序检验并发现所捕捉的 SQL 活动与“cust_on_A”和“all_on_B”策略的条件都不符合时就会丢弃该 SQL 活动。

如果捕捉的 SQL 活动为数据库服务器 B 上的 SQL 活动，那么系统在依序检验并发现所捕捉的 SQL 活动与“all_on_B”策略的条件相符合后停止检验，并依照该策略设置来记录该 SQL 活动。

11. 单击清单页面上的【数据捕捉条件】，再单击**数据捕捉条件**页面上的【添加】以添加特定数据格式条件。

于**表达式名称**输入条件名，例如：Visa 卡号。于**表达式**以正规表示法输入数据格式。然后单击【提交】以创建数据的捕捉条件。

针对符合某个策略的 SQL 活动，如果其返回数据内容符合任一**数据捕捉条件**页面上列出的数据格式，该返回数据就会被记录下来。此示例中，只有包含 Visa 卡号格式的返回数据才会被记录下来。

13. 排程清单及运行和发送记录

13.1.报表排程清单

无论是在哪个主题之下的报表，一旦设置了定期排程后，您都可以通过【事件管理】>【排程管理】查看到。换言之,【事件管理】>【排程管理】为定期排程报表的一览表，列出 dbAudit 系统中所有的定期排程报表。

从该清单上，可以一目了然有哪些定期排程报表，以及各报表是属于哪个主题的、目前是否启动排程、下一次的预计运行时间点，和是否为重复发送的报表等信息。

按【刷新页面】可重新刷新页面，以更新定期排程报表列表，以及各报表的排程启动状态、预计运行时间和重复发送状态等信息。

13.2.运行记录

当 dbAudit 运行一个排程报表或一个告警事件检查时，无论在报表指定的数据时间段内或告警指定检查的数据时间段内是否有符合条件的数据，dbAudit 都会生成一笔运行记录。

您可以通过【事件管理】>【事件记录】来查看这些运行记录，并可导出或打印查阅的结果；还可以通过【事件管理】>【事件图表】的图表来查阅运行记录的统计信息。

您可以在【事件管理】>【事件记录】自定义运行记录的查阅报表，在【事件管理】>【事件图表】自定义运行记录的统计图表。【事件管理】>【事件记录】的界面操作与报表的界面操作相同，相关说明请参阅 8 报表。【事件管理】>【事件图表】的界面的操作与审计图表的界面操作相同，相关说明请参阅 7 图表。

13.3.发送记录

无论一个排程报表运行生成的报表结果是否有数据，dbAudit 都会将生成的报表结果发送给指定的接收人员，并生成发送记录。一个发送就会生成一笔发送记录。

然而，一个告警事件在指定检查的数据时间段内，如果没有任何告警事件发生，那么 dbAudit 就不会发送告警通知，也就不会生成发送记录；如果有告警事件发生，那么 dbAudit 将会把告警通知发送给指定的接收人员，并生成发送记录，一个发送就会生成一笔发送记录。

您可以通过【事件管理】>【发送通知记录】来查看这些发送通知记录，并可导出或打印查阅的结果；还可以通过【事件管理】>【发送通知图表】的图表来查阅发送记录的统计信息。

您可以在【事件管理】>【发送通知记录】自定义发送通知的查阅报表，在【事件管理】>

【发送通知图表】自定义发送通知的统计图表。【事件管理】>【发送通知记录】的界面操作与报表的界面操作相同，相关说明请参阅 8 报表。【事件管理】>【发送通知图表】的界面的操作与审计图表的界面操作相同，相关说明请参阅 7 图表。