

对外公开

东软 NetEye 数据库审计系统 用户手册

目 录

| | |
|---------------------|-----|
| 一、 系统桌面 | 4 |
| 二、 系统管理 | 4 |
| 2.1 系统配置模块 | 5 |
| 2.1.1 系统配置 | 5 |
| 2.1.2 硬件和诊断 | 15 |
| 2.1.3 可靠性设置 | 26 |
| 2.1.4 告警通知 | 31 |
| 2.2 备份还原模块 | 37 |
| 2.2.1 备份还原 | 37 |
| 2.2.2 数据清理 | 41 |
| 三、 安全配置 | 44 |
| 3.1 数据库引擎管理 | 44 |
| 3.1.1 添加 | 44 |
| 3.1.2 删除 | 45 |
| 3.1.3 编辑 | 46 |
| 3.1.4 自动发现 | 47 |
| 3.1.5 审计防火墙 | 48 |
| 3.1.6 状态监控 | 52 |
| 3.1.7 风险扫描 | 53 |
| 3.1.8 操作 | 55 |
| 3.2 数据库审计与防火墙 | 57 |
| 3.2.1 审计防火墙 | 57 |
| 3.2.2 策略中心 | 74 |
| 3.2.3 最新流量 | 94 |
| 3.3 设备和敏感数据扫描 | 95 |
| 3.3.1 模块构成 | 96 |
| 3.3.2 服务扫描 | 96 |
| 3.3.3 数据扫描 | 106 |

| | | |
|-----------|----------------------|------------|
| 3.3.4 | 服务发现 | 113 |
| 3.3.5 | 数据发现 | 119 |
| 3.4 | 风险扫描 | 126 |
| 3.4.1 | 添加风险扫描 | 126 |
| 3.4.2 | 引擎列表 | 127 |
| 3.4.3 | 数据库风险扫描 | 127 |
| 3.5 | 数据库状态监控 | 135 |
| 3.5.1 | 添加数据库状态监控 | 135 |
| 3.5.2 | 引擎列表 | 136 |
| 3.5.3 | 概况 | 137 |
| 3.5.4 | 配置 | 147 |
| 3.5.5 | 告警 | 148 |
| 3.5.6 | 记录 | 151 |
| 3.6 | 运维审计 | 152 |
| 3.6.1 | FTP 引擎列表 | 152 |
| 3.6.2 | 规则列表 | 154 |
| 四、 | 检索和报表 | 155 |
| 4.1 | 审计检索（检索） | 155 |
| 4.1.1 | 数据库审计检索 | 156 |
| 4.1.2 | FTP 检索 | 187 |
| 4.2 | 报表 | 189 |
| 4.2.1 | 报告 | 189 |
| 4.2.2 | 报告结果 | 203 |
| 五、 | 其他模块和配置 | 203 |
| 5.1 | 监控 | 203 |
| 5.1.1 | 运行信息 | 203 |
| 5.1.2 | 访问趋势 | 204 |
| 5.1.3 | 引擎列表 | 205 |
| 5.1.4 | 高风险告警列表 | 206 |
| 5.1.5 | 系统告警列表 | 207 |
| 5.2 | 通用配置 | 207 |
| 5.2.1 | SysAdmin 用户管理 | 208 |
| 5.2.2 | Auditor 用户管理 | 211 |

| | | |
|-------|--------------------|-----|
| 5.2.3 | SecAdmin 用户管理..... | 213 |
| 5.3 | 告警 | 214 |
| 5.3.1 | 数据库告警..... | 214 |
| 5.3.2 | FTP 告警..... | 218 |
| 5.4 | 系统审计 | 219 |
| 5.4.1 | 审计防火墙操作日志管理..... | 219 |
| 5.4.2 | 日志..... | 220 |

一、 系统桌面

本系统登录后的桌面布局大致如下图，具体功能模块可能随授权许可的具体情况而有增减变化。

Neusoft



二、 系统管理

系统管理包括 license 授权、时间配置、服务配置、系统监控、系统告警、用户安全设置、数据库授权、升级、接口配置、路由配置、接口功能、关机和重启、BYPASS 设置、双机热备、告警通知、备份还原等。主要操作用户为 SysAdmin。

2.1 系统配置模块

2.1.1 系统配置

在系统配置的首页显示当前的系统版本信息，如下图所示：



2.1.1.1 LICENSE 授权

在 LICENSE 授权页面，可进行授权操作。

用户能够从“当前系统状态”栏中查看到系统是否已经授权，以及具体的授权模块等信息。

| | | |
|-----------|-----------|--|
| 系统配置 | LICENSE授权 | |
| LICENSE授权 | 机器的SN码 | <input type="text" value="03010100101163160024"/> 获取机器信息 |
| 时间配置 | 激活文件 | <input type="text" value="选择文件"/> + 授权激活 |
| 服务配置 | | |
| 系统监控 | 当前系统状态 | |
| 系统告警 | 系统状态： | 已授权！ |
| 用户安全设置 | 系统到期时间： | 2016-08-13 14:57:43 |
| 数据库授权 | 授权模块： | 状态监控，风险扫描，运维审计，设备数据发现，审计防火墙， |
| 升级 | | |

2.1.1.2 时间配置

在时间配置模块，用户可以设置系统时间和 NTP 服务器时间的自动同步。

| | | |
|-----------|---------------------------------------|---|
| 备份还原 | 系统配置 | |
| 系统配置 | 时间配置 | |
| LICENSE授权 | 日期和时间 | |
| 时间配置 | 系统时间 | <input type="text" value="2016-05-17 18:12:15"/> 日历 |
| 服务配置 | 更新系统时间 | <div>注意：修改或同步时间可能导致浏览器当前的页面会话失效，设置后需要重新登录系统。</div> |
| 系统监控 | 时间服务器1 | |
| 系统告警 | IP | <input type="text"/> |
| 用户安全设置 | 端口 | <input type="text" value="123"/> |
| 数据库授权 | 自动同步 | <input type="checkbox"/> |
| 升级 | 保存 同步 | <div>注意：设置“自动同步”后，系统会每天和时间服务器同步一次。</div> |
| 硬件和诊断 | 时间服务器2 | |
| 接口设置 | IP | <input type="text"/> |
| 路由设置 | 端口 | <input type="text" value="123"/> |
| 接口功能 | 自动同步 | <input type="checkbox"/> |
| 关机和重启 | 保存 同步 | <div>注意：设置“自动同步”后，系统会每天和时间服务器同步一次。</div> |
| 可靠性设置 | | |
| BYPASS设置 | | |

当您需要修改系统日期时，请单击时间框的右侧“日历”按钮。此时，将弹出一个微型日历。您可以点击选择年、月、日或点击“今天”按钮选择当前操作系统的时间。然后点击“更新系统时间”按钮，即可实现时间的自定义设置。

时间配置

日期和时间

系统时间

2016-05-17 18:12:15

更新系统时间

时间服务器1

IP

端口

自动同步

保存

同步

注意：设置失败会导致浏览器当前的页面会话失效，设备将重新同步一次。

五月 2016

| | | | | | | |
|----|----|----|----|----|----|----|
| 日 | 一 | 二 | 三 | 四 | 五 | 六 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |

18:12:15

今天 确定 关闭

在时间服务器中，用户可设置 NTP 服务器的 IP 地址及服务端口（默认端口 123）。设置后要点击“保存”按钮进行保存。点击“同步”按钮则会从相应的 NTP 服务器进行时间同步。勾选“自动同步”后，设备将每天定时自动从相应 NTP 服务器进行时间同步。且支持 NTP 主备服务配置。

| | |
|---|----------------------------------|
| 时间服务器1 | |
| IP | <input type="text"/> |
| 端口 | <input type="text" value="123"/> |
| 自动同步 | <input type="checkbox"/> |
| <div><div>保存</div><div>同步</div><div>注意：设置"自动同步"后，系统会每天和时间服务器同步一次。</div></div> | |
| 时间服务器2 | |
| IP | <input type="text"/> |
| 端口 | <input type="text" value="123"/> |
| 自动同步 | <input type="checkbox"/> |
| <div><div>保存</div><div>同步</div><div>注意：设置"自动同步"后，系统会每天和时间服务器同步一次。</div></div> | |

2.1.1.3 服务配置

服务配置包括 DNS 配置，WEB 配置、SSH 配置三个部分。

系统配置

LICENSE授权

时间配置

服务配置

系统监控

系统告警

用户安全设置

数据库授权

升级

硬件和诊断

接口设置

路由设置

接口功能

关机和重启

可靠性设置

BYPASS设置

备份还原

系统配置

系统配置

服务配置

DNS配置

DNS服务器1

DNS服务器2

DNS服务器3

WEB配置

访问权限

完全访问

禁止远程访问

IP白名单访问

所有远程WEB均不可接入服务器，需SSH或主机操作解除。请谨慎选择！

服务端口

443

（1~65535）

SSH配置

访问权限

完全访问

禁止远程访问

IP白名单访问

所有远程SSH均不可接入服务器，需WEB或主机操作解除。请谨慎选择！

服务端口

22

（1~65535）

保存并生效

在 DNS 配置中，可指定三个 DNS 服务器地址，填写后用“保存并生效”按钮保存设置。

DNS配置

DNS服务器1

DNS服务器2

DNS服务器3

在 WEB 配置中，可设置对本系统的 WEB 访问控制。选项包括“完全访问”、“禁止远程访问”、“IP 白名单访问”三个选项。其中“IP 白名单访问”选项需自定义 IP 地址集。如果本系统的 WEB 服务端口被更改，需在服务端口栏将端口修改为被设定的端口值，如下图所示：

| WEB 配置 | |
|--------|---|
| 访问权限 | <div><input type="radio"/> 完全访问</div> <div><input type="radio"/> 禁止远程访问 所有远程WEB均不可接入服务器，需SSH或主机操作解除。请谨慎选择！</div> <div><input checked="" type="radio"/> IP白名单访问</div> |
| 服务端口 | <input type="text" value="443"/> * (1 ~ 65535) |
| IP地址集 | <div><input type="text"/></div> <div>注：IP之间请使用英文逗号 "," 分隔。</div> |

修改配置后需点击“保存并生效”按钮保存配置。

在 SSH 配置中，可设置对本系统的 SSH 远程控制。选项包括“完全访问”、“禁止远程访问”、“IP 白名单访问”三个选项。其中“IP 白名单访问”选项需自定义 IP 地址集。如果本系统的 SSH 服务端口被更改，需在服务端口栏将端口修改为被设定的端口，如下图所示：

| SSH 配置 | |
|--------|---|
| 访问权限 | <div><input type="radio"/> 完全访问</div> <div><input type="radio"/> 禁止远程访问 所有远程SSH均不可接入服务器，需WEB或主机操作解除。请谨慎选择！</div> <div><input checked="" type="radio"/> IP白名单访问</div> |
| 服务端口 | <input type="text" value="22"/> * (1 ~ 65535) |
| IP地址集 | <div><input type="text"/></div> <div>注：IP之间请使用英文逗号 "," 分隔。</div> |

保存并生效

2.1.1.4 系统监控

系统监控页面分为系统资源和网卡运行信息两个部分，包括设备的 CPU、内存、交换分区、磁盘监控曲线图，以及接口信息（MAC 地址、IP 地址、接收和发送数据信息等）。如下图所示：



2.1.1.5 系统告警

系统告警页面可以查看设备运行状态的告警详细信息，包括“发生时间”、“日志类型”、“状态”、“时间级别”、“事件内容”、“处理备注”等。在系统告警页面还可以进行处理告警，和删除告警操作。

| 系统告警 | | | | | | |
|---|-------------------------------------|---------------------|------|-----|------|---------------------|
| <div><input checked="" type="checkbox"/> 处理 <input type="checkbox"/> 告警删除</div> | | | | | | |
| | <input type="checkbox"/> | 发生时间 | 日志类型 | 状态 | 事件级别 | 事件内容 |
| 1 | <input type="checkbox"/> | 2016-05-16 10:43:37 | 应用 | 未处理 | 警告 | 数据库审计防火墙停止完成。。。 |
| 2 | <input type="checkbox"/> | 2016-05-16 10:44:38 | 应用 | 未处理 | 警告 | 数据库审计防火墙启动完成。。。 |
| 3 | <input type="checkbox"/> | 2016-05-16 22:00:00 | CPU | 未处理 | 严重 | 严重：CPU使用量在95%到98%之间 |
| 4 | <input type="checkbox"/> | 2016-05-17 17:46:19 | 应用 | 未处理 | 警告 | 数据库审计防火墙停止完成。。。 |
| 5 | <input type="checkbox"/> | 2016-05-17 17:47:54 | 应用 | 未处理 | 警告 | 数据库审计防火墙启动完成。。。 |
| 6 | <input checked="" type="checkbox"/> | 2016-05-20 21:00:00 | CPU | 未处理 | 警告 | 警告：CPU使用量在90%到95%之间 |

2.1.1.6 用户安全设置

通过用户安全设置页面，用户可进行“登录安全参数”、“密码长度参数”、“密码过期参数”、“下载文件密码”的设置。设置后需点击“保存”按钮进行保存。

| | |
|-----------|--|
| 备份还原 系统配置 | |
| 系统配置 | 用户安全设置 |
| LICENSE授权 | 登录安全参数 60 秒之内，用户尝试登录的失败次数超过 3 次，锁定该用户 1 分钟 |
| 时间配置 | 密码长度参数 密码最短长度 8 密码最长长度 30 |
| 服务配置 | 密码过期参数 状态 <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 |
| 系统监控 | 密码过期时间 30 天（时间只能为正整数且不超过365天） |
| 系统告警 | 下载文件密码 <input type="text"/> 打开 导出或下载的文件时，所需密码；长度6~20字符或不填号； |
| 用户安全设置 | <input type="button" value="保存"/> |
| 数据库授权 | |
| 升级 | |
| 硬件和诊断 | |
| 接口设置 | |
| 路由设置 | |

登录安全参数设置在规定时间内用户输入错误密码的次数，如果超出规定次数，则将该用户锁定一段时间。默认为 1min 内，用户连续 3 次密码输入错误则将该用户锁定 1 分钟。

| | |
|--------|-------------------------------------|
| 用户安全设置 | |
| 登录安全参数 | 60 秒之内，用户尝试登录的失败次数超过 3 次，锁定该用户 1 分钟 |

通过密码长度参数可设定密码的长度范围。

| | |
|--------|--------------------|
| 密码长度参数 | 密码最短长度 1 密码最长长度 21 |
|--------|--------------------|

密码过期参数的设置可控制密码的有效期。

密码过期参数

状态

☐ 启用 ☒ 禁用

密码过期时间 天（时间只能为正整数,且不超过365天）

设置下载文件密码后，下载报告等文件后解压相应压缩包时需输入密码。

下载文件密码

打开 导出或下载的文件时，所需密码；长度6~20字符或不填写；

2.1.1.7 数据库授权

系统以具备一定权限的远端用户账号访问数据库，读取数据库相应信息，来支持状态监控和风险扫描功能。数据库授权页面提供 ORACLE、SQLSERVER 等数据库的授权脚本下载，供数据库 DBA 创建一定权限的数据库用户，开放给数据库审计产品，用于数据库状态监控和风险扫描。

备份还原 系统配置

系统配置

LICENSE授权

时间配置

服务配置

系统监控

系统告警

用户安全设置

数据库授权

升级

硬件和诊断

请下载所需数据库类型授权

| 数据库类型 | 描述 |
|-----------|-----------------|
| ORACLE | 状态监控支持。 |
| SQLSERVER | 状态监控支持。 |
| MYSQL | 状态监控支持，风险扫描不支持。 |
| SYBASE | 状态监控支持，风险扫描不支持。 |
| INFORMIX | 状态监控支持，风险扫描不支持。 |
| DAMENG7 | 状态监控支持，风险扫描不支持。 |

点击相应数据库类型下载SQL脚本；

下载的SQL脚本，由数据库DBA管理员执行，并创建有限用户，本系统相应模块使用该用户；

请详看脚本说明。

如下图所示：

```
-- please replace all the username and password to yours.

create user c##username identified by password;
grant connect to c##username;

-- dbmon
grant select on v_$instance to c##username;
grant select on v_$database to c##username;
grant select on dba_data_files to c##username;
grant select on v_$session to c##username;
grant select on v_$sqlarea to c##username;
grant select on v_$filestat to c##username;
grant select on v_$parameter to c##username;
grant select on dual to c##username;
grant select on sys.dba_registry to c##username;
grant select on dba_sys_privs to c##username;
grant select on v_$sga to c##username;
grant select on v_$sgastat to c##username;
grant select on v_$sysstat to c##username;
grant select on v_$rowcache to c##username;
grant select on v_$librarycache to c##username;
grant select on sys.dba_temp_files to c##username;
grant select on sys.dba_tablespace to c##username;
grant select on sys.dba_free_space to c##username;
grant select on v_$log to c##username;
grant select on v_$logfile to c##username;
grant select on v_$sesstat to c##username;
grant select on v_$session_wait to c##username;
grant select on sys.dba_rollback_segs to c##username;
grant select on dba_blockers to c##username;
grant select on dba_waiters to c##username;
grant select on v_$statname to c##username;
grant select on sys.dba_segments to c##username;
grant select on v_$filestat to c##username;
grant select on v_$datafile to c##username;
grant select on v_$rollstat to c##username;
grant select on v_$sql to c##username;

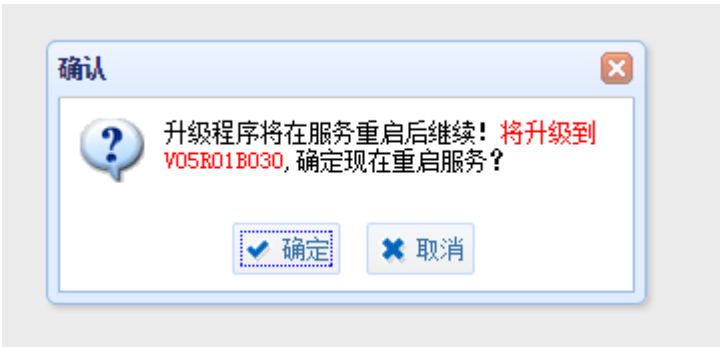
-- scan
grant select on sys.user$ to c##username;
grant select on t_bus_pswconf_code_user to c##username;
grant select on sys.link$ to c##username;
grant select on v_$session to c##username;
grant select on dba_role_privs to c##username;
grant select on dba_profiles to c##username;
grant select on dba_audit_session to c##username;
grant select on dba_users to c##username;
grant select on v_$parameter to c##username;
grant select on dba_roles to c##username;
grant select on dba_tab_privs to c##username;
grant select on dba_tables to c##username;
grant select on v_$license to c##username;
grant select on dba_indexes to c##username;
```

2.1.1.8 升级

通过升级页面，用户可升级系统补丁包。

点击“手动导入升级文件”弹出导入升级文件的窗口，点击“+”按钮，选择升级文件路径，点击“上传”。点击“升级”。弹出确认窗口，点击“确定”，系统进入升级状态。

在升级页面，用户可以查看到升级记录，包括：时间、概要和详细描述。



2.1.2 硬件和诊断

2.1.2.1 接口设置

通过接口设置页面能够查看到接口状态，包括接口名、接口地址、启用状态等信息，如下图所示：

| 设备接口状态 | | | |
|--------|------|-------------------|------|
| 刷新 | | | |
| | 接口名 | 接口地址 | 启用状态 |
| 1 | enp0 | 44:8a:5b:f4:5f:63 | 连接 |
| 2 | enp1 | d8:cb:8a:ab:d0:0a | 连接 |
| 3 | enp2 | d8:cb:8a:ab:d0:0b | 断开 |
| 4 | enp3 | d8:cb:8a:ab:d0:0c | 连接 |
| 5 | enp4 | d8:cb:8a:ab:d0:0d | 连接 |
| 6 | enp5 | 44:8a:5b:3e:cd:46 | 断开 |
| 7 | enp6 | 44:8a:5b:3e:cd:47 | 断开 |
| 8 | enp7 | 44:8a:5b:3e:cd:48 | 断开 |

旁路审计设置

在旁路审计设置中能够添加、删除和编辑旁路审计接口。如下图所示：

| 旁路审计设置 | | | |
|----------------|------|------|----|
| + 添加 删除 编辑 | | | |
| | 接口名 | IP地址 | 掩码 |
| 1 | enp1 | | |

添加审计接口

点“添加”按钮，弹出旁路审计端口设置窗口，选择相应的接口，依次填写 IP 地址，掩码，网关。点击“确定”按钮进行保存。

旁路审计端口设置

接口名

IP地址

掩码

网关

enp2

enp3

enp4

enp5

enp6

enp7

enp8

该输入项为必填

多个IP地址写,如2个IP : 192.168.1.200/192.168.1.201

确定

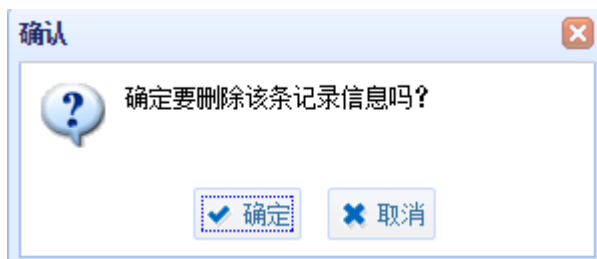
取消

提示：

- 1、IP 地址、掩码、网关为可选填写。
- 2、在完成上述步骤后需要点击右侧“保存”按钮，否则所做配置不生效。

删除审计接口

选中相应的审计接口，点击“删除”按钮，弹出确认窗口，单击“确定”即可成功删除相应审计接口。



提示：在完成上述步骤后需要点击右侧“保存”按钮，否则删除不生效。

编辑审计接口

通过编辑审计接口页面，可以通过接口名更改审计接口；并且可以更改 IP 地址、掩码、网关。选中相应的审计接口，点击“编辑”按钮，弹出旁路审计端口设置窗口，编辑相应信息，单击“确定”。

旁路审计端口设置

| | |
|------|---------------|
| 接口名 | enp2 |
| IP地址 | 192.168.60.6 |
| 掩码 | 255.255.255.0 |
| 网关 | 192.168.60.2 |

多个IP地址和掩码填写时使用"/"分割,且IP和掩码必须成对填写,如2个IP : 192.168.1.200/192.168.1.201

确定

取消

提示：在完成上述步骤后需要点击右侧“保存”按钮，否则编辑的配置不生效。

网桥接口设置

防火墙串联部署时需设置网桥接口，通过网桥接口设置页面，能够查看到已添加的网桥信息，可以进行添加删除等操作。如下图所示：

| | | | | | | |
|-------------------------|--------|--------|--|------|----|-----------|
| 旁路审计设置 | 网桥接口设置 | 其他设置 | | | | 保存 |
| 网桥接口列表 | | | | | | |
| + 添加网桥 删除网桥 + 添加接口 删除接口 | | | | | | |
| 网桥组编号 | | 网桥IP地址 | | 子网掩码 | 接口 | VLAN 透传状态 |

添加网桥

点击“添加网桥”按钮，弹出添加窗口，输入编号、IP 地址、子网掩码，点击“确定”按钮。

网桥组添加

网桥组编号

1

(1~255)

网桥IP地址

192.168.50.5

子网掩码

255.255.255.0

确定

添加接口和 Vlan 透传

选中相应网桥，点击“添加接口”按钮，弹出网桥组接口设置窗口。点击接口栏的下拉三角按钮，选中相应接口；

网桥组接口设置

网桥组编号

br1

接口

enp3,enp4

VLAN ID透传

enp2

enp3

enp4

enp5

enp6

enp7

enp8

确定

勾选 VLAN ID 透传的“开启”选项，输入 VLAN 编号，点击“确定”按钮。

| | |
|-----------|--|
| 网桥组编号 | br1 |
| 接口 | enp4,enp3 |
| VLAN ID透传 | <input checked="" type="checkbox"/> 开启 50 |

💡 接口与VLAN ID透传为完全匹配：
如：接口为A，B，VLAN ID透传为100，则最终设置为A.100，B.100。

✓ 确定

提示：在完成上述步骤后需要点击右侧“保存”按钮，否则编辑的配置不生效。

删除接口

选中相应网桥，点击“删除接口”按钮，弹出提示窗口。点击“确定”

提示

确定要删除该网桥的接口信息吗?

✓ 确定 ✕ 取消

删除网桥

选中相应网桥，点击“删除网桥”按钮，弹出提示窗口。点击“确定”

提示

确定要删除该网桥信息吗?

✓ 确定 ✕ 取消

提示：

- 1、在完成上述步骤后需要点击右侧“保存”按钮，否则删除不生效。
- 2、删除网桥前需先删除接口，否则无法删除网桥。

其他设置

通过其他设置页面，可以设置管理接口和 HA 接口。

| | | | |
|-----------------------------------|--------------------------|------|---------------|
| 旁路审计设置 | 网桥接口设置 | 其他设置 | 保存 |
| 管理口配置 | | | |
| 接口 | enp0 端口不可更改 | | |
| IP地址 | 172.16.1.128 | 子网掩码 | 255.255.255.0 |
| HA口配置 <input type="checkbox"/> 启用 | | | |
| 接口 | | | |
| IP地址 | | 子网掩码 | |

管理口配置

通过管理口配置项目，可配置管理口的 IP 地址。

| | | | |
|-------|--------------------------|------|---------------|
| 管理口配置 | | | |
| 接口 | enp0 端口不可更改 | | |
| IP地址 | 172.16.1.128 | 子网掩码 | 255.255.255.0 |

提示：在完成上述步骤后需要点击右侧“保存”按钮，否则编辑的配置不生效。

HA 口配置

为确保设备的高可用性，系统提供双机热备的功能，正常情况下主机服务运行，备机通过心跳线监视主机的状态，主机出现问题时，切换到备机上运行，保证审计和防火墙模式能够正常运行。双机热备需要在主机和从机上都配置 HA 口。

设置 HA 接口：（主机地址和备机地址需是同一网段（如：主机 192.168.100.100，备机 192.168.100.101）

旁路审计设置

网桥接口设置

其他设置

保存

管理口配置

接口

enp0

端口不可更改

IP地址

172.16.1.77

子网掩码

255.255.255.0

HA口配置

启用

接口

enp1

IP地址

192.168.100.100

子网掩码

255.255.255.0

提示：个别机型平台 HA 口（如 H61 机型没有单独的 HA 口）可以通过去使用，释放作为业务接口使用。

2.1.2.2 路由设置

系统路由表

通过系统路由表页面，能够查看到路由信息。如下图所示：

系统路由表

静态路由表

刷新

| | 目的IP地址 | 子网掩码 | 网关 | 优先级 | 接口 |
|----|------------|---------------|---------|------|------|
| 1 | link-local | 255.255.0.0 | 0.0.0.0 | 1002 | enp5 |
| 2 | link-local | 255.255.0.0 | 0.0.0.0 | 1003 | enp6 |
| 3 | link-local | 255.255.0.0 | 0.0.0.0 | 1004 | enp7 |
| 4 | link-local | 255.255.0.0 | 0.0.0.0 | 1005 | enp8 |
| 5 | link-local | 255.255.0.0 | 0.0.0.0 | 1006 | enp0 |
| 6 | link-local | 255.255.0.0 | 0.0.0.0 | 1007 | enp1 |
| 7 | link-local | 255.255.0.0 | 0.0.0.0 | 1008 | enp2 |
| 8 | link-local | 255.255.0.0 | 0.0.0.0 | 1009 | enp3 |
| 9 | link-local | 255.255.0.0 | 0.0.0.0 | 1010 | enp4 |
| 10 | 172.16.1.0 | 255.255.255.0 | 0.0.0.0 | 0 | enp0 |

静态路由表

在静态路由表页面，可以添加、删除和查看静态路由。

| | | | | |
|--|--------------|---------------|--------------|-----|
| <div><div><div><div></div></div><div>添加</div></div><div><div></div><div>删除</div></div></div> | | | | |
| | 目的IP地址 | 子网掩码 | 网关 | 优先级 |
| 1 | 172.17.200.0 | 255.255.255.0 | 192.168.50.1 | 60 |

添加

点击“添加”按钮，弹出路由添加窗口，输入目的 IP 地址、子网掩码、网关、优先级后点击“确定”即可成功添加路由。

路由添加

目的IP地址

172.17.200.0

子网掩码

255.255.255.0

网关

192.168.50.1

优先级

60

(1~255)

确定

删除

选中已添加的路由条目，点击“删除”按钮，弹出提示窗口，点击“确定”即可成功删除路由。

提示

?

确定要删除该路由信息吗？

确定

取消

2.1.2.3 接口功能

通过接口功能页面，可以设置接口模块审计功能。

| 接口功能 | |
|--------|---|
| 保存并生效 | |
| 接口名 | 开启的功能 (双击此列的单元格可编辑) |
| 1 enp1 | Web审计, Ftp审计, Telnet审计, Vnc审计, Ssh审计, Sntp审计, Pop3审计, Imap审计, 旁路阻断, 数据库审计 |
| 2 enp2 | Web审计, Ftp审计, Telnet审计, Vnc审计, Ssh审计, Sntp审计, Pop3审计, Imap审计, 旁路阻断, 数据库审计 |
| 3 enp5 | |
| 4 enp6 | |
| 5 enp7 | |
| 6 enp8 | |

示例：开启 enp5 接口的数据库审计功能。

双击 enp5 接口右侧的选框，点击下拉三角，选中添加模块审计项。点击“保存并生效”按钮。

| 接口功能 | |
|--------|---|
| 保存并生效 | |
| 接口名 | 开启的功能 (双击此列的单元格可编辑) |
| 1 enp1 | 数据库审计, 旁路阻断, Imap审计, Pop3审计, Sntp审计, Ssh审计, Vnc审计, Telnet审计, Ftp审计, Web审计 |
| 2 enp2 | 数据库审计, 旁路阻断, Imap审计, Pop3审计, Sntp审计, Ssh审计, Vnc审计, Telnet审计, Ftp审计, Web审计 |
| 3 enp5 | 数据库审计 |
| 4 enp6 | 数据库审计 |
| 5 enp7 | 旁路阻断 |
| 6 enp8 | Imap审计 |
| | Pop3审计 |
| | Sntp审计 |
| | Ssh审计 |
| | Vnc审计 |
| | Telnet审计 |
| | Ftp审计 |
| | Web审计 |

示例：取消 enp5 接口的数据库审计功能。

双击 enp5 接口右侧的选框，点击下拉三角，将已选中数据库审计选项点掉。点击“保存并生效”按钮。

| 接口功能 | |
|--------|---|
| 保存并生效 | |
| 接口名 | 开启的功能 (双击此列的单元格可编辑) |
| 1 enp1 | Web审计, Ftp审计, Telnet审计, Vnc审计, Ssh审计, Sntp审计, Pop3审计, Imap审计, 旁路阻断, 数据库审计 |
| 2 enp2 | Web审计, Ftp审计, Telnet审计, Vnc审计, Ssh审计, Sntp审计, Pop3审计, Imap审计, 旁路阻断, 数据库审计 |
| 3 enp5 | |
| 4 enp6 | 数据库审计 |
| 5 enp7 | 旁路阻断 |
| 6 enp8 | Imap审计 |
| | Pop3审计 |
| | Sntp审计 |
| | Ssh审计 |
| | Vnc审计 |
| | Telnet审计 |
| | Ftp审计 |
| | Web审计 |

2.1.2.4 关机和重启

通过关机和重启页面，可对设备进行关机和重启操作。

关机和重启

当按下此按钮，系统服务器将立即重启。

当按下此按钮，系统服务器将立即关机。

点击“重启”按钮，弹出确认窗口，点击“确定”

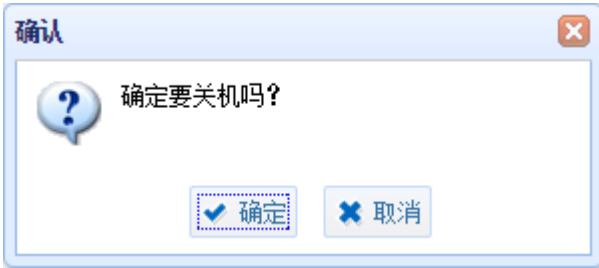
确认

确定要重启吗？

✓ 确定

✗ 取消

点击“关机”按钮，弹出确认窗口，点击“确定”



2.1.3 可靠性设置

2.1.3.1 BYPASS

BYPASS 保障当设备意外宕机等情形下，作为防火墙串口部署方式不会影响客户端与数据库的连通性，保障业务能够正常进行。通过 BYPASS 设置页面可手动控制 BYPASS 的启用与停用。



示例：启用 BYPASS

点击“启用”按钮，弹出提示窗口，点击“确定”。相应接口进入 BYPASS 状态，此时设备不再对相应接口的数据进行审计也不能够实现阻断等功能。



示例：停止 BYPASS

点击“停止”按钮，弹出提示窗口，点击“确定”。相应接口退出 BYPASS 状态，此时设备恢复对相应接口的数据进行审计，能够实现阻断等功能。



2.1.3.2 双机热备

为确保设备的高可用性，系统提供双机热备的功能，正常情况下主机上服务运行，备机通过心跳线监视主机的状态，主机出现问题时，切换到备机上运行，确保数据库防火墙功能正常运行，同时保障了用户生产环境下的高可用性。

示例：防火墙模式开启双机热备

1) 设置 HA 接口：(主机地址和备机地址需同一网段（如：主机 192.168.100.100，备机 192.168.100.101）

旁路审计设置

网桥接口设置

其他设置

保存

管理口配置

接口

enp0

端口不可更改

IP地址

172.16.1.77

子网掩码

255.255.255.0

HA口配置

启用

接口

enp1

IP地址

192.168.100.100

子网掩码

255.255.255.0

2) 添加网桥（主机和备机都要操作，备机不能自动学习）

旁路审计设置

网桥接口设置

其他设置

保存

网桥接口列表

+ 添加网桥

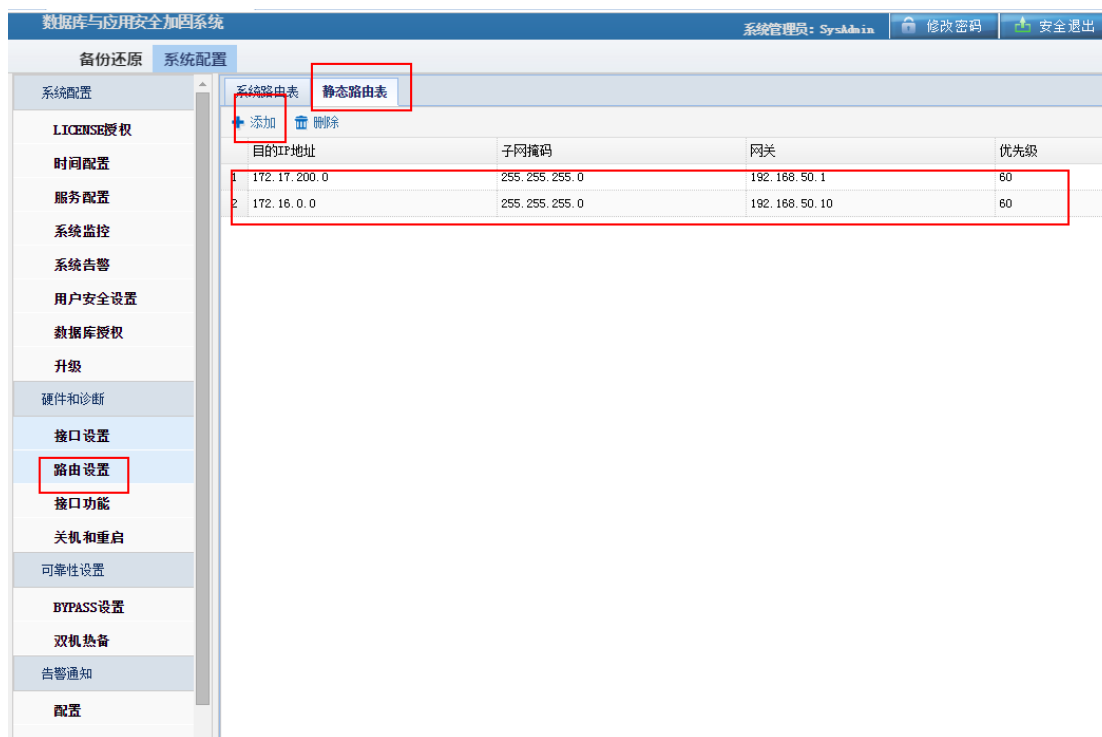
删除网桥

+ 添加接口

删除接口

| 网桥组编号 | 网桥IP地址 | 子网掩码 | 接口 | VLAN | 透传状态 |
|-------|--------|--------------|---------------|------------|------|
| 1 | br1 | 192.168.50.5 | 255.255.255.0 | enp2, enp3 | 未开启 |

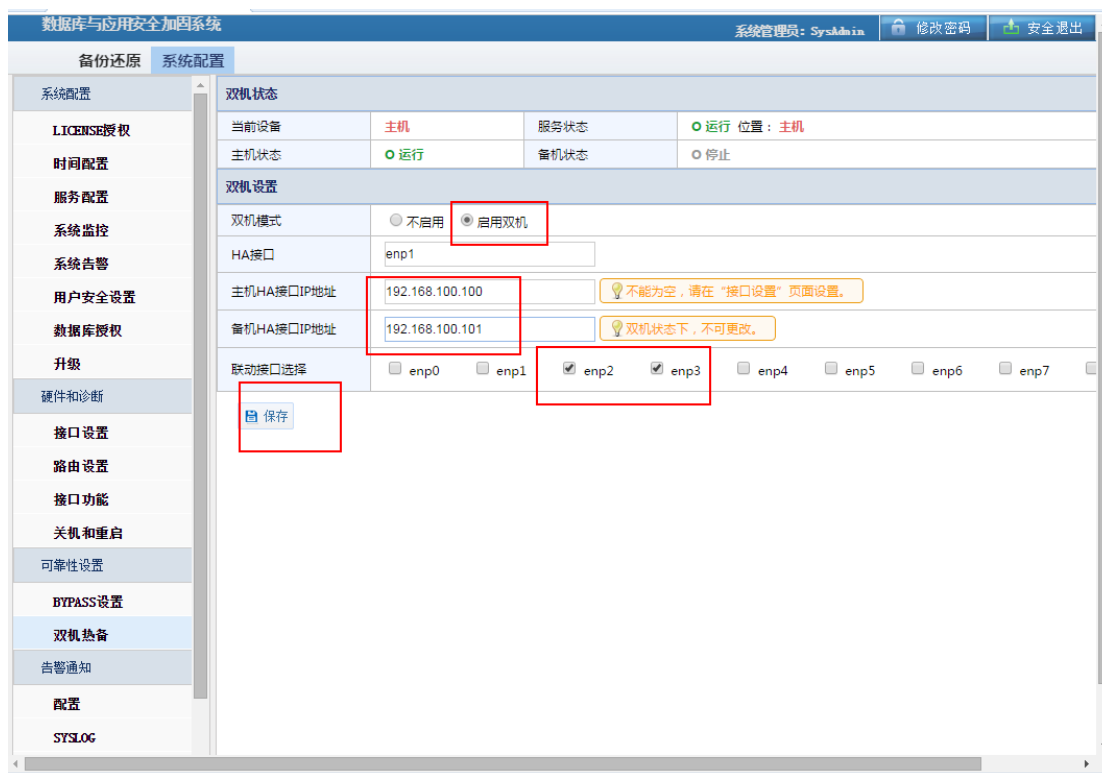
3) 添加路由（只在主机上配置即可）



4) 添加并开启数据库引擎（只在主机上配置即可）



5) 开启双机热备（只在主机上操作即可,需要勾选网桥端口）



备注：

- 1) 备机能够自动学习数据库引擎等设置（开启双机热备后就学习，并非在主机掉线后学习）；
- 2) 备机不能自动学习网桥，需要在主机和备机上都做设置，如果备机没有设置网桥，会影响到备机对加固点的学习；
- 3) 主机重新上线后，服务会自动切回主机上运行。

2.1.4 告警通知

2.1.4.1 配置

在告警配置页面可查看已添加的告警条目，并对告警条目进行添加、删除和重新加载等操作。

| 告警配置 | | | |
|------------------|-------|------------------------------|----------------------------|
| + 添加 删除 重新加载 | | | |
| 告警级别 | 通知类型 | 类型详情 | 引擎 |
| 1 中风险 | EMAIL | admin_user1@datafort.cn (启用) | 172.17.200.190:60000/test1 |

添加

点击“添加”按钮，弹出新增告警的窗口。通过点击下拉三角符号，选择告警级别、通知类型、类型详情、引擎等选项，点击“确定”按钮，实现添加告警。

新增告警

告警级别

中风险

通知类型

EMAIL

类型详情

admin_user1@datafort.cn (启用)

引擎

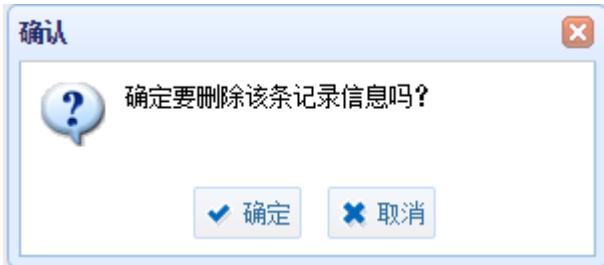
172.17.200.190:60000/test1

确定

取消

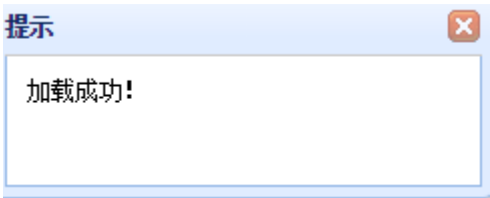
删除

选中相应告警条目。点击“删除”按钮，弹出确认窗口，点击“确定”，即可删除相应告警条目。



重新加载

点击“重新加载”按钮，对告警条目重新加载。



2.1.4.2 SYSLOG

通过 SYSLOG 页面可以查看到已添加的 SYSLOG 条目，实现 SYSLOG 条目的添加、编辑、和删除操作。

| SYSLOG ? | | | | |
|----------------|----------------|-----|-------|----|
| + 添加 编辑 删除 | | | | |
| | IP | 端口 | 发送者标识 | 状态 |
| 1 | 172.17.200.103 | 514 | test | 启用 |

添加与编辑

点击“添加”按钮，弹出新增窗口。输入 IP 、端口、发送标识等参数，选择启用或禁用，点击“确定”按钮，实现添加。“测试”按钮，能够测试是否成功。



新增

| | |
|------|--|
| IP | 172.16.1.127 * |
| 端口 | 514 * (1 ~ 65535) |
| 发送标识 | test * |
| 是否启用 | <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 |

💡 SYSLOG特性，同一网段内均可发送成功。请准确配置！

测试 确定 取消

点击“编辑”按钮，能够对上述添加中设置的参数进行修改。



编辑

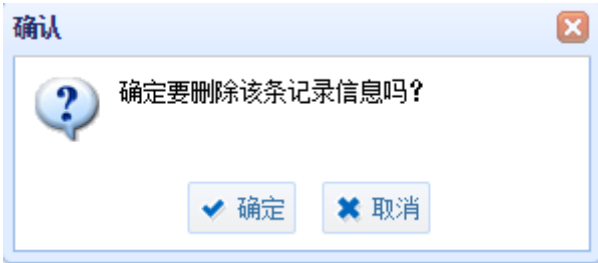
| | |
|------|--|
| IP | 172.16.1.127 * |
| 端口 | 514 * (1 ~ 65535) |
| 发送标识 | test * |
| 是否启用 | <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 |

💡 SYSLOG特性，同一网段内均可发送成功。请准确配置！

测试 确定 取消

删除

點選已添加的条目，点击“删除”按钮，弹出确认窗口，点击“确定”实现删除。



2.1.4.3 邮件

通过邮件页面。可配置邮件服务器地址，发件人等信息。在收件人条目中输入接收告警信息的管理员的邮件地址；邮件主机条目中输入邮件服务器的 IP 地址；发件人和密码条目中输入发送邮件账户的相关信息；SMTP 是否验证选择启用或禁用；发送设置中可设置单封邮件中包含的条数。配置参数后，点击“保存”按钮，保存相关配置。可通过“测试”按钮测试是否成功。

邮件服务器配置 ?

邮件服务器配置

| | |
|----------|--|
| 收件人 | <input type="text" value="admin_user1@datafort.cn"/> * |
| 邮件主机 | <input type="text" value="172.17.200.103"/> * |
| 发件人 | <input type="text" value="root"/> * |
| 密码 | <input type="password" value="....."/> * |
| SMTP是否验证 | <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 |

发送设置

| | |
|--------|--|
| 单封邮件包含 | <input type="text" value="10"/> 条* (1 ~ 500) |
|--------|--|

保存

测试

2.1.4.4 FTP

通过 FTP 页面，可配置 FTP 服务器地址，上传用户等信息。在状态条目中选择启用或禁用；在 IP 地址条目中输入接收告警信息的 FTP 服务器的 IP 地址,并配置相应的端口信息；用户名和密码条目中输入上传用户的相关信息；上传目录条目中设置上传到 FTP 服务器的目录；发送设置中可设置单次包含的条数。配置参数后，点击“保存”按钮，保存相关配置。可通过“测试”按钮测试是否成功。

FTP服务器配置 ?

FTP服务器配置

| | |
|------|--|
| 状态 | <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 |
| IP地址 | <input type="text" value="172.17.200.194"/> * 端口 <input type="text" value="21"/> * (1 ~ 65535) |
| 用户名 | <input type="text" value="user1"/> * |
| 密码 | <input type="password" value="*****"/> * |
| 上传目录 | <input type="text" value="/pub"/> * |

发送设置

| | |
|------|--|
| 单次包含 | <input type="text" value="10"/> 条* (1 ~ 500) |
|------|--|

保存

测试

2.1.4.5 SNMP

通过 SNMP 页面，设置 SNMP 服务器地址等信息。在状态条目中选择启用或禁用；在 IP 地址条目中输入 SNMP 服务器的 IP 地址,并配置相应的端口信息；OID 和 MIB 中输入相

关信息（默认 OID 条目为 public）；发送设置中可设置发送类型为“发送统计信息”或“发送单条”。配置参数后，点击“保存”按钮，保存相关配置。可通过“测试”按钮测试是否成功。

SNMP服务器配置 ?

SNMP服务器配置

| | |
|---------|--|
| 状态 | <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 |
| 服务器IP地址 | <input type="text"/> * 端口 <input type="text" value="162"/> * (1 ~ 65535) |
| OID | <input type="text" value="public"/> * |
| MIB | <input type="text" value=".1.1.1.1.1.1.1.1.1"/> * 样例：.1.1.1.1.1.1.1.1.1 (1可替换数字) |

发送设置

| | |
|------|--|
| 发送类型 | <input type="radio"/> 发送统计信息 <input checked="" type="radio"/> 发送单条 |
|------|--|

💡 SNMP特性，同一网络内均可发送成功。请准确配置！

保存

测试

2.1.4.6 短信

通过短信页面，配置短信服务器地址等信息。在状态条目中选择启用或禁用；在 IP 地址条目中输入服务器的 IP 地址,并配置相应的端口信息；发送设置中可设置单次包含的条数及发送格式。配置参数后，点击“保存”按钮，保存相关配置。可通过“测试”按钮测试是否成功。

短信接口配置 ?

短信接口配置

状态

启用

禁用

服务器IP地址

* 端口18259 * (1 ~ 65535)

发送设置

单次包含

10

条* (1 ~ 500)

发送格式

13811112222#

格式：目标手机号#信息内容；支持单一手机发送！

保存

测试

2.2 备份还原模块

2.2.1 备份还原

备份还原 系统配置

备份还原

自动备份

手动备份

FTP备份

备份还原

数据清理

备份文件清理

自动清理

恢复出厂设置

自动备份

是否开启自动备份

是

否

在每天的

1

(0~23)点进行备份，存放位置: backup

保存

备份文件列表

| 备份文件名 | 备份时间 | 备份耗时 (s) | 数据结束时间 | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 |
|-------|------|----------|--------|--------|------|------|--------|
|-------|------|----------|--------|--------|------|------|--------|

2.2.1.1 自动备份

通过自动备份页面可设置是否开启自动备份功能，以及自动备份的时间和存放位置。在备份文件列表中可以看到自动备份所生成的备份文件。

自动备份

是否开启自动备份

☐ 是

☒ 否

在每天的

(0~23)点进行备份，存放位置:

保存

备份文件列表

| 备份文件名 | 备份时间 | 备份耗时(s) | 数据结束时间 | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 |
|-------|------|---------|--------|--------|------|------|--------|
|-------|------|---------|--------|--------|------|------|--------|

2.2.1.2 手动备份

通过手动备份页面可进行手动备份，在备份文件列表中可以看到所生成的备份文件。包括备份文件名、备份时间、备份耗时、数据结束时间、备份文件大小、备份方式、最后一次恢复等信息

手动备份

备份

备份文件列表

| 备份文件名 | 备份时间 | 备份耗时(s) | 数据结束时间 | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 |
|----------------------------------|---------------------|----------|---------------------|-------------|------|------|--------|
| manuBackup_20160517135011_9650.t | 2016-05-17 13:50:11 | 1054.818 | 2016-05-17 13:50:11 | 5286.571718 | 手动备份 | 未上传 | |

2.2.1.3 FTP 备份

在 FTP 备份页面中，可设置是否开启 FTP 备份，设置备份文件上传时间等，如下图：

FTP配置

状态

启用

禁用

自动上传

在每天的 1 (0~23) 点，自动上传 2 (1~365)天以前的备份文件。

FTP服务器IP

FTP服务器端口

21

登录FTP的用户名

需要具有创建和删除文件和文件夹的权限的用户

登录FTP的密码

上传文件存放在FTP上的目录

(为空即FTP服务器跟路径)

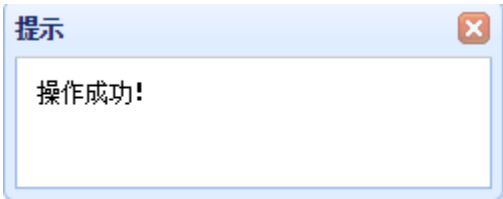
保存

测试

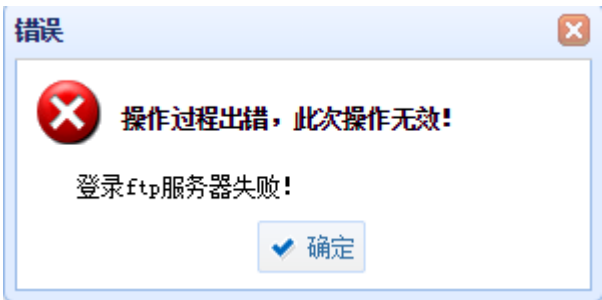
备份文件列表

| 备份文件名 | 备份时间 | 备份耗时 (数据结束时间 | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 | 操作 |
|------------------------------|---------------------|---------------|---------------------|-------------|------|--------|---------------|
| manuBackup_20160517135011_96 | 2016-05-17 13:50:11 | 1054.818 | 2016-05-17 13:50:11 | 5286.571716 | 手动备份 | 未上传 | <div>上传</div> |

- 状态：选择启用和禁用。
- 自动上传：设置每天上传的时间，及上传的内容。
- FTP 服务器 IP：设置备份文件所上传存放的 FTP 服务器的 IP 地址。
- FTP 服务器端口：FTP 服务器所开启的 FTP 服务的端口，默认为 21。
- 登录 FTP 的用户名：登录 FTP 服务器所用的用户名，该用户需要具有创建和删除文件及文件夹的权限。
- 登录 FTP 的密码：登录 FTP 服务器的用户所对应的密码。
- 上传文件存在在 FTP 上的目录：文件在 FTP 服务器上的存放位置。
- “保存” 和 “测试” 按钮
- 通过 “保存” 按钮保存以上配置。通过 “测试” 按钮测试是否能够成功登录 FTP 服务器。
- 成功则在右下角弹出成功提示窗口



失败则在屏幕中央提示错误。



备份文件列表

在备份文件列表中可以查看到所生成的备份文件。包括备份文件名、备份时间、备份耗时、数据结束时间、备份文件大小、备份方式、最后一次恢复等信息。并且通过操作栏的“上传”按钮可将相应的备份文件上传至相应的 FTP 服务器。

| 备份文件列表 | | | | | | | |
|------------------------------|---------------------|----------|---------------------|-------------|------|------|--------|
| 备份文件名 | 备份时间 | 备份耗时 | 数据结束时间 | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 |
| manuBackup_20160517135011_96 | 2016-05-17 13:50:11 | 1054.818 | 2016-05-17 13:50:11 | 5286.571718 | 手动备份 | 未上传 | |

2.2.1.4 备份还原

通过备份还原页面，可进备份查询，可以“备份方式”、“备份日期”、“备份文件存放的目录”三个条件进行筛选查询，筛选后符合条件的备份文件将会显示在备份文件列表中。通过备份文件所对应的“还原”按钮进行还原。

备份查询

备份方式

自动备份

手动备份

备份日期

备份文件存放的目录

backup

查询

重置

备份文件列表

| 备份文件名 | 备份时间 | 备份耗时 (数据结束时间) | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 | 操作 |
|------------------------------|---------------------|---------------|---------------------|-------------|------|--------|---------------|
| manuBackup_20160517135011_96 | 2016-05-17 13:50:11 | 1054.818 | 2016-05-17 13:50:11 | 5286.571716 | 手动备份 | 未上传 | <div>还原</div> |

2.2.2 数据清理

2.2.2.1 备份文件清理

通过备份文件清理页面，可进备份查询，可以“备份方式”、“备份日期”、“备份文件存放的目录”三个条件进行筛选查询，筛选后符合条件的备份文件将会显示在备份文件列表中。可通过备份文件所对应的“删除”按钮行删除。

备份查询

备份方式

自动备份

手动备份

备份的日期

至

备份文件存放的目录

backup

查询

备份文件列表

| 备份文件名 | 备份时间 | 备份耗时 (数据结束时间) | 备份文件大小 | 备份方式 | 文件状态 | 最后一次恢复 | 操作 |
|------------------------------|---------------------|---------------|---------------------|-------------|------|--------|---------------|
| manuBackup_20160517135011_96 | 2016-05-17 13:50:11 | 1054.818 | 2016-05-17 13:50:11 | 5286.571716 | 手动备份 | 未上传 | <div>删除</div> |

2.2.2.2 自动清理

通过自动清理页面，可对文件系统默认配置和每日自动清理配置进行设置。

文件系统默认配置

配置

当文件系统达到80%时，存储系统将执行审计停止写入操作。

每日自动清理配置

每日自动清理

启用

禁用

启用后，系统在每天的0点开始清理

在线数据可占有文件系统的最大比例是

80%

如果大于此设定值系统将自动产生告警并

备份系统并上传所有备份文件

开启此功能需要确保远程(FTP)页面中的ftp配置可用

清理系统业务数据

扫描、检索、报表中的数据，配置信息不处理，如引擎、策略等

清理系统配置数据

系统监控、系统报警、告警配置的信息

删除3个月以前的审计日志

删除3个月以前的审计日志

保存

文件系统默认配置

通过文件系统默认配置，可设置当文件系统达到一定百分数时，存储系统执行“审计停止写入”或是“覆盖最早的记录”操作。

文件系统默认配置

配置

当文件系统达到80%时，存储系统将执行审计停止写入操作。

每日自动清理配置

审计停止写入

覆盖最早记录

每日自动清理配置

通过每日自动清理配置，可设置是否开启此功能，以及在线数据可占有文件系统的最大比例；如果大于此设定值系统将自动产生告警并执行那些操作。

| 每日自动清理配置 | |
|--------------------|--|
| 每日自动清理 | <input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 <div>启用后，系统在每天的0点开始清理</div> |
| 在线数据可占有文件系统的最大比例是 | <input type="text" value="80"/> % |
| 如果大于此设定值系统将自动产生告警并 | <div> <input checked="" type="checkbox"/> 备份系统并上传所有备份文件 <div>开启此功能需要确保远程(FTP)页面中的ftp配置可用</div> </div> <div> <input checked="" type="checkbox"/> 清理系统业务数据 <div>扫描、检索、报表中的数据，配置信息不处理，如引擎、策略等</div> </div> <div> <input checked="" type="checkbox"/> 清理系统配置数据 <div>系统监控、系统报警、告警配置的信息</div> </div> <div> <input checked="" type="checkbox"/> 删除3个月以前的审计日志 <div>删除3个月以前的审计日志</div> </div> |
| <div>保存</div> | |

每日自动清理：设置是否启用。

在线数据可占有文件系统的最大比例是：设置相应的百分值。

如果大于此设定值系统将自动产生告警并：选取所需要执行的操作。

提示：所做的配置需要点击“保存”按钮进行保存，否则不能生效。

2.2.2.3 恢复出厂设置

通过恢复出厂设置页面可以进行清理系统配置数据、清理系统业务数据、恢复出厂设置操作。

| 恢复出厂设置 | |
|----------|--|
| 清理系统配置数据 | <div>清理系统管理数据</div> <div>系统配置数据主要包括：系统监控、系统报警、告警配置的信息</div> |
| 清理系统业务数据 | <div>清理系统业务数据</div> <div>系统业务数据主要包括：扫描、报表中的数据，配置信息不处理，如引擎、策略等</div> |
| 恢复出厂设置 | <div>恢复到出厂时的设置</div> <div>恢复出厂设置：此操作将删除系统所有数据，恢复到出厂时的状态，请谨慎操作！</div> |

系统配置数据主要包括：系统监控、系统报警、告警配置的信息。

系统业务数据主要包括：扫描、报表中的数据，配置信息不处理，如引擎、策略等。

恢复出厂设置：此操作将删除系统所有数据，恢复到出厂时的状态，请谨慎操作！

警告：以上操作将会更改已做的系统配置等，请谨慎点击。

三、 安全配置

安全配置主要包括添加数据库引擎、配置并开启审计或防火墙功能等。主要操作用户为 SecAdmin，主要模块包括“通用配置”、“数据库审计与防火墙”、“设备和敏感数据扫描”、“风险扫描”、“数据库状态监控”等。

3.1 数据库引擎管理

所要审计保护的数据库被称为引擎。在使用数据库审计、防火墙以及数据库状态监控、风险扫描等功能前首先需要添加数据库引擎信息。包括数据库 IP、端口、类型、缺省数据库等。添加数据库引擎，需 SecAdmin 用户在“通用配置”模块进行操作

3.1.1 添加

进入“通用配置”模块的“数据库引擎”页面，点击“添加”按钮，弹出添加引擎窗口，如下图所示：

| | |
|-------|----------------------------|
| 名称 | 172.17.200.191:5236/DAMENG |
| IP | 172.17.200.191 |
| 端口 | 5236 |
| 类型 | 达梦7 |
| 缺省数据库 | DAMENG |

💡 数据库的默认端口：[Oracle 1521] [SQL Server 1433] [DB2 50000] [MySQL 3306] [Sybase 5000] [达梦 5236]

✓ 确定

名称：名称可以根据填写的引擎信息自动生成，建议根据本引擎数据库功能用途手动改写名称以便区分。

IP：所要审计保护的数据库 IP 地址。

端口：系统显示为各数据库默认端口号，在实际配置中请按照环境情况填写。

类型：系统所支持的所有数据库类型，根据情况选择所审计保护的数据库类型。

缺省数据库：即数据库实例名，系统显示为各数据库默认实例名；根据实际情况填写数据库实际实例名。

3.1.2 删除

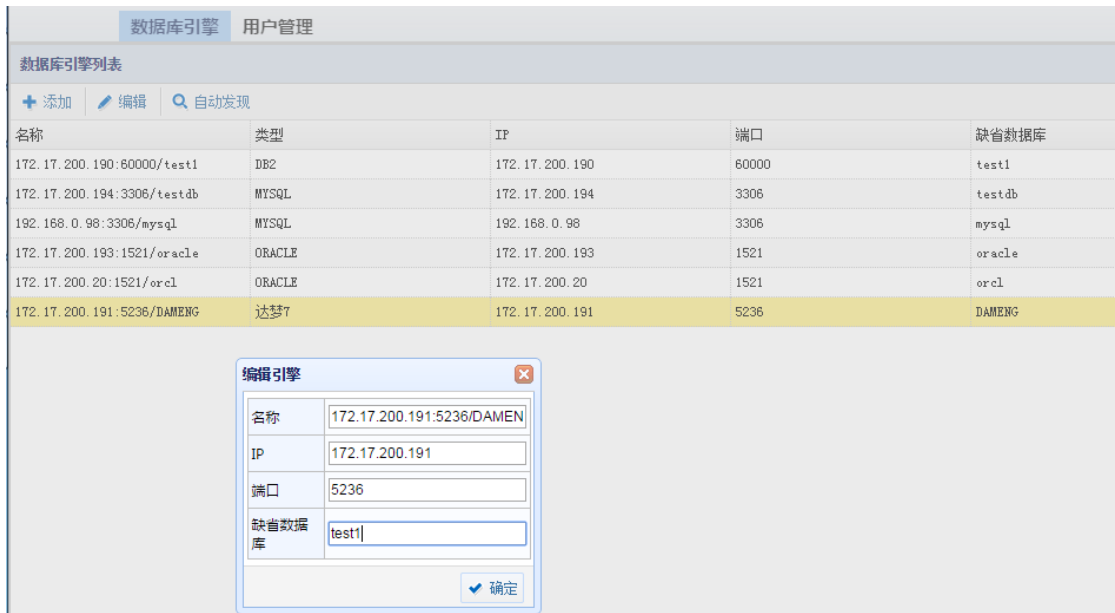
点击需要删除的引擎的“删除引擎”按钮，弹出“提示”窗口，点击确定即可删除



提示：当数据库引擎正在被“审计防火墙”、“状态监控”、“风险扫描”之中的任一模块所使用，则不能删除，需要先停止使用方可删除。

3.1.3 编辑

点选需要编辑的引擎，点击“编辑”按钮，弹出编辑引擎窗口，编辑需要修改的信息，点击“确定”



提示：当数据库引擎正在被“审计防火墙”、“状态监控”、“风险扫描”之中的任一模块所使用，则不能进行编辑，需要先停止使用方可编辑。

3.1.4 自动发现

点击“自动发现”按钮，弹出自动发现窗口，输入起始和结束 IP 及端口，点击“扫描”按钮，扫描结束后，扫描到的引擎会被自动加入到数据库引擎列表中。



3.1.5 审计防火墙

在使用数据库审计或防火墙功能时首先需要添加数据库引擎，添加数据库引擎后添加审计与防火墙功能。若设备为旁路部署则使用审计功能，同时需要选择镜像数据库的来源接口；若设备串联在网络中则使用防火墙功能。详细配置需结合“数据库审计与防火墙模块”

点击数据库引擎所对应的“审计或防火墙”的“添加”按钮，弹出添加审计或防火墙窗口，如下图所示：

| 审计防火墙 | 状态监控 | 风险扫描 | 操作 |
|--------|--------|--------|------------|
| 详情 删除 | 添加 | 详情 删除 | 删除引擎 测试连接 |
| 详情 删除 | 详情 删除 | - | 删除引擎 测试连接 |
| 详情 删除 | 添加 | - | 删除引擎 测试连接 |
| 详情 删除 | 添加 | 详情 删除 | 删除引擎 测试连接 |
| 添加 | 添加 | 添加 | 删除引擎 测试连接 |
| 添加 | 添加 | 添加 | 删除引擎 测试连接 |
| 添加 | 添加 | - | 删除引擎 测试连接 |

添加审计或防火墙

名称

172.17.200.20:1521/orcl

应用模式

☒ 审计 ☐ 防火墙

网口名称

enp1

确定

名称：所添加审计防火墙的名称，默认为添加的数据库引擎的名称。

应用模式：根据需求以及设备在网络环境中的连接情况，选择是审计模式还是防火墙模式。

网口名称：审计数据的来源口,根据镜像所连接设备的网口进行选择。

3.1.5.1 示例 1：添加审计

添加 IP 为 172.17.200.20 的数据库引擎的旁路审计功能。

点击数据库引擎所对应的审计或防火墙的 “添加” 按钮，弹出 “添加审计或防火墙” 窗口，如下图所示：

| 审计防火墙 | 状态监控 | 风险扫描 | 操作 |
|--------|--------|--------|------------|
| 详情 删除 | 添加 | 详情 删除 | 删除引擎 测试连接 |
| 详情 删除 | 详情 删除 | - | 删除引擎 测试连接 |
| 详情 删除 | 添加 | - | 删除引擎 测试连接 |
| 详情 删除 | 添加 | 详情 删除 | 删除引擎 测试连接 |
| 添加 | 添加 | 添加 | 删除引擎 测试连接 |
| 添加 | 添加 | 添加 | 删除引擎 测试连接 |
| 添加 | 添加 | - | 删除引擎 测试连接 |

添加审计或防火墙

名称

172.17.200.20:1521/orcl

应用模式

☒ 审计

☐ 防火墙

网口名称

enp1

确定

根据实际情况镜像口连接设备的 enp1 口（需要 SysAdmin 用户或是有系统管理模块权限的用户，在 “系统管理” 模块> “系统配置” > “接口设置” 中将 enp1 设置为审计口，并在 “接口功能” 中开启 enp1 口的审计功能），故网口选择 enp1。点击 “确定”。

3.1.5.2 示例 2：添加防火墙

添加 IP 为 172.17.200.191 的数据库引擎的防火墙功能。设备通过设备的 enp3,enp4 串联接入网络环境（需要 SysAdmin 用户或是有系统管理模块权限的用户，在系统管理模块> “系统配置” > “接口设置” 中将 enp3,enp4 设置为网桥，网桥名为 br1），网口名称选择 br1。

| 审计防火墙 | 状态监控 | 风险扫描 | 操作 |
|---------------------------------------|---------------------------------------|---------------------------------------|---|
| 详情 删除 | + 添加 | 详情 删除 | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | 详情 删除 | - | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | + 添加 | - | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | + 添加 | 详情 删除 | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | + 添加 | + 添加 | ✕ 删除引擎 🔗 测试连接 |
| + 添加 | + 添加 | + 添加 | ✕ 删除引擎 🔗 测试连接 |
| + 添加 | + 添加 | - | ✕ 删除引擎 🔗 测试连接 |

添加审计或防火墙

名称

172.17.200.191:5236/DAME

应用模式

☐ 审计

☒ 防火墙

网口名称

br1

确定

3.1.5.3 示例 3：删除审计或防火墙

点击已添加的审计或防火墙对应的 “删除” 按钮，弹出确认窗口点击 “确定” 即可删除。

| 审计防火墙 | 状态监控 | 风险扫描 | 操作 |
|---------------------------------------|---------------------------------------|---------------------------------------|---|
| 详情 删除 | + 添加 | 详情 删除 | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | 详情 删除 | - | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | + 添加 | - | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | + 添加 | 详情 删除 | ✕ 删除引擎 🔗 测试连接 |
| 详情 删除 | + 添加 | + 添加 | ✕ 删除引擎 🔗 测试连接 |
| + 添加 | + 添加 | + 添加 | ✕ 删除引擎 🔗 测试连接 |

确认

?

确认删除吗?

确定

取消

提示：添加了数据库引擎的审计防火墙功能后，点击“详情”按钮，能够跳转到“数据库审计与防火墙”模块，在此模块可以控制该引擎的审计和防火墙功能是否开启，并为其进行“策略”设置。

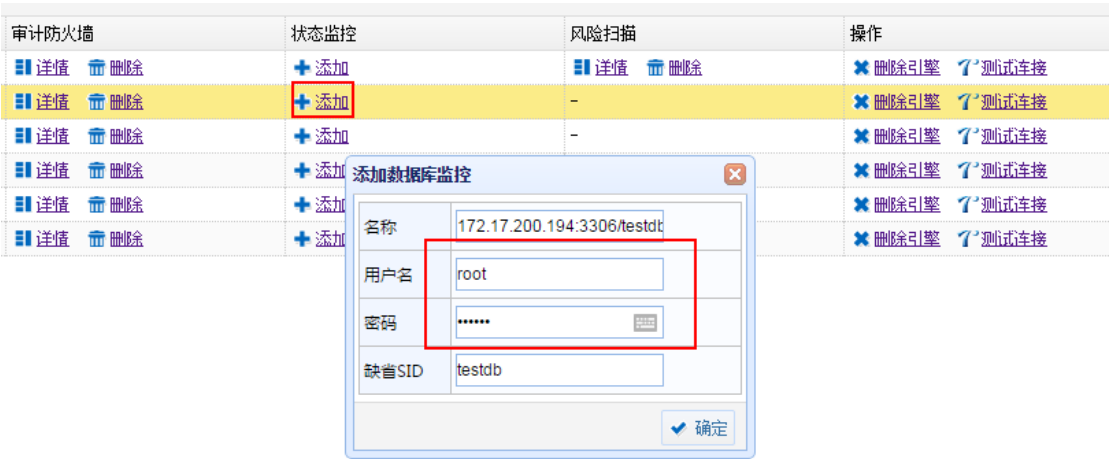
3.1.6 状态监控

数据库状态监控，实时监控数据库运状态，如服务器的运行时间、内存及存储的使用情况等。在异常时进行预警，防止业务瘫痪，保障业务系统的可用性（详细信息参考 5.5 章节）。

示例 1：添加数据库监控

添加 IP 为 172.17.200.194 的数据库引擎的状态监控功能。

点击数据库引擎所对应的“状态监控”的“添加”按钮，弹出添加数据库监控窗口，如下图所示：



名称：数据库状态监控的名称，默认为数据库引擎的名称。

用户名：所要监控数据库的用户名。此用户名需要具有一定的数据库系统权限。

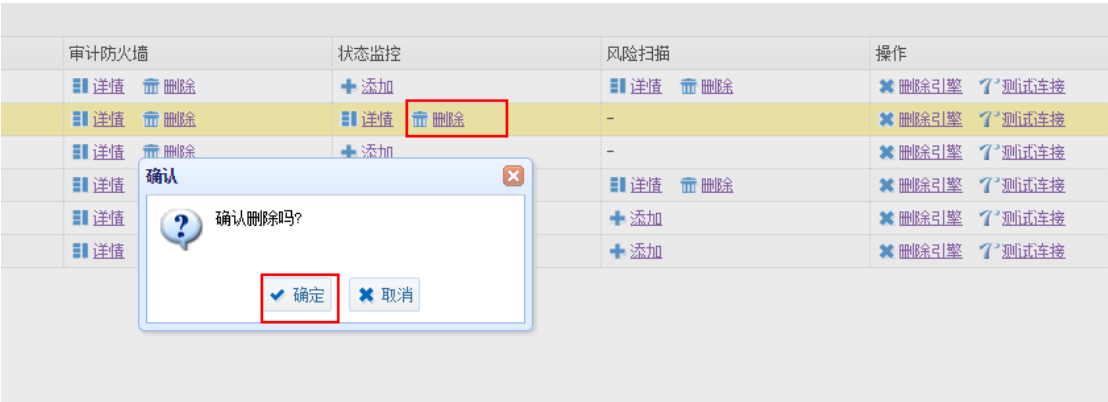
密码：填写用户名对应的密码。

缺省 SID：所监控数据库的实例名，系统默认显示的为各数据库所默认的实例名。

输入相应信息后点击 “确定” 即可。

示例 2：删除数据库监控

点击已添加的数据库监控对应的 “删除” 按钮，弹出 “确认” 窗口点击 “确定” 即可删除。



提示：添加了数据库引擎的状态监控功能后，点击“详情”按钮，能够跳转到 “数据库状态监控” 模块。

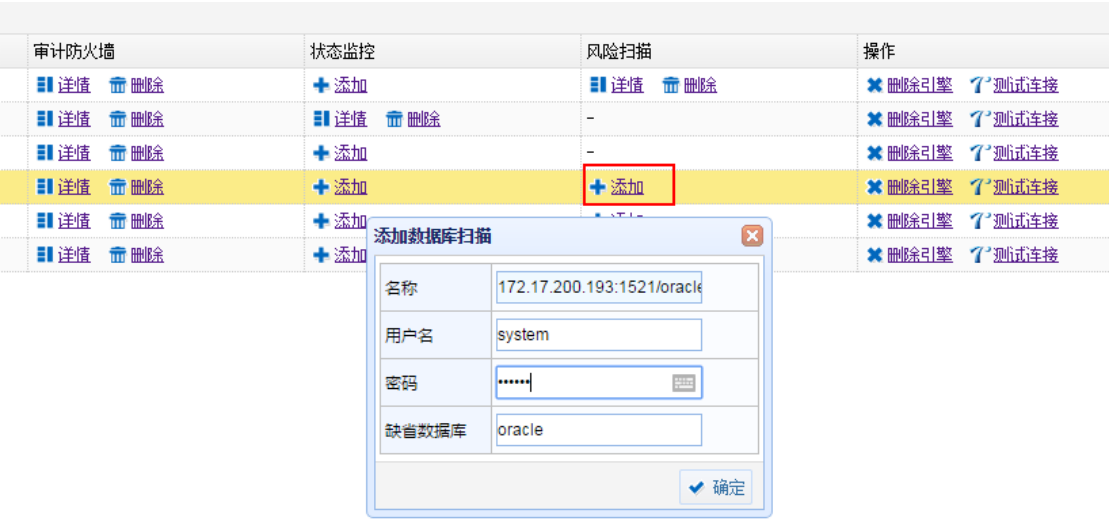
3.1.7 风险扫描

数据库系统是一个复杂的系统资料，数据库存在许多风险，其中不少是致命的缺陷和漏洞。一旦遭到攻击，攻击者可能以 DBA 的身份进入数据库系统，也可能进入操作系统，下载整个数据库文件。为此本系统提供风险扫描模块，使用户能更早的发现风险与漏洞。

示例 1：添加数据库风险扫描

添加 IP 为 172.17.200.193 的数据库引擎的风险扫描功能。

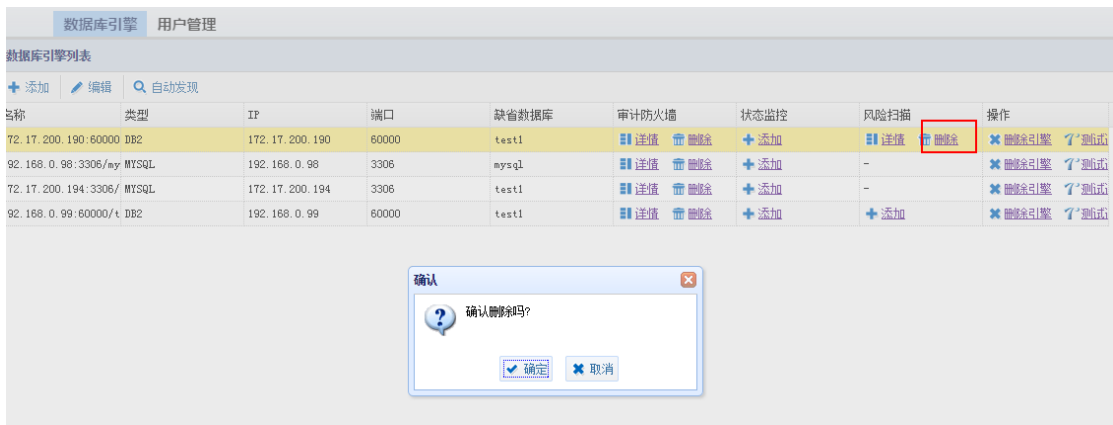
点击数据库引擎所对应的“风险扫描”的“添加”按钮，弹出添加风险扫描窗口，如下图所示：



- 名称：数据库状态监控的名称，默认为数据库引擎的名称。
- 用户名：所要监控数据库的用户名。此用户名需要具有一定的数据库系统权限。
- 密码:填写用户名对应的密码。
- 缺省数据库：所监控数据库的实例名，系统默认显示的为各数据库所默认的实例名。
- 输入相应信息后点击 “确定” 即可。

示例 2：删除风险扫描

点击已添加的风险扫描的数据库引擎对应的“删除”按钮，弹出确认窗口点击“确定”即可删除。



提示：添加了数据库引擎的风险扫描功能后，点击“详情”按钮，能够跳转到“风险扫描”模块。

3.1.8 操作

操作对应“删除引擎”和“测试连接”两个按钮。

3.1.8.1 删除引擎

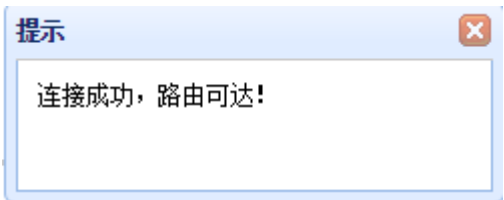
点击需要删除的引擎的“删除引擎”按钮，弹出提示窗口，点击“确定”即可删除。



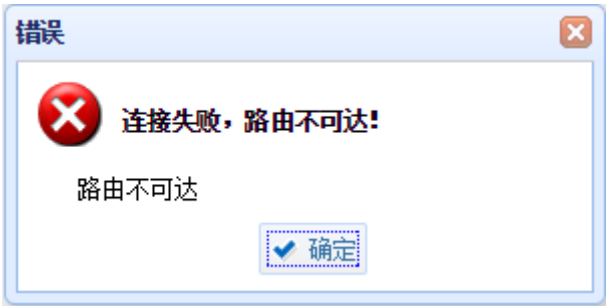
提示：当数据库引擎正在被“审计防火墙”、“状态监控”、“风险扫描”之中的任一模块所使用，则不能删除，需要先停止使用方可删除。

3.1.8.2 测试连接

点击需要测试的引擎的“测试连接”按钮，如何网络可达则在屏幕右下角提示如下：



如果网络不可达则提示如下：



3.2 数据库审计与防火墙

所属用户：SecAdmin。

审计，即数据库审计模块，旁路部署在数据库和客户端之间，提供数据库操作的事后查询分析和实时的告警，同时带有旁路阻断等功能。

防火墙即数据库防火墙，串联部署在数据库和客户端之间，能主动防御或阻断对数据库的攻击或自定义的危险行为，能有效地对数据库提供防护。

3.2.1 审计防火墙

3.2.1.1 审计和防火墙列表

审计和防火墙列表显示已经添加的数据库审计或防火墙引擎信息，可对引擎进行编辑、删除、启动和停止操作。

| 审计防火墙 | | | | |
|------------------------|------|-----|-------|-----|
| 策略中心 最新流量 | | | | |
| 审计防火墙列表 | | | | |
| <div>编辑 删除 启动 停止</div> | | | | |
| 名称 | 审计类型 | 状态 | 类型 | IP |
| 172.17.200.190:6 | 审计 | 运行中 | DB2 | 172 |
| 172.17.200.194:3 | 审计 | 已停止 | MYSQL | 172 |
| 192.168.0.98:330 | 审计 | 已停止 | MYSQL | 192 |
| 192.168.0.99:600 | 审计 | 运行中 | DB2 | 192 |

编辑

选择要编辑的引擎，点击审计防火墙列表下的 “编辑” 此模式下只可以修改以下四项信息。

- a) 名称：可以修改引擎的名称，便于查看和分析。
- b) 所属采集器：修改所属采集器，以应用其它采集器。
- c) 应用模式：切换审计或防火墙模式。
- d) 网口名称：在切换镜像口后需要修改为切换后对应的网口名称才能继续接收数据。

添加审计或防火墙

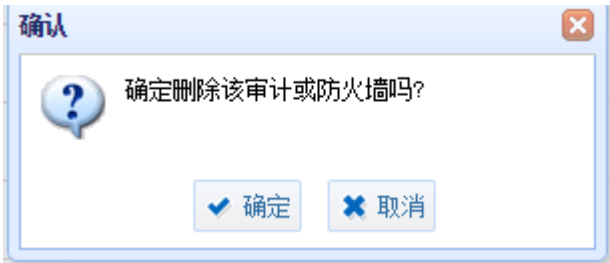
| | |
|-------|---|
| 名称 | 172.17.200.20:1521/orcl |
| IP | 172.17.200.20 |
| 端口 | 1521 |
| 类型 | ORACLE |
| 缺省SID | orcl |
| 所属采集器 | localhost |
| 应用模式 | <input type="radio"/> 审计 <input checked="" type="radio"/> 防火墙 |
| 网口名称 | br1 |

确定

提示： 审计或防火墙功能运行中的引擎要先停止再进行编辑。

删除

删除数据库引擎的审计或防火墙功能。点选相应引擎，点击 “删除” 按钮，弹出确认窗口，点击 “确认”。



提示：审计或防火墙功能运行中的引擎要先停止才能删除。

启动

数据库引擎添加审计和防火墙功能后，默认是停止状态，需要启动才能开始记录信息。

点击要启动的引擎，选择“审计防火墙列表”下的 “启动”。需要启动的引擎的状态栏显示为运行中后，引擎启动成功，可以继续进行其它配置。

| 审计防火墙列表 | | | | |
|------------------------|------|-----|--------|-----|
| <div>编辑 删除 启动 停止</div> | | | | |
| 名称 | 审计类型 | 状态 | 类型 | IP |
| 172.17.200.190:6 | 防火墙 | 运行中 | DB2 | 172 |
| 172.17.200.191:5 | 防火墙 | 运行中 | 达梦7 | 172 |
| 172.17.200.193:1 | 审计 | 运行中 | ORACLE | 172 |
| 172.17.200.194:3 | 审计 | 运行中 | MYSQL | 172 |
| 172.17.200.20:15 | 防火墙 | 已停止 | ORACLE | 172 |
| 192.168.0.98:330 | 审计 | 运行中 | MYSQL | 192 |

停止

有些情况需要停止引擎的审计或防火墙功能，如排查故障、编辑引擎信息、删除引擎。

选择要停止的引擎，选择“审计防火墙列表”下的 “停止”，此引擎对应的数据库审计或防火墙功能暂时停止。此引擎的“状态”栏显示为“已停止”后，引擎停止成功

| 审计防火墙 | | | | | 策略中心 | 最新流量 |
|---|------|-----|--------|-----|------|------|
| 审计防火墙列表 | | | | | | |
|  编辑  删除  启动  停止 | | | | | | |
| 名称 | 审计类型 | 状态 | 类型 | IP | | |
| 172.17.200.190:6 | 防火墙 | 运行中 | DB2 | 172 | | |
| 172.17.200.191:5 | 防火墙 | 运行中 | 达梦7 | 172 | | |
| 172.17.200.193:1 | 审计 | 运行中 | ORACLE | 172 | | |
| 172.17.200.194:3 | 审计 | 运行中 | MYSQL | 172 | | |
| 172.17.200.20:15 | 防火墙 | 已停止 | ORACLE | 172 | | |
| 192.168.0.98:330 | 审计 | 运行中 | MYSQL | 192 | | |

3.2.1.2 设置

点击相应的数据库引擎，右侧会出现对应的设置页面。

审计防火墙策略中心最新流量

审计防火墙列表

编辑删除启动停止

| 名称 | 审计类型 | 状态 | 类型 | IP |
|------------------|------|-----|-------|-----|
| 172.17.200.190:6 | 审计 | 运行中 | DB2 | 172 |
| 172.17.200.194:3 | 审计 | 已停止 | MYSQL | 172 |
| 192.168.0.98:330 | 审计 | 已停止 | MYSQL | 192 |
| 192.168.0.99:600 | 审计 | 运行中 | DB2 | 192 |

设置特征模型模型策略

应用模式

审计

防火墙

引擎停止的状态下才可编辑

数据来源(接口)

enp1

引擎停止的状态下才可编辑

监控数据库应答

开启数据库应答监控

数据库登录辅助

开启数据库辅助获取连接信息 [适用于SQL SERVER2005、2008]

远程监控

启动远程监控

应用模式为审计时才可编辑

本地监控

启动本地监控

威胁监控

启动威胁监控

模糊化日志

启动模糊化日志

旁路阻断

启用旁路阻断

引擎停止的状态下才可编辑

保存并生效

自动学习状态

一段时间后关闭&生成规则

停止时间: 2016-05-30

保存

应用模式

根据实际的需求选择应用模式：审计或防火墙。

应用模式

审计

防火墙

引擎停止的状态下才可编辑

提示：注意部署方式是否对应。

数据来源

配置数据库的通讯包的来源的网络接口，要与此数据库的数据实际连接的镜像口对应。

数据来源(接口)

enp1

引擎停止的状态下才可编辑

监控数据库应答

处理数据库的响应分析和结果分析的设置。

开启数据库应答监控：开启时分析数据库的回应信息。

开启返回结果解析：开启时分析数据库的回应信息的结果内容，如分析出返回行数等。

监控数据库应答

☒ 开启数据库应答监控
☒ 开启返回结果解析

数据库登录辅助

由于有些特殊的数据库对通讯进行了加密处理，造成了直接解析数据库的协议无法得到所需要的审计信息，如用户名等。这种情况下直接添加引擎无法实现审计和防火墙的功能，此时就需要使用数据库登录辅助功能，对数据库进行再次通讯以获取必要的信息。目前适用于 SQL SERVER 2005、2008 及以上版本，设置界面如下图所示。

☒ 开启数据库辅助获取连接信息 [适用于SQL SERVER2005、2008] ?

设置

| | | | |
|------|----------------------|-------------------------------------|--------------------------|
| IP地址 | <input type="text"/> | 端口 | <input type="text"/> |
| 用户名 | <input type="text"/> | 密码 | <input type="password"/> |
| 数据库名 | <input type="text"/> | <input type="button" value="测试连接"/> | |

IP 地址：数据库引的 IP。但如果条件允许，建议最好给数据库新增 1 个专门用于该类通信的 IP 以便区分。

端口：对应的端口号。

用户名：可以是 tools\ddi 建立的受限用户。

密码：用户名对应的密码。

数据库名：默认 master，若为其它请手动修改。

点击“测试连接”，显示成功后保存配置，若测试失败请检查数据库是否正常连接以及配置是否正确。

此处的用户名可以是数据库超级管理员。有些情况为了安全起见，不能提供很大的管理员权限，此时可以使用我们提供的 SQL 脚本，建立受限权限的用户，只保留数据库审计和防火墙所需的数据库权限。

远程监控

远程监控适用于软件镜像部署的模式。首先需要在数据库上安装镜像软件，然后在页面上进行配置，即可进行远程监控。

修改脚本

linux:

```
./linux/csremote.sh
```

将其中 DB_PORT=3306 中 3306 改为 数据库端口

将其中 DB_IP=192.168.1.55 中 192.168.1.55 改为 数据库 ip

将其中 INTERFACE=eth3 中 eth3 改为 数据库使用网卡

将其中 RA_TARGET_IP=192.168.1.157 中 192.168.1.157 改为 审计

接口对应 ip。

windows:

```
./windows/csremote.bat
```

将其中 DB_PORT=1433 中 1433 改为 数据库端口

将其中 DB_IP=192.168.1.61 中 192.168.1.61 改为 数据库 ip

将其中 INTERFACE=1 中 1 改为 数据库使用网卡

将其中 GATEWAY=192.168.1.254 中 192.168.1.254 改为 数据库所在

网关

将其中 RA_TARGET_IP=192.168.1.189 中 192.168.1.189 改为 审计

接口对应 ip.

在被监控的数据库所在主机上执行如下脚本

linux: ./linux/csremote.sh

windows: ./linux/csremote.bat

检查审计系统 nc 是否启动, 若没有启动执行 `sudo nc -l 7000`

系统配置, IP 地址设置为当前引擎对应数据库的 IP, 端口号默认为 7000。

本地监控

一些小型的 B/S 应用, WEB 服务器和数据库服务器在一台机器上, 此时数据库和客户端不需要通过网络接口, 需要需要审计和防火墙, 应进行本地监控的配置。本地监控需要运行被监控的数据库和我们的 WEB 应用, 并对其进行一定配置, 系统中配置页面如下图所示。下面我们举例说明本地监控的使用方法。

| 设置 | | | |
|------|----------------------|----------------------|--------------------------|
| IP地址 | <input type="text"/> | 端口 | <input type="text"/> |
| 用户名 | <input type="text"/> | 密码 | <input type="password"/> |
| 数据库名 | <input type="text"/> | 测试连接 | |

数据库相关配置

向数据库安装 `install-script` 中的脚本, 按照 `localmon\Oracle` 和 `localmon\SQLServer` 下 `readme.txt` 中的说明执行安装, 并记下其中的密码。

WEB 应用所需配置

WEB 应用中的配置为建立引擎以及配置本地监控, 具体操作步骤如下:

- 在引擎项目下, 选择"添加", 填入相应的数据库信息。
- 对已添加的引擎, 选择"审计与防火墙"列下的"添加", "应用模式"选择"审计", 填入自定义的名称, 并选择网口名称, 选择完成。

c) 查看已添加"审计与防火墙"的详情,选择"设置"分页,选择"本地监控",在本地监控的详细设置中填入相关信息:被监控的数据库 Ip, 用户名和密码, 用户名为: CSBIT_CONSOLE_ACCESS_QRY, 密码为安装过程中输入的后一个密码。数据库端口、名称。

点击“测试连接”,如果提示连接成功则表示以上数据可用,否则,请检查以上输入是否正确。

在左侧的“引擎列表”中选择启动以上设置的引擎。

本地监控测试

启动 tapcenter 测试版,tapcenter 会将本地监控收到的 SQL 信息在控制台中输出,其启动命令行如下:

```
#./tapcenter --logtostderr=true --minloglevel=0
```

tapcenter 将会收到对被监控数据库进行的操作并显示在控制台中,包括以下内容

操作类型:login, logout 和 Others(执行 SQL 语句)

一般操作相关信息:seesionid,操作发生的时间,执行 sql 所花费的时间,对于 login 操作,还包括以下信息:

数据库用户名, 连接数据库的应用程序名称, 系统名称, 系统用户名, 主机名,数据库名, 客户端 IP, 客户端, 客户端端口, 数据库 MAC。

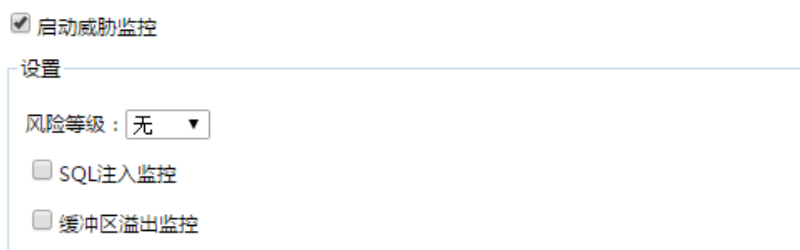
对于 Other 类型的操作,包括 sql_text(被执行的 SQL 语句),reply(执行结果),replyLen(执行结果长度)

注意:

- a) 目前仅支持 Oracle 和 SQLServer。
- b) 测试过程中可以手工输入一些 SQL 语句,查看 tapcenter 是否监控到。
- c) 如果用户 login,执行 sql,马上 logout,将较难监控到其操作。

威胁监控

有一些特殊的状态，虽然行为合规，但可能会对数据库造成威胁，对此时需要进行数据库威胁监控，如下图所示：



主要的可选设置项有：

风险等级：可以主动设置威胁行为的风险等级，高风险和致命风险会显示在告警页面上，以便管理员及时发现威胁行为。

SQL 注入监控：SQL 注入就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终能够欺骗服务器执行恶意的 SQL 命令。开启 SQL 注入监控后系统会识别恶意的 SQL 命令并及时告警或阻拦。

缓冲区溢出监控。缓冲区溢出攻击可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。开启缓冲区溢出监控后，系统在面对缓冲区溢出风险的时候会进行告警或阻拦。

模糊化日志

为了保护敏感的信息，如电话号码、身份证号等，可以将这些信息进行模糊处理以增加保密性，设置界面如下图所示。

☒ 启动模糊化日志

设置

+ 添加

编辑

删除

| 名称 | 正则式 | 替换值 |
|----|-----|-----|
|----|-----|-----|

每个项有如下的内容：

名称：该条模糊化信息的标识。

正则式：替换的正则式内容。点击“添加”，出现如下图所示界面。

添加

| | | |
|-----|----------------------------------|-----------|
| 名称 | <input type="text"/> | |
| 正则式 | <input type="text"/> | |
| 替换值 | <input type="text" value="###"/> | (默认'###') |

确定

点击图中的“？”，会出现如下图所示的正则表达式帮助文档。

正则表达式帮助文档

什么是正则表达式？

正则表达式(regular expression)描述了一种字符串匹配的模式。本系统用来检查一个数据库请求中是否含有某种子串。是由普通字符（例如字母a到z）以及特殊字符（称为元字符）组成的文字模式。正则表达式作为一个模板，将某个字符模式与所搜索的字符串进行匹配。本系统采用使用最广泛的perl兼容正则表达式系统。

主要的正则表达式符号表

| 字符 | 描述 |
|-------|--|
| \ | 将下一个字符标记为一个特殊字符、或一个原义字符、或一个向后引用、或一个八进制转义符。例如，'n' 匹配字符 'n'。'\n' 匹配一个换行符。序列 '\\' 匹配 '\' 而 '\(' 则匹配 '('。 |
| ^ | 匹配输入字符串的开始位置。如果设置了RegExp对象的Multiline 属性，^ 也匹配 '\n' 或 '\r' 之后的位置。 |
| \$ | 匹配输入字符串的结束位置。如果设置了RegExp 对象的Multiline 属性，\$ 也匹配 '\n' 或 '\r' 之前的位置。 |
| * | 匹配前面的子表达式零次或多次。例如，zo* 能匹配 "z" 以及 "zoo"。* 等价于 {0,}。 |
| + | 匹配前面的子表达式一次或多次。例如，'zo+' 能匹配 "zo" 以及 "zoo"，但不能匹配 "z"。+ 等价于 {1,}。 |
| ? | 匹配前面的子表达式零次或一次。例如，"do(es)?" 可以匹配 "do" 或 "does" 中的 "do"。? 等价于 {0,1}。 |
| {n} | n 是一个非负整数。匹配确定的n次。例如，'o{2}' 不能匹配 "Bob" 中的 'o'，但是能匹配 "food" 中的两个 o。 |
| {n,} | n 是一个非负整数。至少匹配n次。例如，'o{2,}' 不能匹配 "Bob" 中的 'o'，但能匹配 "fooooood" 中的所有 o。'o{1,}' 等价于 'o+'。'o{0,}' 则等价于 'o*'。 |
| {n,m} | m和n均为非负整数，其中n <= m。最少匹配 n 次且最多匹配m次。例如，"o{1,3}" 将匹配 "fooooood" 中的前三个o。'o{0,1}' 等价于 'o?'。请注意逗号和两个数之间不能有空格。 |

替换值：敏感信息替换成的文字，默认'# # #'，可以修改为任意值，则凡是出现匹配到上面的正则表达式的信息，即自动替换为此值。

旁路阻断

在引擎未启动的情况下，可以选择启用旁路阻断功能，此时在旁路部署的数据库审计模式下依然可以对数据库操作进行阻断。旁路阻断与数据库防火墙的阻断区别：旁路阻断通过旁路发 RST 包进行阻断。如下图所示，启用旁路阻断，选择阻断包发送的网卡，成功开启旁路阻断功能。

旁路阻断

☒ 启用旁路阻断

引擎停止的状态下才可编辑

网卡：

enp1

保存并生效

自动学习状态

通过自动学习状态可以控制学习开始和结束及生成策略。如下图所示：

自动学习状态

一段时间后关闭&生成规则

开启

关闭&生成规则

一段时间后关闭&生成规则

关闭&不生成规则

停止时间：2016-05-16

保存

3.2.1.3 特征模型

在“特征模型”模块中可对“学习”进行设置，自动学习访问数据库的行为，并对行为进行分析学习，将学习到的模型，生成相应的策略，只要点击停止学习后，模型就会应用到相应的策略上。

设置特征模型模型策略

+ 添加

删除

刷新

| 用户名 | 查询数量 | 查询组数量 | 源IP数量 | 应用程序数量 |
|--------|------|-------|-------|--------|
| system | 0 | 0 | 0 | 0 |
| sys | 0 | 0 | 0 | 0 |

学习

查询组

时间限制

特权操作

高级设置

目标

+ 添加

删除

保存

刷新

锁定

任意值

| 数据库 | Schema | 数量 |
|-----|--------|----|
|-----|--------|----|

表格与操作

+ 添加

删除

保存

刷新

锁定

任意值

| 表 | 选择 | 更新 | 插入 | 删除 |
|---|----|----|----|----|
|---|----|----|----|----|

学习

东软公司 网络安全

69

“学习” 的内容包括目标，表格与操作，源 IP，源应用程序，操作系统主机名，操作系统用户。

学习

查询组

时间限制

特权操作

高级设置

目标

+ 添加

删除

保存

刷新

锁定

任意值

| 数据库 | Schema | 数里 |
|-----|--------|----|
|-----|--------|----|

表格与操作

+ 添加

删除

保存

刷新

锁定

任意值

| 表 | 选择 | 更新 | 插入 | 删除 |
|---|----|----|----|----|
|---|----|----|----|----|

源

查询组

“查询组” 提供特征模型学习到的 sql 语句，可进行策略配置。

学习

查询组

时间限制

特权操作

高级设置

查询组

+ 添加SQL

删除

保存

刷新

锁定

任意值

| 查询组 | 查询 | 建议模式 | 强制模式 |
|-------------------|----|------|---|
| <div>select</div> | 1 | 细颗粒度 | <div>细颗粒度</div> <div>中颗粒度</div> <div>细颗粒度</div> |

时间限制

用户可以根据自己的实际环境，设置具体的时间，年月日均可选择。

学习

查询组

时间限制

特权操作

高级设置

天时间段

☐

 -

周时间段

☐

 -

月时间段

☐

 -

保存

特权操作

系统提供默认的特权操作类型，用户可以根据需要选择相应的特权操作，选择完成后点击“保存”即可。



高级设置

“高级设置”中主要包括了“特征模型与保护策略”、“学习普通（DML）查询组的单个查询”、“查询组列表设置”，“表格与操作列表设置”等。

学习

查询组

时间限制

特权操作

高级设置

特征模型与保护策略

☐ 不保护 (DBA)

☐ 访问敏感表时保护

☒ 任何操作都保护

学习普通 (DML) 查询组的单个查询

☒ 将所有查询组切换为“细颗粒度”

☐ 将所有查询组切换为“中颗粒度”

☐ 切换为“中颗粒度”所需的查询数：

正在处理不属于特征模型，并且与任何查询组都不匹配的查询

查询组列表设置

☒ 关闭：任何不属于特征模型的查询组都会引发违规

☐ 敏感时关闭：只有在包含敏感表格时，不属于特征模型的查询组才会引发违规

☐ 开放模式：不属于特征模型的查询组将不会引发违规

表格与操作列表设置

☐ 关闭模式：任何不属于特征模型的表格与操作都将引发违规

☐ 敏感表格时关闭：只有表格为敏感表格时，不属于特征模型的表格与操作才会引发违规

☒ 开放模式：不属于特征模型的表格与操作将不会引发违规

计入规则的最小重复次数：

10

保存

3.2.1.4 模型策略

系统默认的策略，用户可根据实际情况对这些默认的策略进行风险等级以及操作类型设置，点击“保存”后生效。

| 设置 | 特征模型 | 模型策略 | | | |
|----------------|-------------------------------------|------|----|--|--|
| 名称 | 已启用 | 告警级别 | 操作 | | |
| 尝试执行特权操作 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 无法跟踪的数据库用户 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 时间违规 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的主机 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的操作系统用户 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的敏感表格 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的数据库和Schema | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的数据库用户 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的查询组 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的源IP地址 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的源应用程序 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |
| 未授权的表操作访问 | <input checked="" type="checkbox"/> | 高风险 | 通过 | | |

保存

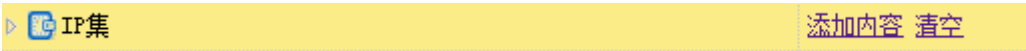
3.2.2 策略中心

3.2.2.1 全局参数

在策略和规则下都可以进行“全局参数”的配置，配置好全局参数，可以在配置每一条具体的规则时直接使用已配置好的参数。

IP 集

“IP 集”即访问数据库服务的 IP 地址段。点击如下图的 IP 集，点击 “添加内容”。在弹出框中输入起始和结束 IP，点击 “确定”，成功设置 IP 集。



如下图所示，如果有不再需要的 IP 集，点击“删除”可以删除该 IP 集，或点击“清空”清空所有 IP 集。

| IP集 | 添加内容 清空 |
|-----------------------|---------|
| 10.0.0.120~10.0.0.122 | 删除 |
| 10.0.0.122~10.0.0.123 | 删除 |

也可以通过 “清空” 按钮将所有 IP 集删除

源应用程序集

源应用程序，即访问数据库服务的机器上的执行程序标题。点击如下图所示的源应用程序集，点击“添加内容”，在弹出框中输入客户端程序，点击“确定”，成功设置源应用程序集。删除、清空同上。

| | |
|-----------|---------|
| 源应用程序集 | 添加内容 清空 |
| db2bp.exe | 删除 |

操作系统用户集

操作系统用户，即访问数据库服务的机器的登陆系统的用户，如下图所示。点击“操作系统用户集”，点击“添加内容”，在弹出框中输入操作系统用户名，点击“确定”，成功设置操作系统用户集。

| | |
|---------|---------|
| 操作系统用户集 | 添加内容 清空 |
| tom | 删除 |

操作系统主机集

操作系统主机，即访问数据库服务的机器的主机，如下图所示。点击“操作系统主机集”，点击“添加内容”，在弹出框中输入操作系统主机名，点击“确定”，成功设置操作系统主机集。删除、清空同上。

| | |
|---------------|---------|
| 操作系统主机集 | 添加内容 清空 |
| TANG-DATAFORT | 删除 |

数据库用户集

数据库用户，即访问数据库的用户。点击“数据库用户集”，点击“添加内容”，在弹出框中输入数据库用户名，点击“确定”，成功设置数据库用户集。

| | |
|----------|---------|
| 数据库用户集 | 添加内容 清空 |
| dbm | 删除 |
| db2inst1 | 删除 |
| tom | 删除 |

数据库表

数据库表，即数据库中存放数据的具体的表。点击 “数据库表”，点击 “添加集”，在弹出框中输入数据库表组名，点击 “确定”，成功设置数据库表组。

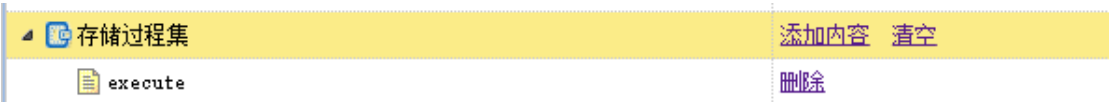
选中添加的表组，点击 “添加内容”，输入表名，点击 “确定”，成功在数据库表组下添加数据库表名。

| | |
|------------------------------|---------|
| 数据库表 | 添加集 |
| 自动学习 | 添加内容 删除 |
| xixi | 删除 |
| emp | 删除 |
| SYSCAT.TABLES | 删除 |
| user_test1 | 删除 |
| 'user_test2' | 删除 |
| INFORMATION_SCHEMA.PROFILING | 删除 |
| 'user_test1' | 删除 |
| user_test2 | 删除 |
| user_info | 删除 |
| user_test | 删除 |
| newone | 删除 |
| newon | 删除 |
| gl | 添加内容 删除 |
| use_info | 删除 |

存储过程集

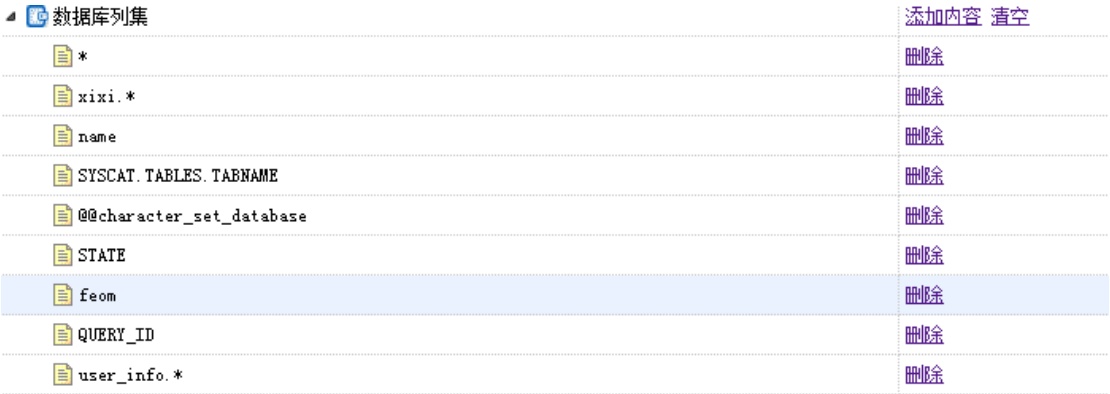
存储过程是在大型数据库系统中，一组为了完成特定功能的 SQL 语句集，存储在数据库中经过第一次编译后再次调用不需要再次编译，用户通过指定存储过程的名字并给出参数（如

果该存储过程带有参数）来执行它。如图，点击 “添加内容” 后，输入存储过程集名，成功添加存储过程集。



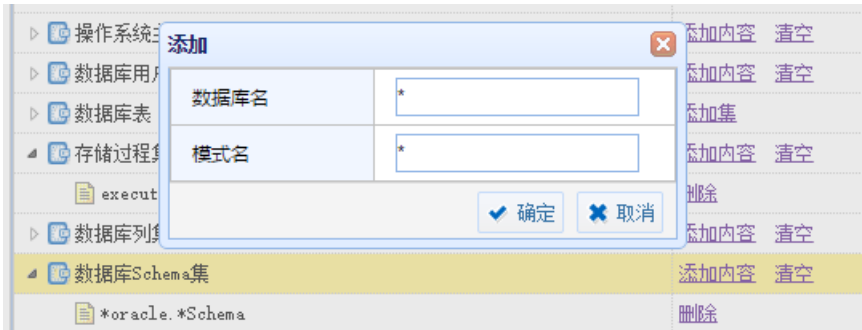
数据库列集

数据库列，即数据库中存放数据的具体的表中的列。点击 “数据库列集”，点击 “添加集”，在弹出框中输入数据列名，点击 “确定”，成功设置数据库列集。



数据库 Schema 集

数据库中的 Schema，为数据库对象的集合，一个用户一般对应一个 schema。为了区分各个集合，数据库 Schma 需要一个名字，在数据库 Schema 集的设置中需要添加的就是集合的名字。点击 “数据库 Schema 集” 后的 “添加内容”，填写数据库名与模式名，点击 “确定” 后成功添加数据库 Schema 集。



SQL 异常字符串组

点击 “SQL 异常字符串组”，点击 “添加集”，在弹出框中输入数据库表组名，点击 “确定”，成功设置 SQL 异常字符串组。

选中添加的组，点击 “添加内容”，输入异常字符串，点击 “确定”，成功添加异常字符串。

| | |
|-----------|---------|
| SQL异常字符串组 | 添加集 |
| gl | 添加内容 删除 |
| where | 删除 |
| select | 删除 |

查询组

点击查询组，点击 “添加集”，在弹出框中输入组名，点击 “确定”，成功设置组。

选中添加的组，点击 “添加内容”，输入查询语句，点击 “确定”，成功添加查询语句。

| | |
|--------------------|---------|
| 查询组 | 添加集 |
| (select, xixi) | 添加内容 清空 |
| select * from xixi | 删除 |

3.2.2.2 策略

策略可以应用于引擎中，所有对引擎对应的数据库的操作，都要经过引擎中配置的策略的分析，当一个引擎存在多个策略时，要分别被每个策略所分析，并根据每个策略的结果进行记录、告警或其它操作。

添加删除策略

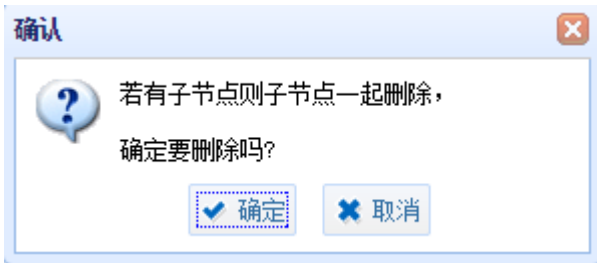
在“策略中心”下，点击 “添加策略”。弹出 添加策略的弹窗



首先填写策略名称作为标识。基于选项条目选择“新建”或已存在的策略，点击 “确定”，成功建立一条新的策略；若选择基于已存在的策略，如基于默认策略，则建立的策略中包含默认策略中的所有配置。

删除策略，点击策略后面的 “删除”，弹出确认窗口，点击 “确定”，成功删除策略。





策略配置

概要

如下图所示，概要处显示该策略的名称和最后的修改时间。

| | | |
|----|------|---------------------|
| 概要 | 名称 | AS |
| | 修改时间 | 2015-02-27 01:00:51 |

大小写敏感设置

如下图所示，可以设置数据库用户、操作系统用户、客户端程序是否区分大小写，默认不区分。

| | | |
|---------|--------|---|
| 大小写敏感设置 | 数据库用户 | <input type="radio"/> 区分大小写 <input checked="" type="radio"/> 不区分大小写 |
| | 操作系统用户 | <input type="radio"/> 区分大小写 <input checked="" type="radio"/> 不区分大小写 |
| | 客户端程序 | <input type="radio"/> 区分大小写 <input checked="" type="radio"/> 不区分大小写 |

应用到引擎

如下图所示，选择策略应用到的引擎，可以同时选择多条，则该策略的配置以及该策略下的规则的配置全部应用到选择的引擎。

| 应用到 | | | | | | |
|-----|----------------------|------------|------|-------|--------|------|
| 保存 | | | | | | |
| | 名称 | IP | 端口 | 网口 | 数据库类型 | 审计类型 |
| 1 | 10.0.0.121:1521/orcl | 10.0.0.121 | 1521 | fire1 | ORACLE | 防火墙 |

规则

添加删除规则

如下图，首先选中一条策略，点击“添加规则”或策略后的“添加”，都会弹出添加规则框。

| + 添加策略 | | | + 添加规则 | | | ↑ 上移 | | | ↓ 下移 | | |
|--------|--|----|--------|-------|--|------|--|--|------|--|--|
| 规则名称 | | 类型 | | 操作 | | | | | | | |
| 默认策略 | | | | 添加 删除 | | | | | | | |
| AS | | | | 添加 删除 | | | | | | | |

规则的逻辑关系

如下图，规则中包含“默认”、“优先级”、“白名单”、“黑名单”四种。四种类型之间的优先级为：黑名单、白名单、优先级、默认。

添加规则

名称:

类型:

☒ 默认

☐ 优先级

☐ 白名单

☐ 黑名单

确定

取消

一条操作的匹配过程如下：

黑名单规则

匹配到黑名单的规则，匹配到一条则不再继续往下匹配，处理方式为“阻断→总是记录→高风险”；若未匹配成功，进入白名单规则。

白名单规则

匹配到白名单的规则，匹配到一条则不再继续往下匹配，处理方式为“通过→不记录→无风险”；若未匹配成功，进入优先级规则。

优先级规则

优先级规则从上往下匹配，匹配到一条则不再继续往下匹配；若未匹配成功，进入默认规则。

默认规则

需要将默认规则下的规则依次进行匹配，对所有匹配到的结果进行处理。

规则的上移下移

规则的位置会影响匹配的优先级，所以规则,需要上移下移，点击要移动的规则，点击“上移”或“下移”，改变规则顺序。

|  添加策略 |  添加规则 |  上移 |  下移 |
|--|--|---|--|
| 规则名称 | 类型 | 操作 | |
|  默认策略 | |  添加  删除 | |
|  黑名单 | 黑名单 |  删除 | |
|  白名单 | 白名单 |  删除 | |
|  优先级 | 优先级 |  删除 | |
|  默认规则 | 无优先级 |  删除 | |

规则的保存

一条规则设置完成后，一定要保存，未保存的配置在离开页面后会全部消失，操作人员在配置的过程中一定要养成随时保存的良好习惯，如下图，点击“保存规则”，弹出提示框“保存成功”，成功保存规则。



规则的展开

要配置某个条件的具体内容，需要先把规则条目展开。如下图所示，点击规则条目前面的“展开”，展开此条目的配置栏，按实际需要配置好相应条目后，点击“保存规则”。

| | | |
|---|---|---|
|  |  | 时间 |
| 天时间段 | | <input type="checkbox"/> 0 - 23 <small>⚡ 设置为x-y则表示x:00:00-y:59:59</small> |
| 周时间段 | | <input type="checkbox"/> 1 - 7 |
| 月时间段 | | <input type="checkbox"/> 1 - 31 |
|  |  | 源 IP 地址 |
|  |  | 源应用程序 |
|  |  | 目标表 |
|  |  | 存储过程 |
|  |  | 操作 |
|  |  | 受影响的行 |

条件的选取

一条规则有很多条件可选，但多数情况下并不需要所有的条件。在需要某个条件时，需要拉取规则，如下图所示，点击一个条件前的“选取”，即此规则中选取了这个条件，只有被拉取的条件才会在规则中生效，页面上被拉取到绿线内。

| | | |
|----|----|---------|
| 展开 | 取消 | 时间 |
| 展开 | 取消 | 源 IP 地址 |
| 展开 | 取消 | 源应用程序 |
| 展开 | 取消 | 目标表 |
| 展开 | 取消 | 操作 |
| 展开 | 取消 | 列 |
| 展开 | 取消 | 操作系统主机名 |
| 展开 | 取消 | 存储过程 |
| 展开 | 选取 | 受影响的行 |
| 展开 | 选取 | 特权操作 |

条件是否包括

每个条件后面都有“包括”、“不包括”的选项。如下图，条件“目标表”已经展开，填写了表“help”，若默认选择“不包括”，则所有操作中未影响表“help”的都会匹配到此条件。

折叠

选取

目标表

>>

<<

自定义:

help

☐ 包括

☒ 不包括


条件间的逻辑关系

设置规则时有许多可选条件，在一般情况下的配置中，我们只选取其中的一部分条件进行配置。这些条件之间是“与”的关系，一条操作在对此规则进行匹配时，需匹配规则下配置的所有条件才能成功匹配此规则。

规则配置

处理方式

如下图所示，处理方式包括“操作”、“日志记录级别”、“风险等级”三个内容。

| | |
|--|----------------|
|  折叠 处理方式 | |
| 操作 | <div>通过</div> |
| 日志记录级别 | <div>不记录</div> |
| 风险等级 | <div>无风险</div> |

左上角的“折叠”处可以选择“折叠”或“展开”。



“操作”分为三种，“通过”、“报警”、“阻断”。“通过”则不做任何额外处理。“报警”则依然通过，但会提示告警信息以便管理员及时发现问题。“阻断”则匹配到此条规则的操作会被阻断。

“日志记录级别”分为三种，“不记录”、“采样”、“总是记录”。“不记录”即凡是匹配到此条规则的操作都不做记录。“采样”即匹配到此规则的操作随机记录部分。“总是记录”即匹配到此规则的操作全部记录。

风险等级共五种，“无风险”、“低风险”、“中风险”、“高风险”、“致命”。为不同的规则分别选择不同的风险等级，以便区分风险操作的危险程度。

时间

可以将客户端访问操作数据库的时间作为规则，如在非工作时间的操作可视为高风险。

| | |
|---|--|
|  折叠  取消 时间 | |
| 天时间段 | <div><input type="checkbox"/> 0 - 23</div> <div>💡 设置为x-y则表示x:00:00-y:59:59</div> |
| 周时间段 | <div><input type="checkbox"/> 1 - 7</div> |
| 月时间段 | <div><input type="checkbox"/> 1 - 31</div> |

源 IP 地址

每一项客户端对数据库的操作都包含源、目的 IP。其中“目的 IP”就是所操作的数据库的 IP，源 IP 即客户端 IP。规则可以针对源 IP 进行筛选。



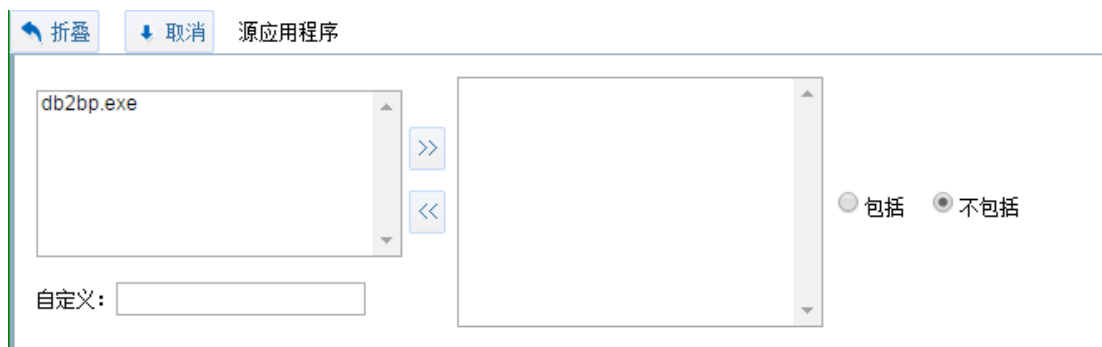
选中要配入规则的 IP， 点击图中“>>”后将此 IP 集配入规则，点击后如下图所示：



在下方的“自定义”处添加 IP 后，点击“>>”同样可以添加 IP 集到规则中。添加好 IP 集，选择是否包括，保存后“源 IP 地址”条件生效。

源应用程序

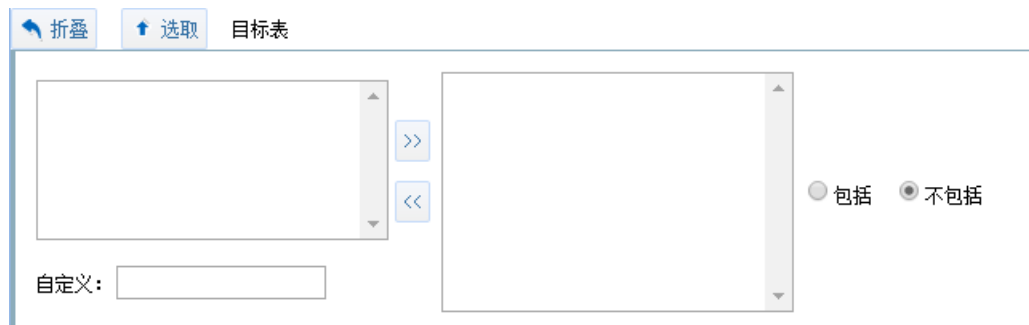
源应用程序，即数据库客户端访问数据库服务的应用程序。



选择已经在全局参数配置好的源应用程序或自定义的应用程序，点击“>”，选择是否包括，保存后，成功配置“源应用程序”条件。

目标表

目标表，即对数据库的操作实际所影响到的表。准确的设置目标表后，凡是涉及到该目标表的操作都会匹配此条件。设置方式同上。



存储过程

存储过程是在大型数据库系统中，一组为了完成特定功能的 SQL 语句集，存储在数据库中经过第一次编译后再次调用不需要再次编译，用户通过指定存储过程的名字并给出参数（如果该存储过程带有参数）来执行它。选中已经在全局参数配置好的存储过程或自定义，点击“>”，选择是否包括后，保存规则，成功配置条件“存储过程”。

折叠

选取

存储过程

>>

<<

execute

☐ 包括

☒ 不包括

自定义:

操作

“操作”指的是数据库操作具体的操作类别。分为“查询、添加、修改、删除、特权操作、登入、登出”七种操作，可选择其中的一项或几项。保存后成功配置条件“操作”。

折叠

选取

操作

查询
添加
修改
删除
特权操作
登入
登出

>>

<<

☐ 包括

☒ 不包括

受影响的行

“受影响的行”指的是数据库操作所影响的表中的行的数量，此项只对 mysql 数据库起作用。选择好限定条件大于、小于、等于等关系后，写入影响行数，如按图中设定，则影响大于等于 5 行的一条数据库操作会匹配到此条件。

影响行数

☒ 大于等于

5

行 (注: 该条件只对 mysql 数据库起作用)

展开

选取

列

展开

选取

特权

展开

选取

操作

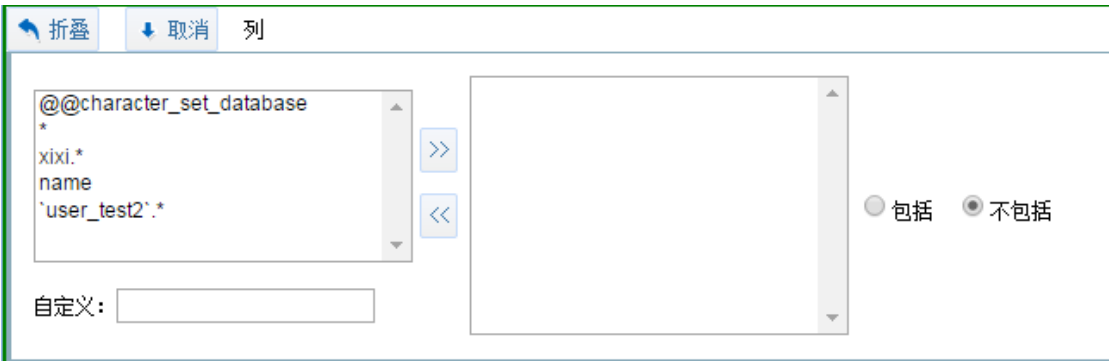
展开

选取

操作

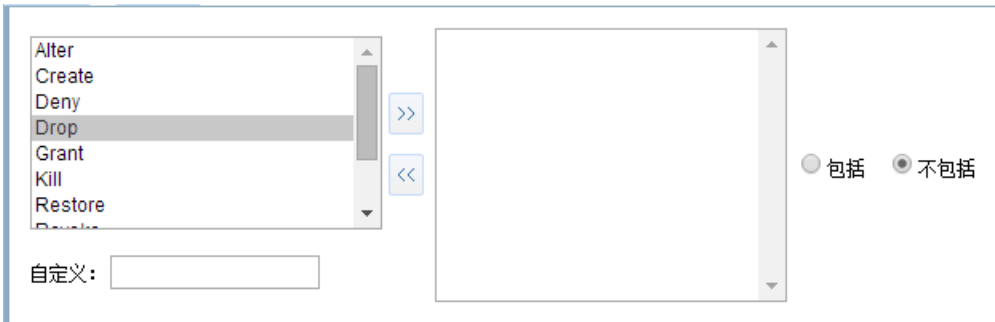
列

“受影响的列”指的是数据库操作所影响的表中的行名。添入相应的列名，选择是否包括后保存，成功设置条件“列”。



特权操作

数据库中除了基本的增、删、改、查操作外的操作都称为特权操作。系统自带了特权操作类型，选择要配置的特权操作类型，点击“>”，选择是否包括后，保存规则，成功配置条件“特权操作”。



操作系统主机名

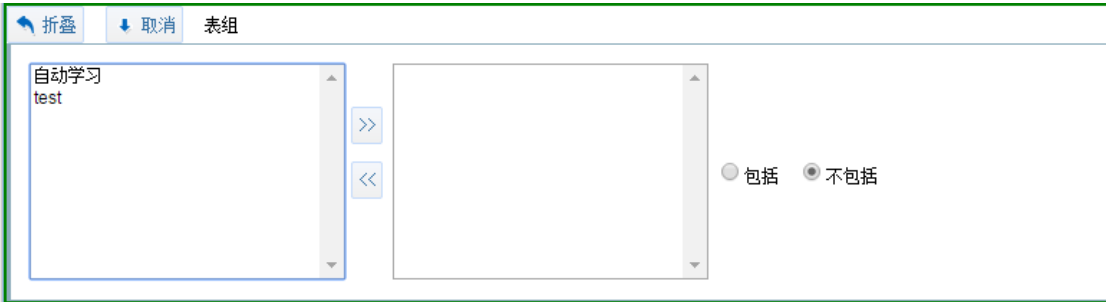
操作系统主机，即数据库客户端访问数据库服务器的登陆系统的主机。添加操作系统的主机名称作为条件选择是否包括，保存，成功设置条件“操作系统主机名”。

操作系统用户名

操作系统用户，即数据库客户端访问数据库服务器登陆系统的用户。选择已经配置好的操作系统用户名或自定义操作系统用户名，点击“>”，选择“包括”或“不包括”后保存，成功配置“操作系统用户名”条件。

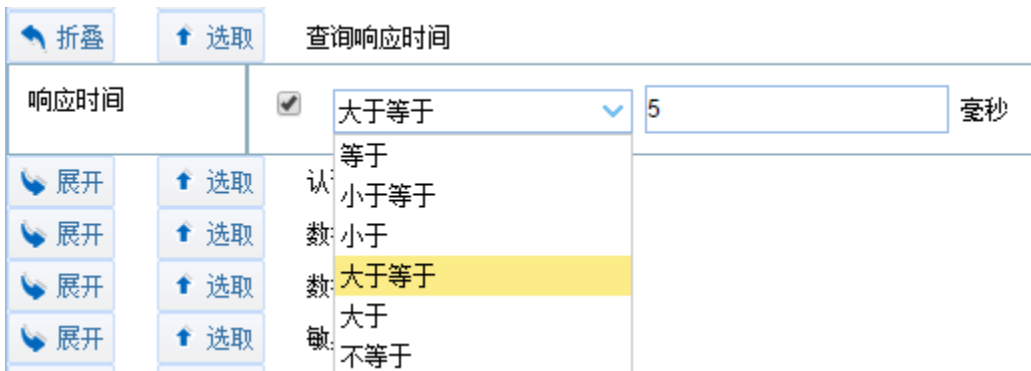
表组

在全局参数下配置好数据库表组后，在此处可以对数据库表组进行配置，匹配到表组下的表，则成功匹配到“表组”条件。



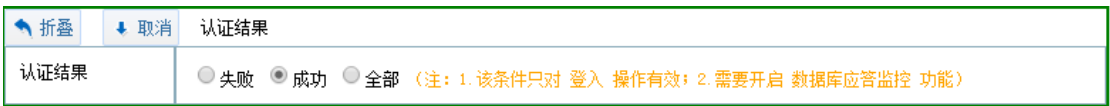
查询响应时间

“查询响应时间”指的是数据库查询的响应速度。选择好限定条件“大于、小于、等于”等关系后，毫秒数，如按图中设定，则查询的响应时间大于等于 5 毫秒的查询会匹配到此条件。



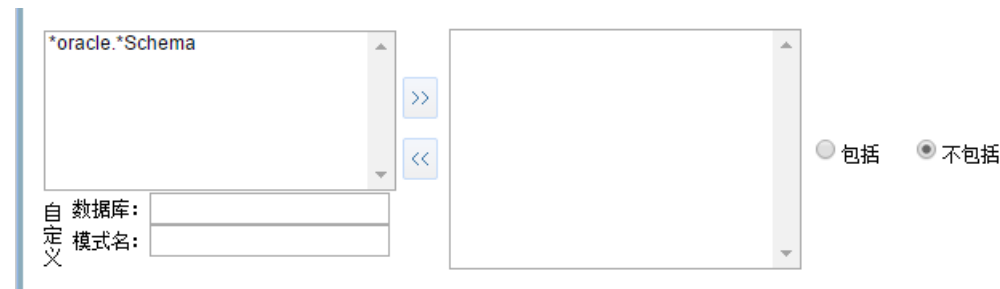
认证结果

认证结果，即一次操作的返回结果，执行是成功还是失败（只对登入动作有效），选择“成功”、“失败”或“全部”后，相应结果的操作会匹配到此条件。



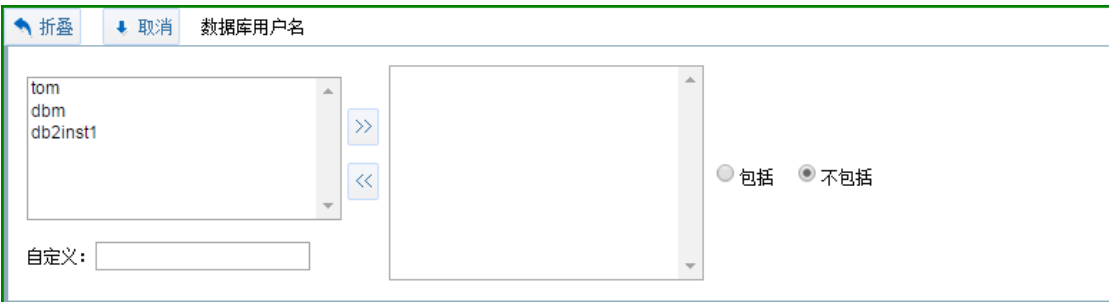
数据库与 Schema

数据库中的 Schema，为数据库对象的集合，一个用户一般对应一个 schema。为了区分各个集合，数据库 Schma 需要一个名字，在数据库 Schema 集的设置中需要添加的就是集合的名字。选择已经在全局参数配置好的数据库与 Schema 集，点击“>”，选择是否包括后，保存规则。



数据库用户名

数据库用户名，即登录数据库的用户名称，当此条件中包含的数据库用户登录数据库或做任何操作时，都会匹配到此条件。



敏感数据访问

如果在“敏感数据扫描”模块下扫描出了数据库的敏感数据，开启判断敏感数据后，所有对敏感数据的操作都会匹配到此条件。选择是否开启“判断敏感数据”后，保存规则，成功配置条件“敏感数据访问”。

折叠

选取

敏感数据访问

判断敏感数据

☐ 是 ☒ 否

发生次数

发生次数限定的是 IP 或用户的操作频率，按照图中设置，若任意 IP 在 1 秒内做了 5 次操作，则匹配到此规则。

折叠

选取

发生次数

发生次数

ip 在 1 秒 发生 5 次

SQL 异常

SQL 语句有时会提示异常，例如执行超时、表不存在等情况，启用 SQL 异常检测，在 SQL 执行出现异常时会匹配到此条件。

折叠

选取

SQL异常

是否启用

☐ 启用 ☒ 不启用

SQL 异常字符串

设置异常字符串后，会检测使 SQL 出现异常的字符串，添入 SQL 异常字符串，或通过正则表达式确定 SQL 异常字符串格式，选择是否包括后，保存规则，成功配置条件“SQL 异常字符串”。

折叠

选取

SQL异常字符串

SQL异常字符串

☐ 包括 ☐ 不包括 ☒ 正则 ?

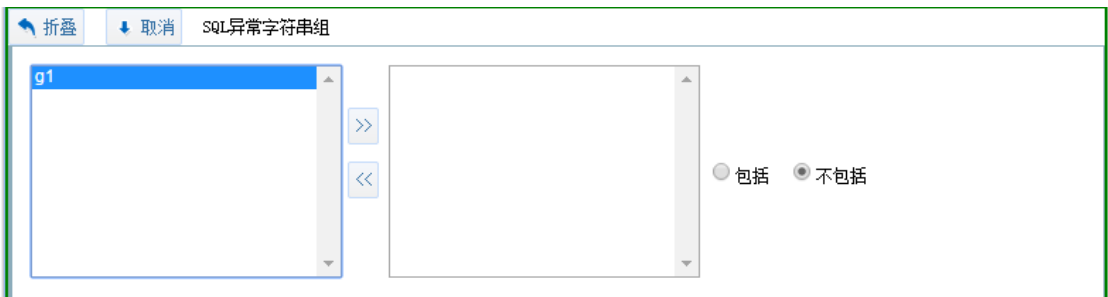
折叠

选取

敏感字典

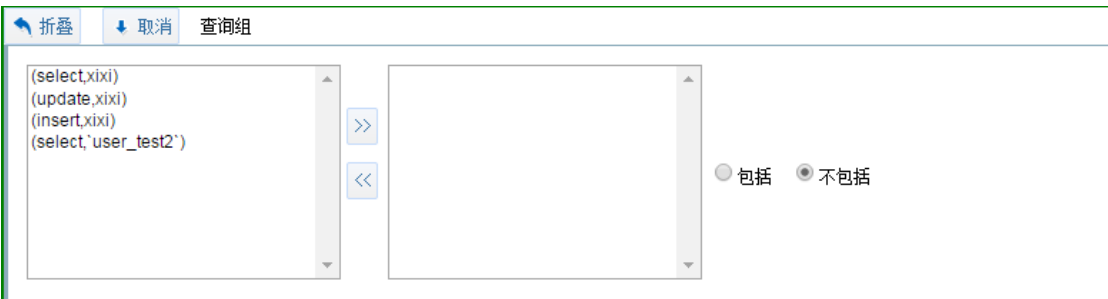
SQL 异常字符串组

在全局参数下配置好 SQL 异常字符串组后，在此处可以对 SQL 异常字符串组进行配置。
SQL 语句匹配到 SQL 异常字符串组中的 SQL 异常字符串，则此条件被成功匹配。



查询组

在全局参数下配置好查询组后，在此处可以对查询组进行配置。SQL 语句匹配到查询组中的条目，则此条件被成功匹配。



3.2.3 最新流量

通过最新流量页面能够查看到日志列表，點選列表中的日志条目，在页面下侧将显示该条日志的详细信息。如下图所示：

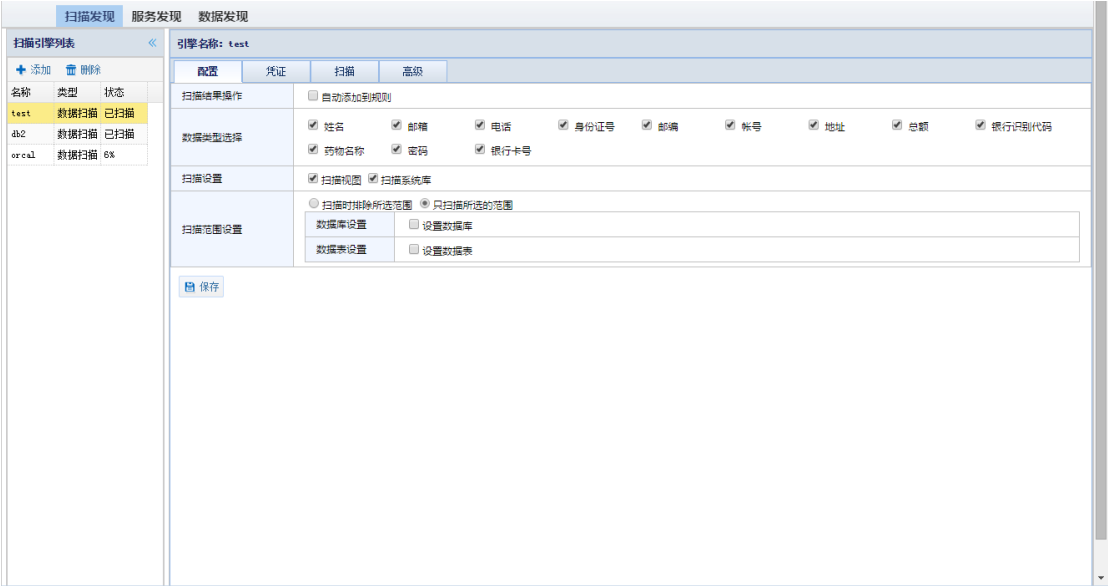


| 审计防火墙 策略中心 策略设置 | | | | | | | | | | | | | |
|-----------------|-----------------------------|--|--|--------|--|---------------------|--|---------|--|----------------|--|---|--|
| 日志列表 | | | | | | | | | | | | | |
| 审计防火墙 | | 策略名称 | | 风险等级 | | 操作时间 | | 数据库用户 | | SQL类型 | | SQL语句 | |
| 1 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:06:57 | | dbinst1 | | Select | | SELECT * FROM SYSSTAT.SCHEMATA ORDER BY SCHEMANAME WITH UR | |
| 2 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:06:57 | | dbinst1 | | Select | | SELECT * FROM SYSSTAT.SCHEMATA WHERE ROWNUM <= 2 ORDER BY TYPEID, TYPEID WITH UR | |
| 3 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:06:56 | | dbinst1 | | Select | | SELECT 'A' TRIM(CORNAME) ' ' SPECIFICNAME FROM SYSSTAT.SCHEMATA WHERE (CHARACTERTYPE = 'C' OR CHARACTERTYPE = 'F') | |
| 4 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:06:56 | | dbinst1 | | None | | SELECT AUTHORITY FROM TABLE SYSSTAT.AUTH_LIST_AUTHORIZATIONS_FOR_AUTHID ('V') AS T WHERE 'V' IS | |
| 5 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:06:56 | | dbinst1 | | Login | | Login | |
| 6 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:06:56 | | dbinst1 | | Login | | Login | |
| 7 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:07:40 | | dbinst1 | | Login | | Login | |
| 8 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:07:40 | | dbinst1 | | Login | | Login | |
| 9 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:07:47 | | dbinst1 | | Login | | Login | |
| 10 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:07:47 | | dbinst1 | | Login | | Login | |
| 11 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:04:26 | | dbinst1 | | Select | | SELECT * FROM SYSSTAT.SCHEMATA ORDER BY SCHEMANAME WITH UR | |
| 12 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:04:26 | | dbinst1 | | Select | | SELECT * FROM SYSSTAT.SCHEMATA WHERE ROWNUM <= 2 ORDER BY TYPEID, TYPEID WITH UR | |
| 13 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:04:26 | | dbinst1 | | Select | | SELECT 'A' TRIM(CORNAME) ' ' SPECIFICNAME FROM SYSSTAT.SCHEMATA WHERE (CHARACTERTYPE = 'C' OR CHARACTERTYPE = 'F') | |
| 14 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:04:26 | | dbinst1 | | None | | SELECT AUTHORITY FROM TABLE SYSSTAT.AUTH_LIST_AUTHORIZATIONS_FOR_AUTHID ('V') AS T WHERE 'V' IS | |
| 15 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:04:26 | | dbinst1 | | Login | | Login | |
| 16 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 12:04:25 | | dbinst1 | | Login | | Login | |
| 17 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 11:56:25 | | dbinst1 | | Login | | Login | |
| 18 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 11:56:25 | | dbinst1 | | Login | | Login | |
| 19 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 11:56:26 | | dbinst1 | | Login | | Login | |
| 20 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 11:56:26 | | dbinst1 | | Login | | Login | |
| 21 | 172.17.200.190:60000/sample | 默认策略-默认规则: 无风险 | | 无风险 | | 2016-05-24 11:56:26 | | dbinst1 | | None | | Session Start | |
| 显示1到30, 共499记录 | | | | | | | | | | | | | |
| 审计防火墙名称 | | 172.17.200.190:60000/sample | | 数据库实例 | | test1 | | 数据库类型 | | DB2 | | 数据库用户 | |
| 操作类型 | | Table | | 操作对象 | | SYSCAT.SCHEMATA | | 数据库IP | | 172.17.200.190 | | 客户端IP | |
| 数据库MAC | | 00-00-00-00-00-00 | | 客户端MAC | | 00-00-00-00-00-00 | | 主机名 | | Lenovo-PC | | 操作系统用户 | |
| 客户端程序 | | db2jcc_application | | 客户端用户 | | | | 客户端端口 | | 50185 | | 操作时间 | |
| 执行时长(毫秒) | | 0 | | 操作 | | 通过 | | 日志级别 | | 信息记录 | | 风险等级 | |
| 策略规则 | | 默认策略-默认规则: 无风险 | | SQL类型 | | Select | | 响应状态 | | 成功 | | | |
| SQL语句 | | SELECT * FROM SYSSTAT.SCHEMATA ORDER BY SCHEMANAME WITH UR | | | | | | | | | | | |
| SQL结果 | | | | | | | | | | | | | |

3.3 设备和敏感数据扫描

所属用户：SecAdmin。

扫描与发现功能用于确定网络中用户核心数据库和关键数据位置的有效方法。管理员可以配置扫描范围并进行扫描，扫描发现执行完毕后，即可配置监测这些发现的项目并对访问它们的行为进行监控和报告。数据库审计设备允许您根据要求和网络的情况创建自定义默认扫描。



3.3.1 模块构成

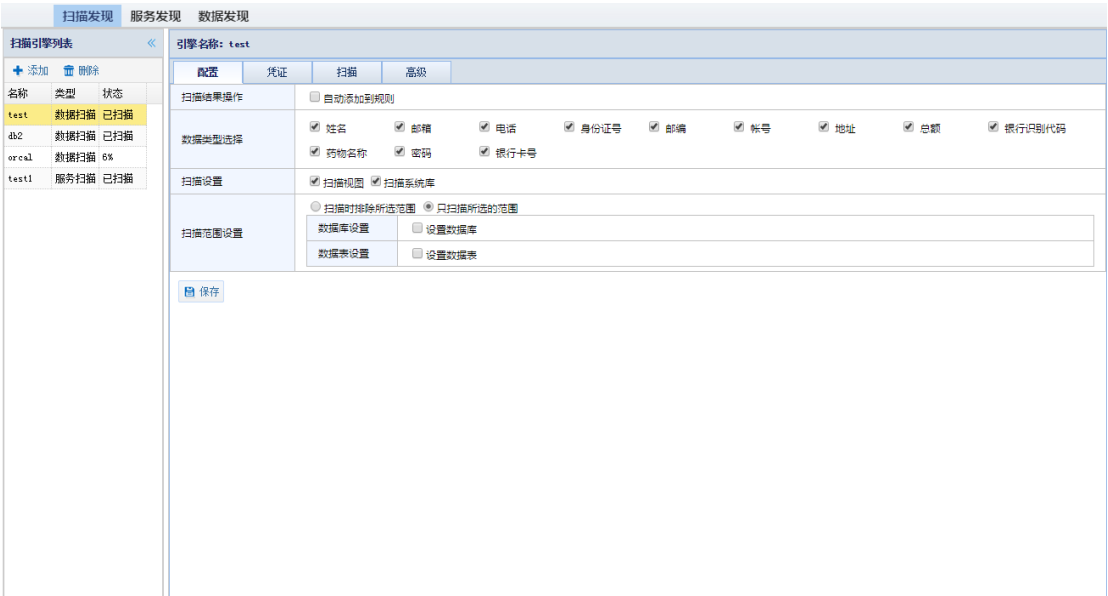
扫描与发现功能由 2 部分构成：服务扫描、数据库扫描。

服务发现：服务发现功能能够扫描网络中的开放端口以及确定这些监听端口的服务。如主机 IP、端口、主机操作系统类型和服务的类型等。并实现自动或手动将这些服务添加到“引擎”上的功能。

数据发现：通过对数据库服务器的扫描，实现对数据库的表名称、schema、敏感数据、敏感表等的自动发现，帮助用户快速定位核心数据资产并对其进行保护。

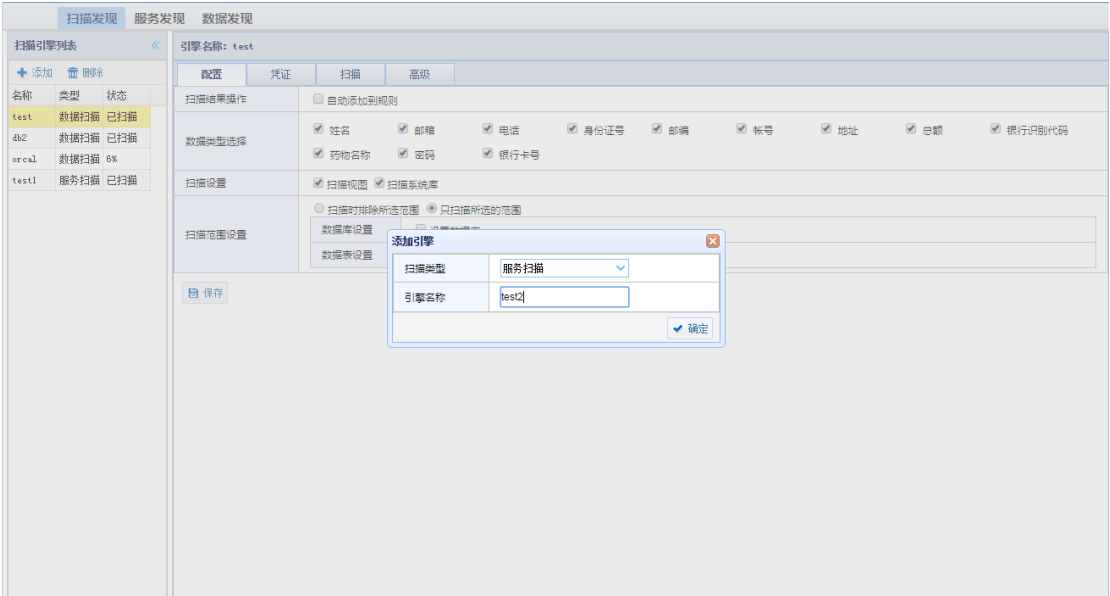
3.3.2 服务扫描

扫描引擎界面如下图所示



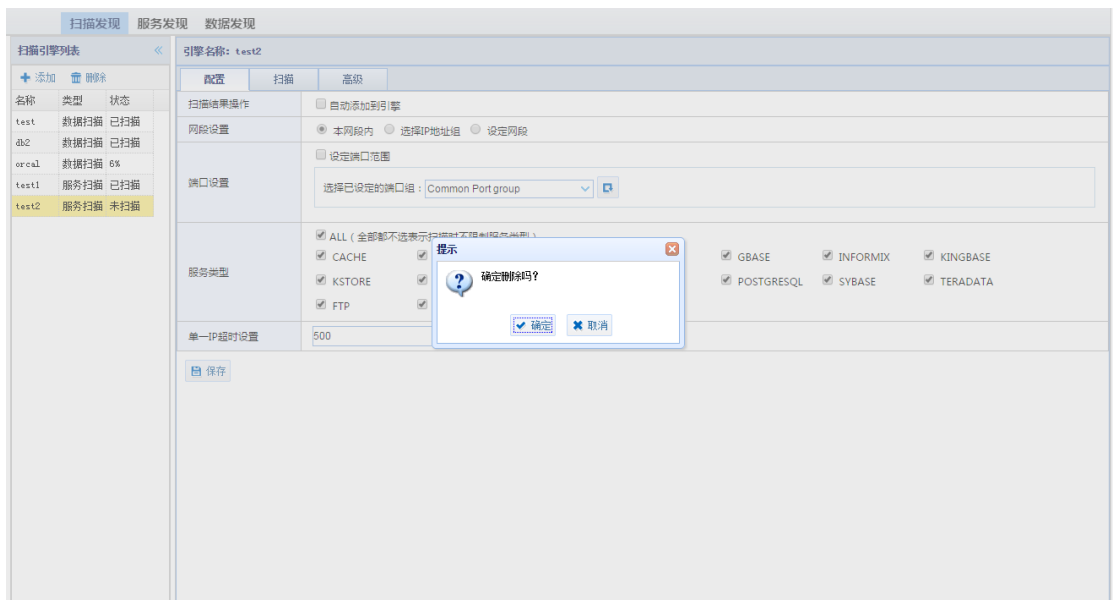
3.3.2.1 添加服务扫描

- 1.在扫描功能页面中，选择 “扫描发现” > “添加”。出现添加扫描引擎窗口；
- 2.在添加扫描引擎窗口中，选择扫描类型为：“服务扫描”
- 3.输入引擎名称，点击“确定” 按钮后完成添加扫描引擎。



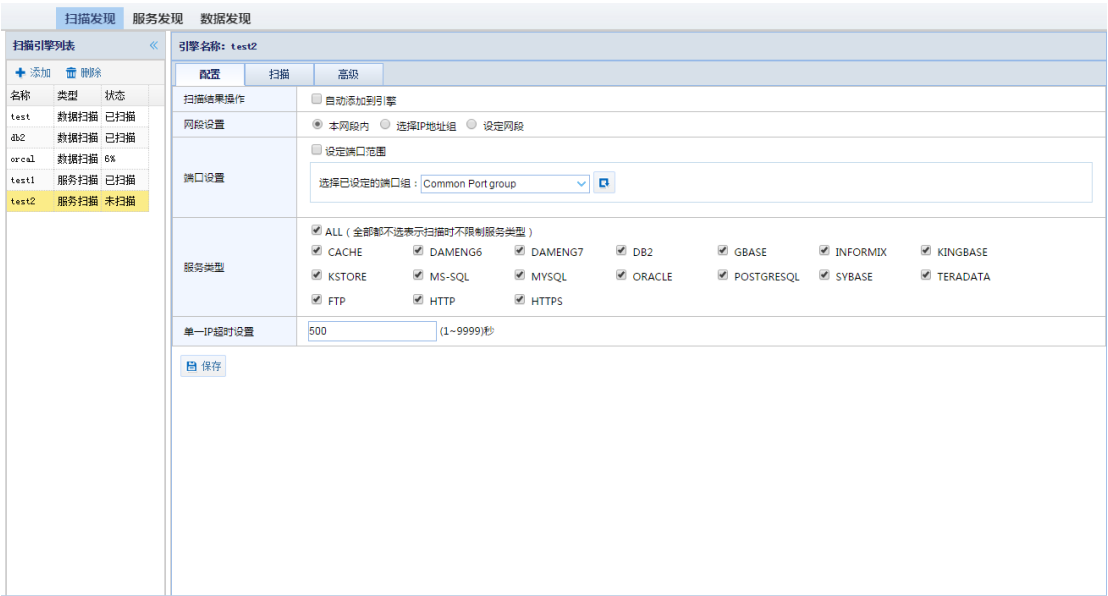
3.3.2.2 删除服务扫描

- 1.在扫描引擎列表中，选中要删除的服务扫描引擎，选择 “删除”。出现删除扫描引擎窗口；
- 2.在删除扫描引擎提示框中，点击“确定”按钮后删除选定的扫描引擎。



3.3.2.3 配置

扫描引擎配置界面如下图所示：



配置方法如下：

在扫描引擎列表中，选中已经添加的扫描引擎，出现引擎配置信息界面；

选择“配置”页面，配置如下信息：

扫描结果操作：

自动添加到引擎：扫描完成后自动添加到引擎列表中

网段设置：

本网段内：扫描当前网段；

选择 IP 地址组：扫描设置的 IP 地址组(在“高级”页面中设置 IP 地址组)；

设定网段：扫描设置的特定网段；

端口设置：设置扫描的端口(在“高级”页面中设置端口组)

服务类型：

ALL：表示以下所有服务类型；

CACHE、DAMEN6、DAMEN7、DB2、GBASE、INFORMIX、KINGBASE、KSTORE、MS-SQL、MYSQL、ORACLE、POSTGRESQL、SYBASE、TERADATA、FTP、HTTP、HTTPS

用户可根据需要选择上述所列任意组合的服务类型进行扫描；

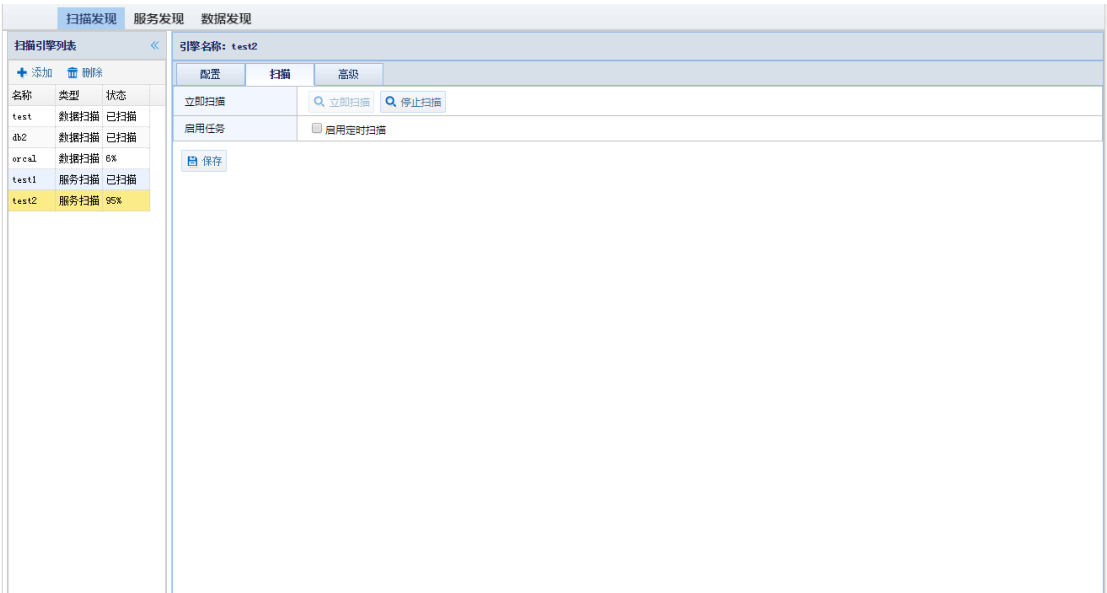
扫描超时设置：扫描超时返回时间，默认 500 毫秒。

配置完成后，点击“保存”按钮完成配置扫描引擎。

3.3.2.4 扫描

立即扫描

- 1.在扫描页面中，选择配置完成后的服务扫描引擎名称，点击“扫描”子页面进入服务扫描功能页面；
- 2.在扫描页面中，选择立即扫描，开始进行服务扫描，并实时显示扫描进度。



定时扫描

如果需要设置定时扫描功能，可以进行如下设置：

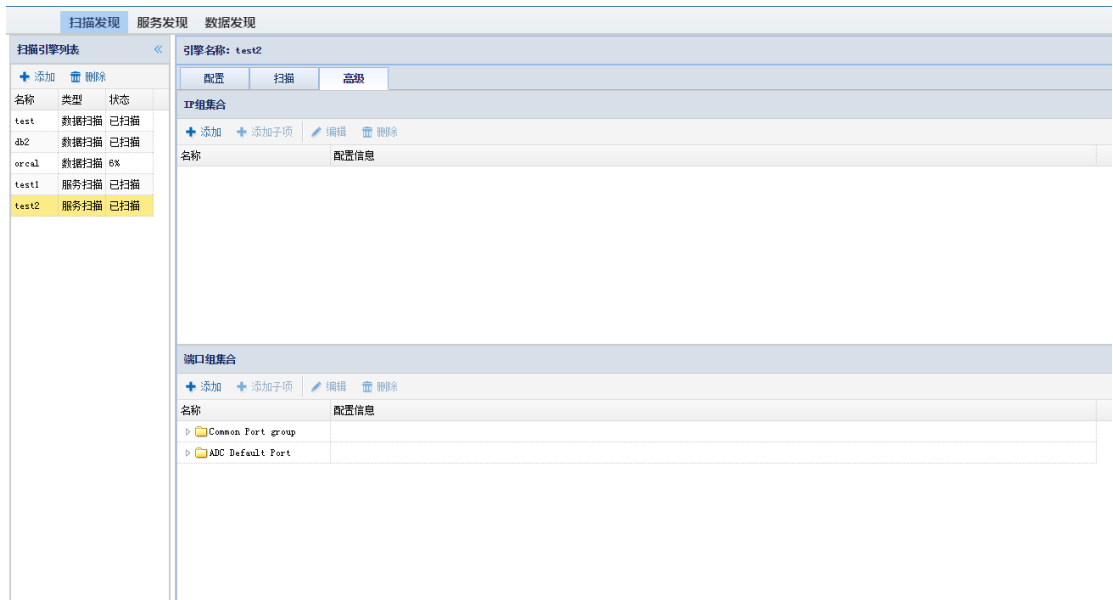
- 1.在扫描页面中，勾选“启用定时扫描”，展开定时扫描配置项；
- 2.设置定时扫描选项：
 - 频率设置：设置扫描只执行一次，或者是重复执行
 - 定时设置：设置扫描执行的时间和周期
 - 开始日期：设置定时扫描开始日期
- 3.设置完成后，点击“保存”后，系统会按照用户的设置，定时调度扫描服务进行扫描。



3.3.2.5 高级设置

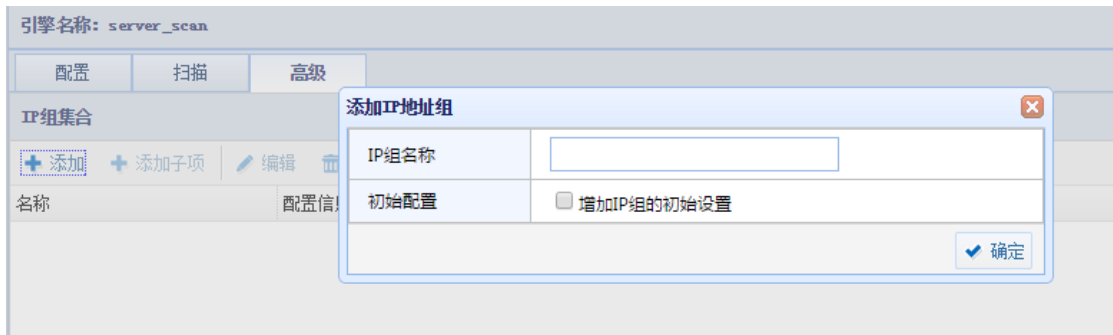
高级设置菜单中，设置 IP 组集合和端口组集合，在服务扫描配置时使用。

高级设置默认初始界面如下所示：

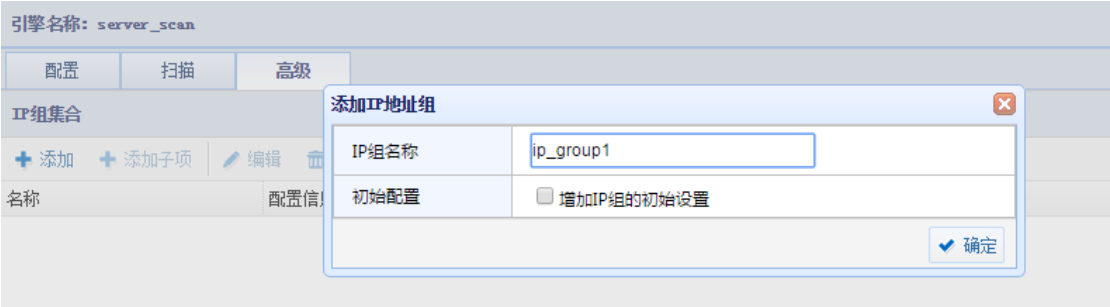


IP 组集合

IP 组集合添加初始页面如下图所示：



- 1.在扫描引擎列表页面中，添加的扫描引擎后，进入高级设置页面；
- 2.选择 IP 组集合> “添加”，弹出添加 IP 地址组窗口
- 3.输入 IP 组名称，点击 “确定” 按钮后完成添加扫描引擎。



4.选择成功添加的 IP 组集合名称后，点击“添加子项”，弹出如下图所示页面，根据需
要选择设置 IP 类型和 IP 地址后，点击“确定”按钮后完成添加 IP 组。



端口组集合

端口组集合初始页面如下图所示：

| 端口组集合 | |
|------------------------------|------|
| <div>+ 添加 + 添加子项 编辑 删除</div> | |
| 名称 | 配置信息 |
| ▶ Common Port group | |
| ▶ ADC Default Port | |

默认 Common Port group 和 ADC Default Port 两个集合可以包括常大多数见服务端
口；

如果用户需要自己定义端口组集合，操作步骤如下：

- 1.在扫描引擎列表页面中，选择添加的扫描引擎后，进入高级设置页面；
- 2.选择端口组集合> “添加”，弹出添加端口组窗口
- 3.输入“端口组名称”，点击“确定”按钮后完成添加扫描引擎。

端口组集合

+ 添加 + 添加子项 编辑 删除

| 名称 | 配置信息 |
|---------------------|------|
| ▶ Common Port group | |
| ▶ ADC Default Port | |

添加端口组

端口组名称

port_group

引用已有设置

▼

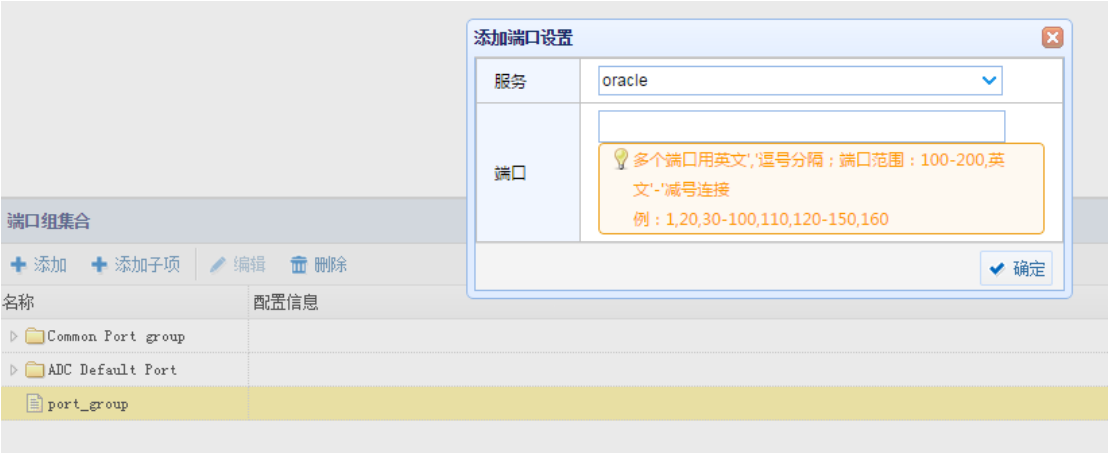
🔄

初始配置

☐ 增加端口组的初始设置

✓ 确定

4.选择成功添加的端口组集合名称后，点击 “添加子项”，弹出如下图所示页面，根据
需要选择设置服务类型和对应的端口后，点击“确定”按钮后完成添加。



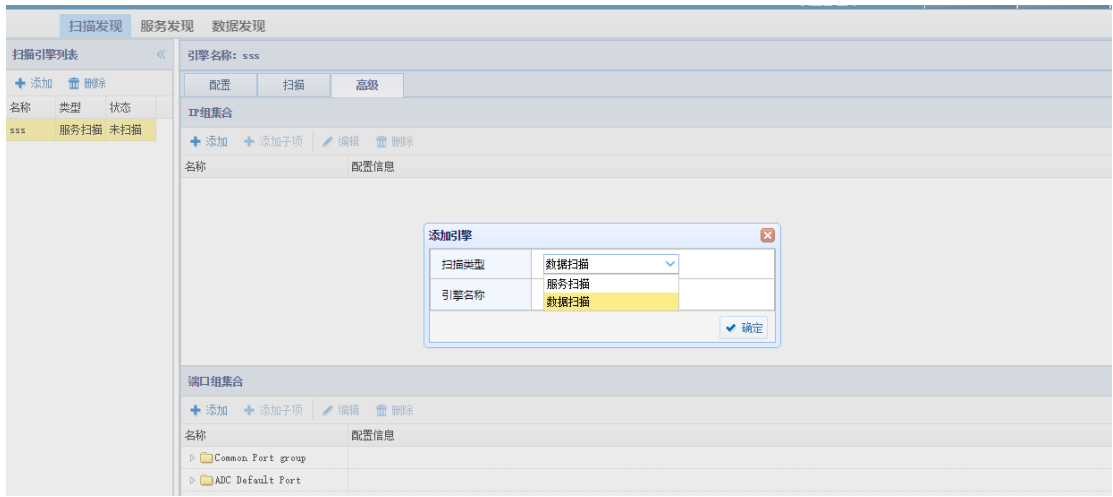
3.3.3 数据扫描

数据扫描模块对网络中的数据库进行扫描，并使用自定义算法对数据库中各种类型的数据进行分类。这些扫描信息可以用来保护针对敏感数据库的活动，并对此类活动进行审计。

对数据敏感表和字段扫描需要的配置包括确定在网络中搜索数据库和数据时使用的用户名、密码、数据库类型、service ID(MSSQL)，以及确定是否要将它们自动添加至引擎进行监测和保护。

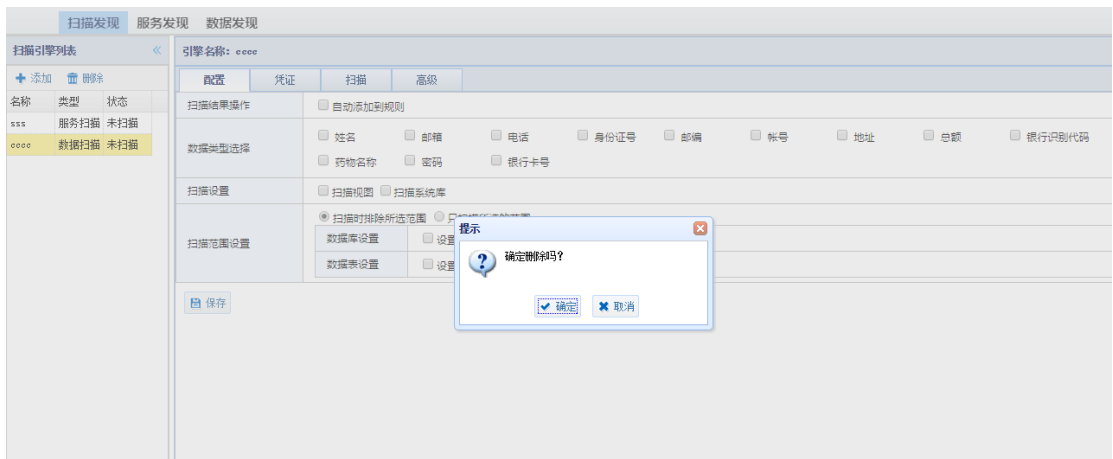
3.3.3.1 添加数据扫描引擎

- 1.在扫描功能页面中，点击“扫描发现”>“添加”。弹出添加引擎窗口；
- 2.在添加扫描引擎窗口中，选择扫描类型“数据扫描”；
- 3.输入引擎名称，点击确定按钮后完成添加扫描引擎。



3.3.3.2 删除数据扫描引擎

- 1.在扫描引擎列表中，选择要删除的数据扫描引擎；点击 “删除”。出现删除数据扫描引擎窗口；
- 2.在删除扫描引擎提示框中，点击“确定”按钮，删除选定的扫描引擎。



3.3.3.3 配置

- 1.在扫描引擎列表中，选择添加的数据扫描引擎。出现引擎配置信息界面；
- 2.配置条目如下：

扫描结果操作：勾选“自动添加到规则”后，扫描完成后自动添加到规则列表中；

数据类型选择：选择要扫描的数据类型，默认支持类型：姓名、邮箱、电话、身份证号、邮编、帐号、地址、总额、银行识别代码、药物名称、密码、银行卡号，用户可根据需要自定义扫描类型；

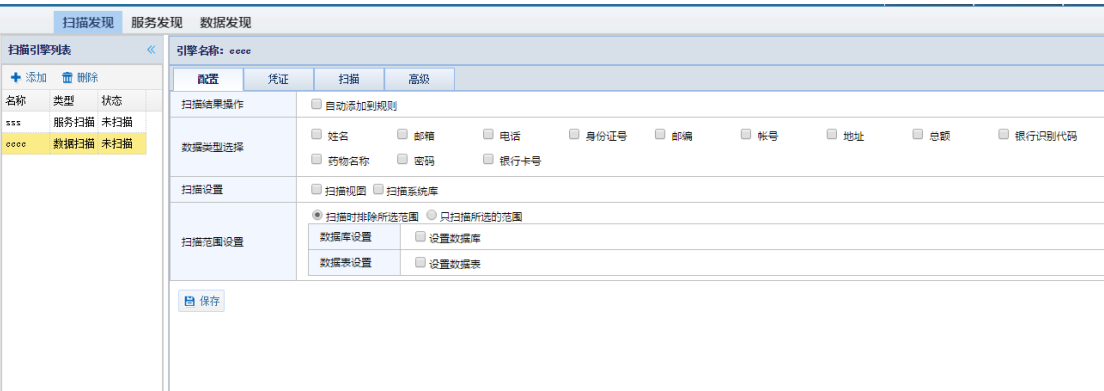
扫描设置：可根据用户数据需要，选择“扫描视图”或者“扫描系统库”；

扫描范围设置：设置扫描的范围；

数据库设置：设置数据库，手动添加需要扫描的数据库；

数据表设置：手动设置要扫描的数据表及其列名；

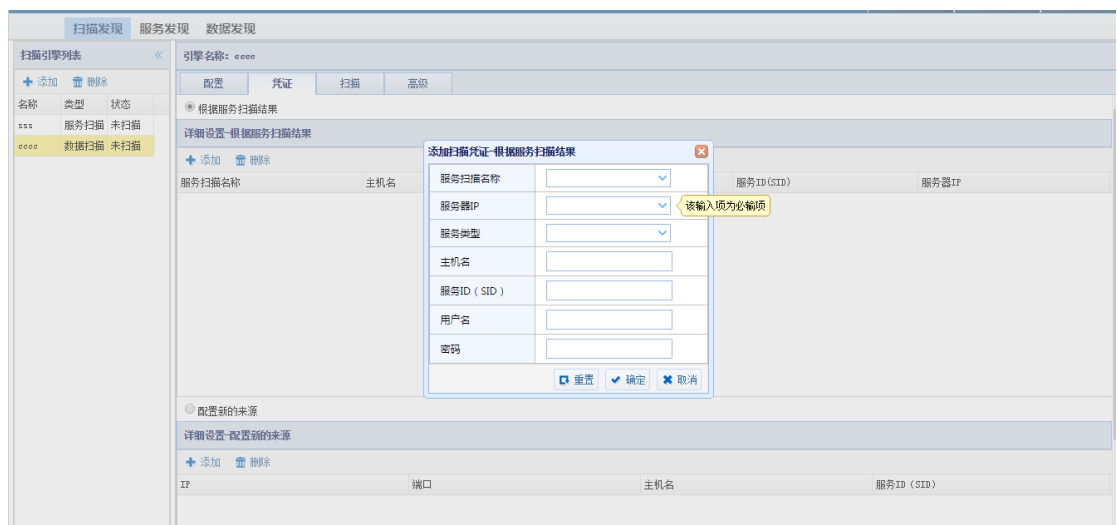
- 3.配置完成后，点击 “保存” 按钮完成配置数据扫描引擎。



3.3.3.4 凭证

凭证页面用来设置数据扫描时使用的数据库权限，方法如下：

- 1.在扫描引擎列表中，选择已添加的数据扫描引擎。出现引擎配置信息界面；
- 2.单击选择“凭证”页面，配置如下信息：
- 扫描源：可以“根据服务扫描结果”配置扫描源，也可自定义进“配置新的来源”进行配置，如下图所示：



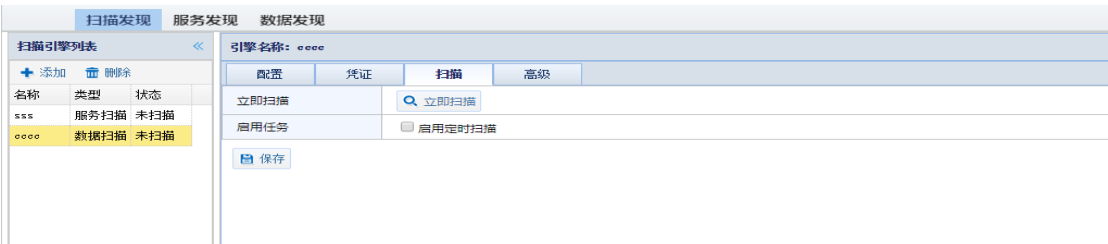
- 3.配置完成后（例如：配置新的来源），点击“保存”按钮完成配置凭证。



3.3.3.5 扫描

立即扫描

- 1.在“扫描发现”页面中，选择已添加的数据扫描引擎名称后，点击“扫描”配置页面，打开数据扫描页面；
- 2.在数据扫描页面中，选择“立即扫描”，开始进行数据扫描，并实时显示扫描进度。



定时扫描

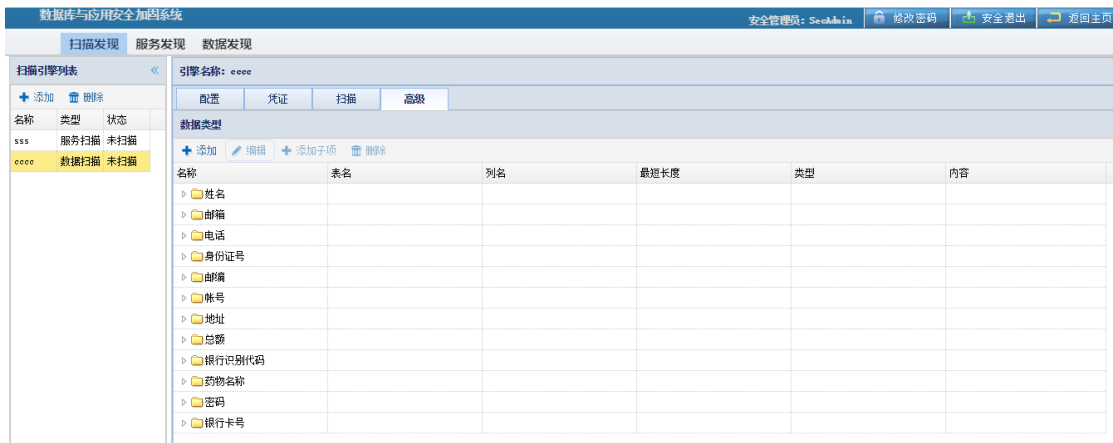
如果需要设置定时扫描功能，可以进行如下设置：

- 1. 在扫描页面中，勾选“启用定时扫描”页面展开定时扫描配置项；
- 2. 设置定时扫描选项：
 - 频率设置：设置扫描只执行一次，或者是重复执行
 - 定时设置：设置扫描执行的时间和周期
 - 开始日期：设置定时扫描开始日期
- 3. 设置完成后，点击“保存”后，系统会按照用户的设置，定时调度数据扫描服务进行扫描。

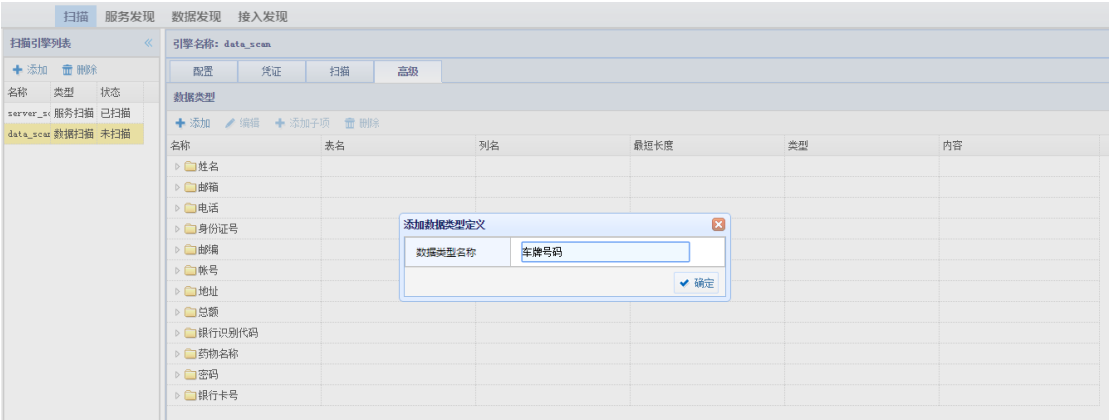


高级

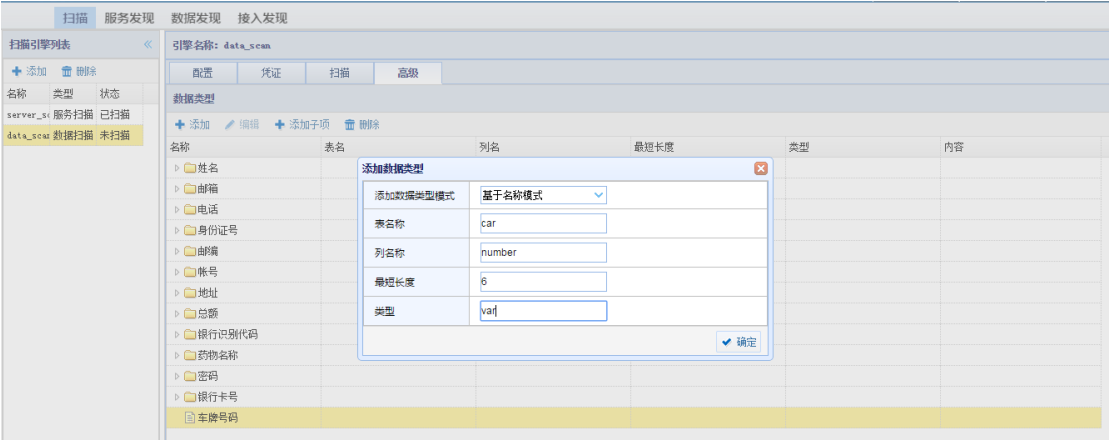
1. 在扫描功能页面中，选择相应的服务扫描引擎名称后，点击 “扫描发现” 页面。
点击数据扫描引擎，打开数据扫描页面；
2. 在数据扫描页面中，单击进入 “高级” 设置页面，如下图所示：



3. 在此页面中，用户可以添加需要关注的数据类型设置，在 “数据类型” 项中单击 “添加”，如下图所示：



4.选中自定义添加的数据类型，点击 “添加子项,” 设置数据类型的内容后，点击 “确定” 即可。



3.3.4 服务发现

3.3.4.1 服务发现结果

1.单击 “服务发现” > “服务器发现结果” 页面，页面显示服务发现的扫描结果，如下图所示：

扫描

服务发现

数据发现

接入发现

服务器发现结果

数据

服务类型

操作系统类型

服务发现

开始时间

结束时间

任务名称

服务器IP

服务器名称

Q 查询

重置

导出

| 扫描时间 | 服务器IP | 服务器端口 | 服务器名 | 状态 | 版本信息 | 操作系统 | 操作系统版本 | 加入加粗点 | |
|------|------------------|--------------|-------|--------|--------|-------------------------------------|-------------------|----------------------|---------|
| 1 | 2015-04-03 13:43 | C:172.16.4.9 | 443 | HTTPS | open | TLS 1.0 | Linux | 2.6.X | - |
| 2 | 2015-04-03 13:43 | C:172.16.4.1 | 21 | FTP | open | FileZilla ftpd 0.9.41 beta | Microsoft Windows | 7[2008 | - |
| 3 | 2015-04-03 13:43 | 172.16.4.1 | 1433 | MS-SQL | open | Microsoft SQL Server 2008 10.0.1600 | Microsoft Windows | 7[2008 | + 加入加粗点 |
| 4 | 2015-04-03 13:43 | 172.16.4.1 | 1521 | ORACLE | open | Oracle TNS Listener 11.1.0.6.0 (for | Microsoft Windows | 7[2008 | + 加入加粗点 |
| 5 | 2015-04-02 20:01 | C:172.16.4.1 | 3306 | MYSQL | open | MySQL 5.5.23 | Microsoft Windows | 7[2008 | + 加入加粗点 |
| 6 | 2015-04-03 13:43 | 172.16.4.1 | 523 | DB2 | open | IBM DB2 Database Server 9.07.6 | Linux | 2.6.X | + 加入加粗点 |
| 7 | 2015-04-03 13:47 | 4 172.16.4.1 | 443 | HTTPS | open | SSLv3 | Microsoft Windows | 7[2008 | - |
| 8 | 2015-04-03 13:47 | 4 172.16.4.1 | 3306 | MYSQL | open | MySQL 5.5.3-m3-community | Microsoft Windows | 2003 | + 加入加粗点 |
| 9 | 2015-04-03 13:47 | 4 172.16.4.1 | 443 | HTTPS | open | TLS 1.0 | Linux | 2.6.X | - |
| 10 | 2015-04-03 13:47 | 4 172.16.4.1 | 443 | HTTPS | open | TLS 1.0 | Linux | 2.6.X | - |
| 11 | 2015-04-03 13:47 | 4 172.16.4.2 | 443 | HTTPS | open | TLS 1.0 | Linux | 2.6.X | - |
| 12 | 2015-04-03 13:47 | 4 172.16.4.2 | 3306 | MYSQL | open | MySQL 5.1.73 | Linux | 2.6.X | + 加入加粗点 |
| 13 | 2015-04-03 13:47 | 5 172.16.4.2 | 8080 | HTTP | open | Apache Tomcat/Coyote JSP engine 1.1 | Linux | 2.6.X | - |
| 14 | 2015-04-03 13:47 | 5 172.16.4.2 | 443 | HTTPS | open | SSLv3 | Microsoft Windows | 7[2008 | - |
| 15 | 2015-04-03 13:47 | 5 172.16.4.2 | 523 | DB2 | open | IBM DB2 Database Server 9.07.6 | Microsoft Windows | 7[2008 | + 加入加粗点 |
| 16 | 2015-04-03 13:47 | 5 172.16.4.2 | 8080 | HTTP | open | Apache httpd 2.2.22 (Win32) | Microsoft Windows | 7[2008 | - |
| 17 | 2015-04-03 13:47 | 5 172.16.4.2 | 50000 | DB2 | open | IBM DB2 Database Server Q2802/RT64 | Microsoft Windows | 7[2008 | + 加入加粗点 |
| 18 | 2015-04-03 13:48 | 5 172.16.4.2 | 443 | HTTPS | open | TLS 1.0 | Linux | 2.6.X[3.X | - |
| 19 | 2015-04-02 16:48 | 5 172.16.0.1 | 80 | HTTP | open | unknown | unknown os | 2.4.X[2.6.X,... | - |
| 20 | 2015-04-02 16:48 | 5 172.16.0.1 | 443 | HTTPS | open | OpenSSL (SSLv3) | unknown os | 2.4.X[2.6.X,... | - |
| 21 | 2015-04-02 15:38 | 4 172.16.0.2 | 21 | FTP | closed | unknown | unknown os | 2.6.X[3.X[4.X,...3.X | - |
| 22 | 2015-04-02 15:38 | 4 172.16.0.2 | 80 | HTTP | closed | unknown | unknown os | 2.6.X[3.X[4.X,...3.X | - |
| 23 | 2015-04-02 15:38 | 4 172.16.0.2 | 443 | HTTPS | open | TLS 1.0 | unknown os | 2.6.X[3.X[4.X,...3.X | - |
| 24 | 2015-04-02 15:38 | 4 172.16.0.2 | 1433 | MS-SQL | closed | unknown | unknown os | 2.6.X[3.X[4.X,...3.X | + 加入加粗点 |
| 25 | 2015-04-02 15:38 | 4 172.16.0.2 | 1521 | ORACLE | closed | unknown | unknown os | 2.6.X[3.X[4.X,...3.X | + 加入加粗点 |
| 26 | 2015-04-02 15:38 | 4 172.16.0.2 | 3306 | MYSQL | closed | unknown | unknown os | 2.6.X[3.X[4.X,...3.X | + 加入加粗点 |
| 27 | 2015-04-02 15:38 | 5 172.16.0.2 | 50000 | DB2 | closed | unknown | unknown os | 2.6.X[3.X[4.X,...3.X | + 加入加粗点 |
| 28 | 2015-04-02 16:48 | 5 172.16.0.3 | 21 | FTP | open | FileZilla ftpd 0.9.41 beta | unknown os | 2.6.X[3.X[4.X,...3.X | - |

30

1

共15页

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

显示1到10, 共27

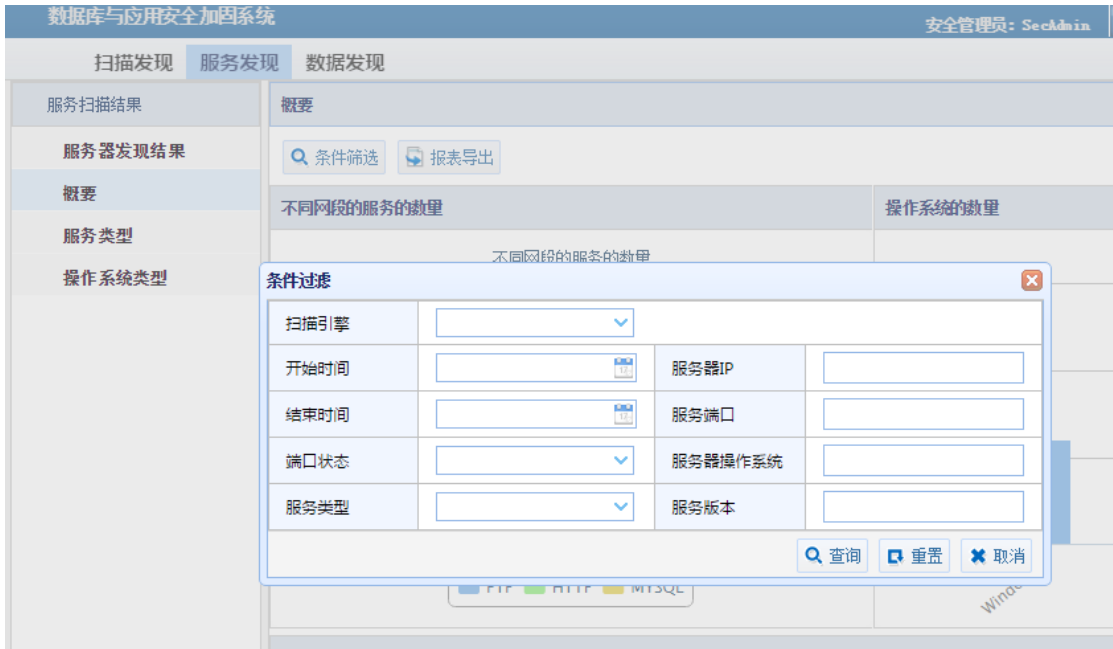
2.用户可以按需求定制查询扫描发现的服务；

3.3.4.2 概要

1.单击 “服务发现” > “概要” 页面，页面显示服务发现的概要信息，如下图所示：



2.用户可以按条件进行过滤筛选 点击“概要”>“条件筛选”



3.用户可以导出报表，点击“概要”>“报表导出”



3.3.4.3 服务类型

1.单击“服务发现”>“服务类型”页面，页面显示服务发现的服务类型信息，如下图所示：



2.用户可以按条件进行过滤筛选 点击“服务类型”>“条件筛选”

3.用户可以导出报表，点击“服务类型”>“报表导出”。

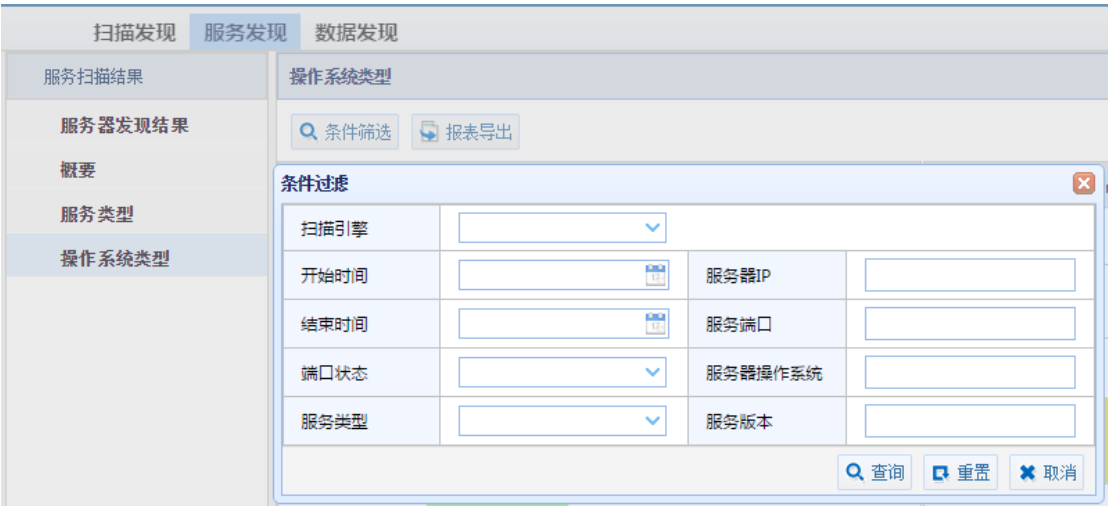


3.3.4.4 操作系统类型

1.单击“服务发现”>“操作系统类型”页面，页面显示服务发现的操作系统类型信息，如下图所示：



2.用户可以按条件进行过滤筛选，点击“操作系统类型”>“条件筛选”。



3.用户可以导出报表，点击“操作系统类型”>“报表导出”。



3.3.5 数据发现

3.3.5.1 数据发现结果

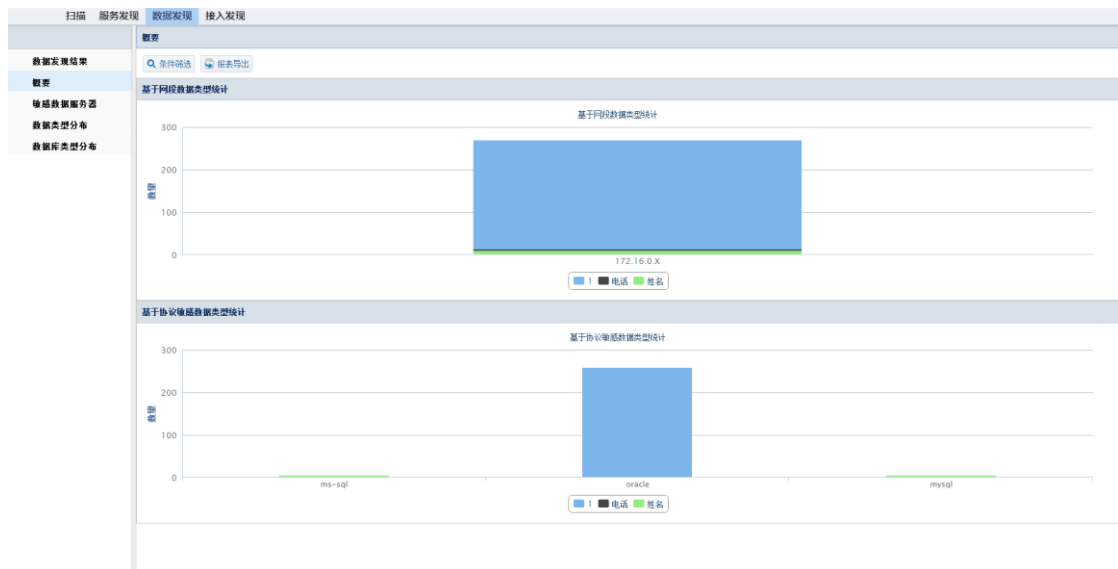
1.单击“数据发现”>“数据发现结果”页面，页面显示数据发现的扫描结果，如下图所示：

| 扫描 服务发现 数据发现 接入发现 | | | | | | | | | |
|---|------------------------|-------------|-------|------|------|-------------|-------|--------|----|
| 数据扫描结果-表数据 | | | | | | | | | |
| 数据发现结果 概要 扫描数据库引擎 数据库类型分布 数据库类型分布 | 开始时间 | | 结束时间 | | 任务名称 | | | | |
| | 服务器IP | | 服务器类型 | | Q 查询 | 重置 | 导出 | 保存当前策略 | |
| | 时间 | 服务器IP | 主机名 | 数据库 | 模式名 | 表 | 表类型 | 索引类型 | 备注 |
| | 1 2015-04-02 18:19:04 | 172.16.0.13 | | orcl | SYS | USERS | TABLE | ORACLE | ☑ |
| | 2 2015-04-02 18:19:04 | 172.16.0.13 | | orcl | SYS | UNDO\$ | TABLE | ORACLE | ☑ |
| | 3 2015-04-02 18:19:04 | 172.16.0.13 | | orcl | SYS | MTAB\$ | TABLE | ORACLE | ☑ |
| | 4 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | VIEWTABLE\$ | TABLE | ORACLE | ☑ |
| | 5 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | ATTACH\$ | TABLE | ORACLE | ☑ |
| | 6 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | CIL\$ | TABLE | ORACLE | ☑ |
| | 7 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | CINS | TABLE | ORACLE | ☑ |
| | 8 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | TIS | TABLE | ORACLE | ☑ |
| | 9 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | ORIS | TABLE | ORACLE | ☑ |
| | 10 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | VIEWS\$ | TABLE | ORACLE | ☑ |
| | 11 2015-04-02 18:19:05 | 172.16.0.13 | | orcl | SYS | SYNS | TABLE | ORACLE | ☑ |
| | 12 2015-04-02 18:19:06 | 172.16.0.13 | | orcl | SYS | PROFANES | TABLE | ORACLE | ☑ |
| | 13 2015-04-02 18:19:06 | 172.16.0.13 | | orcl | SYS | LINKS | TABLE | ORACLE | ☑ |
| | 14 2015-04-02 18:19:06 | 172.16.0.13 | | orcl | SYS | PROFS | TABLE | ORACLE | ☑ |
| | 15 2015-04-02 18:19:06 | 172.16.0.13 | | orcl | SYS | INDEXP | TABLE | ORACLE | ☑ |
| 显示3条6% 共283记录 | | | | | | | | | |
| 数据扫描结果-列数据 | | | | | | | | | |
| 列名称 列数据类型 长度 扫描数据类型 扫描模式 | | | | | | | | | |

2.用户可以按需求定制查询扫描发现的服务。

3.3.5.2 概要

1.单击“数据发现”>“概要”页面，页面显示如下图所示：



2.用户可以按条件进行过滤筛选，点击“概要”>“条件筛选”。

条件过滤

| 扫描引擎 | 数据类型 |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |
| 开始时间 | 服务器IP |
| <input type="text"/> | <input type="text"/> |
| 结束时间 | 服务端口 |
| <input type="text"/> | <input type="text"/> |
| 服务类型 | 主机名 |
| <input type="text"/> | <input type="text"/> |
| DB名称 | Schema名称 |
| <input type="text"/> | <input type="text"/> |
| 表名称 | 表类型 |
| <input type="text"/> | <input type="text"/> |
| 列名称 | 列类型 |
| <input type="text"/> | <input type="text"/> |
| 列最小长度 | 扫描模式 |
| <input type="text"/> | <input type="text"/> |

查询 重置 取消

3.用户可以导出报表，点击“概要”>“报表导出”。

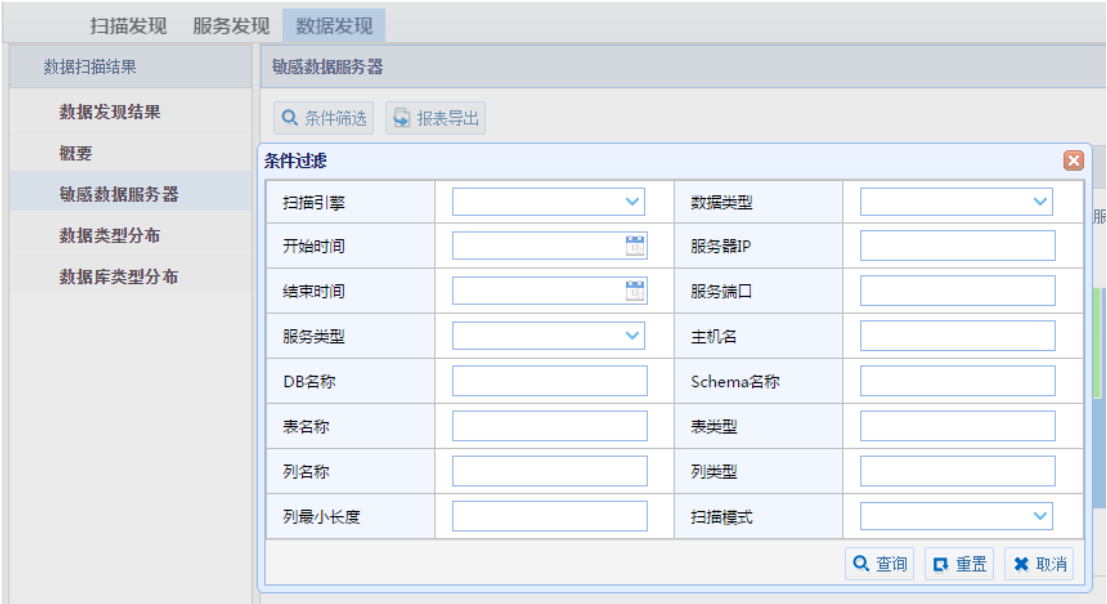


3.3.5.3 敏感数据服务器

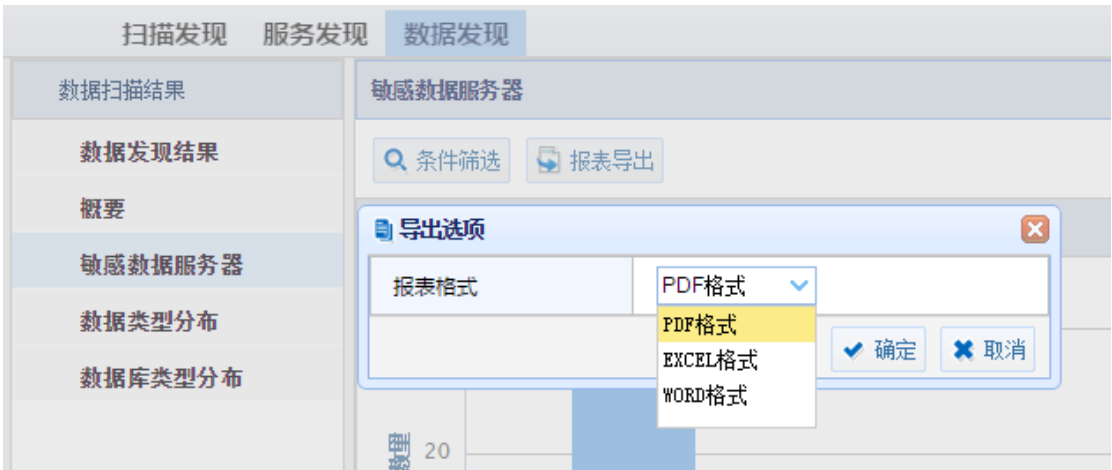
1.单击 “数据发现” > “敏感数据服务器” 页面，页面显示如下图所示：



2.用户可以按条件进行过滤筛选，点击 “敏感数据服务器” > “条件筛选”。

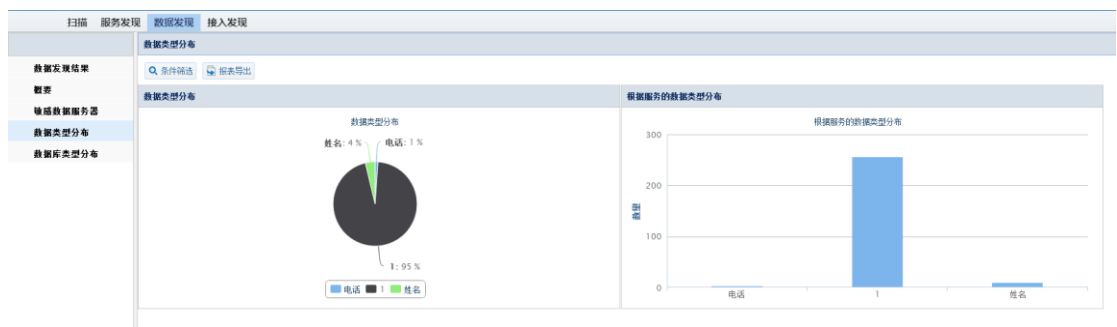


3.用户可以导出报表，点击“敏感数据服务器” > “报表导出”。



3.3.5.4 数据类型分布

1.单击“数据发现” > “数据类型分布” 页面，页面显示如下图所示：



2.用户可以按条件进行过滤筛选，点击“数据类型分布”>“条件筛选”。

The screenshot shows the 'Condition Filter' (条件过滤) dialog box, which is used to refine search results. It features a table with the following fields and input types:

| Field | Input Type | Field | Input Type |
|-------|------------------|----------|------------|
| 扫描引擎 | Dropdown | 数据类型 | Dropdown |
| 开始时间 | Date/Time Picker | 服务器IP | Text |
| 结束时间 | Date/Time Picker | 服务端口 | Text |
| 服务类型 | Dropdown | 主机名 | Text |
| DB名称 | Text | Schema名称 | Text |
| 表名称 | Text | 表类型 | Text |
| 列名称 | Text | 列类型 | Text |
| 列最小长度 | Text | 扫描模式 | Dropdown |

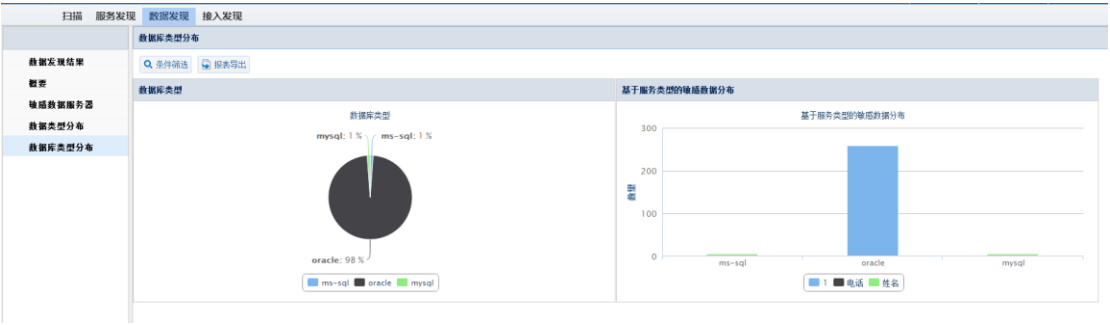
At the bottom right of the dialog, there are three buttons: 查询 (Query), 重置 (Reset), and 取消 (Cancel).

3.用户可以导出报表，点击“数据类型分布”>“报表导出”。



3.3.5.5 数据库类型分布

1.单击“数据发现”>“数据库类型分布”页面，页面显示如下图所示：

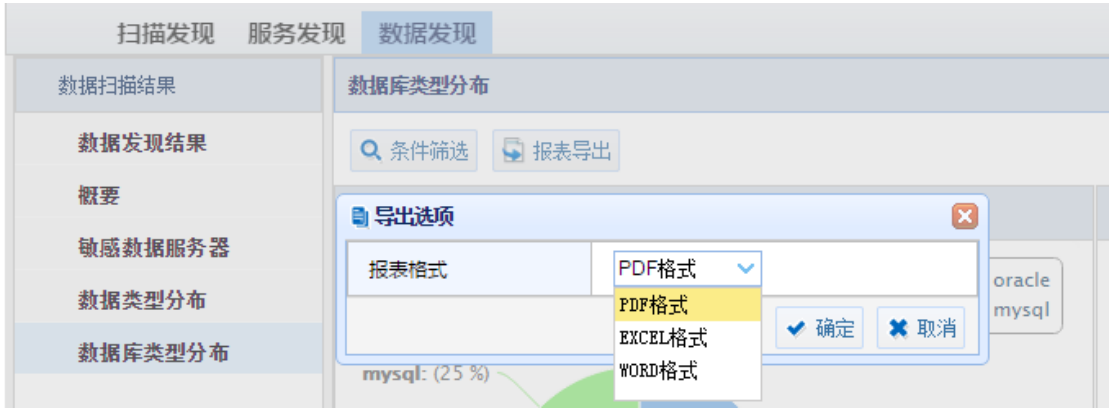


2.

用户可以按条件进行过滤筛选，点击“数据库类型分布”>“条件筛选”。



3. 用户可以导出报表，点击“数据库类型分布” > “报表导出”。



3.4 风险扫描

所属用户：SecAdmin。

数据库系统是一个复杂的系统资料，数据库存在许多风险，其中不少是致命的缺陷和漏洞。一旦遭到攻击，攻击者可能以 DBA 的身份进入数据库系统，也可能进入操作系统，下载整个数据库文件。为此本系统提供风险扫描模块，为用户能更早的发现风险与漏洞。

3.4.1 添加风险扫描

进入 “通用配置” > “选择引擎”，点击添加风险扫描按钮，如下图所示。

数据库引擎

用户管理

数据库引擎列表

+ 添加

编辑

Q 自动发现

| 名称 | 类型 | IP | 端口 | 缺省数据库 | 审计防火墙 | 状态监控 | 风险扫描 |
|----------------------|----------|----------------|-------|--------|---------------------------------------|---------------------------------------|----------------------------|
| 172.17.200.190:60000 | DB2 | 172.17.200.190 | 60000 | test1 | <div><div>详情</div><div>删除</div></div> | <div><div>+ 添加</div></div> | <div><div>+ 添加</div></div> |
| 172.17.200.194:3306 | MYSQL | 172.17.200.194 | 3306 | testdb | <div><div>详情</div><div>删除</div></div> | <div><div>详情</div><div>删除</div></div> | - |
| 192.168.0.98:3306 | my MYSQL | 192.168.0.98 | 3306 | mysql | <div><div>详情</div><div>删除</div></div> | <div><div>+ 添加</div></div> | - |

点击添加按钮后，需输入如下信息：

名称：该风险扫描的名称。

用户名：该数据库管理员的用户名。

密码：该数据库管理员的密码。

缺省数据库：系统默认的数据库。

以下信息输入完成后，点击“确定”后，完成风险扫描的添加。如下图所示。

添加数据库扫描

名称

172.17.200.190:60000/test1

用户名

myadm

密码

.....

缺省数据库

test1

确定

3.4.2 引擎列表

选择该引擎可以进行“删除”操作。

3.4.3 数据库风险扫描

3.4.3.1 扫描策略

进入“风险扫描” > “扫描策略”

扫描策略：扫描数据库时的策略，系统默认有“授权”、“系统”两个大的策略组，每个大组包含了相应的策略，用户可根据自身需要选择相应的策略，策略选择完成后进行扫描，系统将会根据所选的策略扫描出相应的风险。如下图所示：



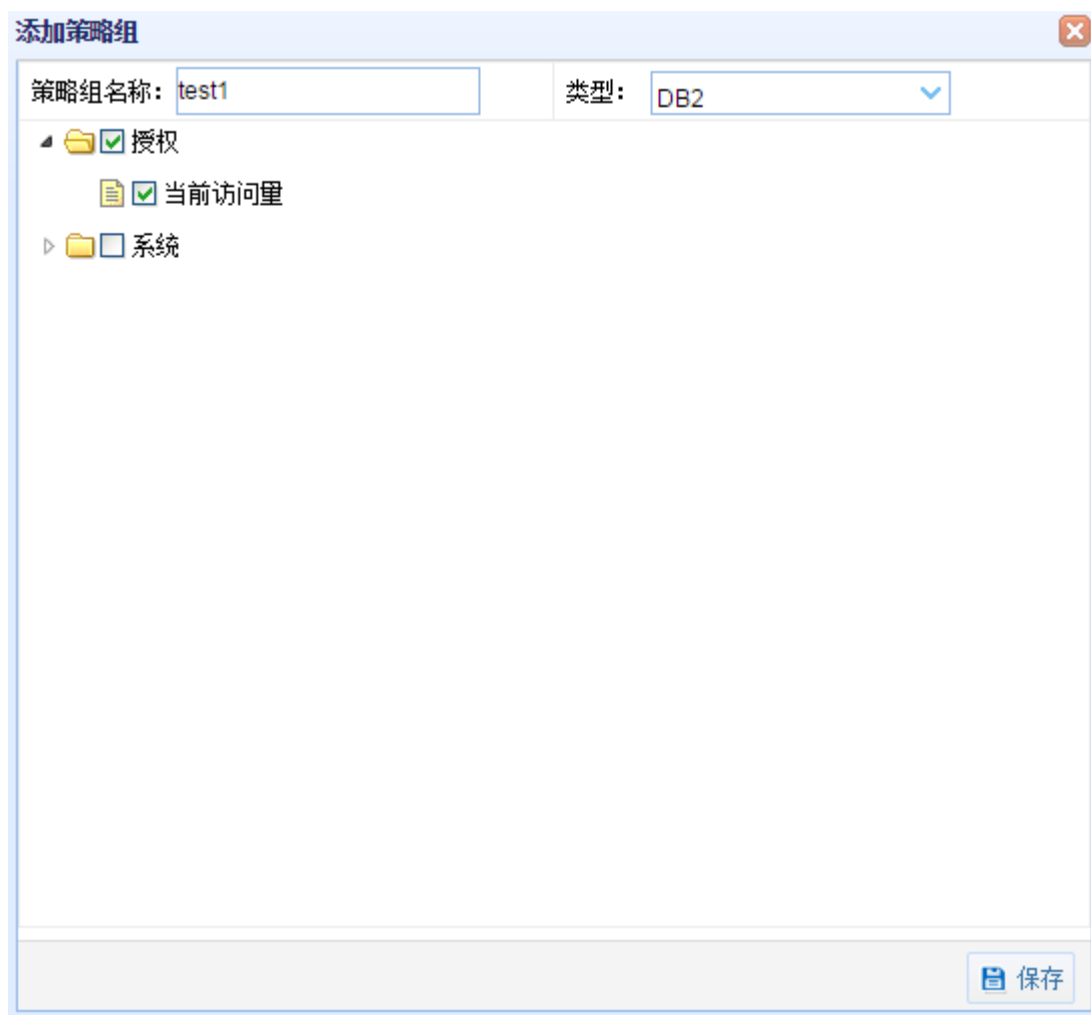
添加策略组

点击“添加策略组”后，弹出添加策略组窗口。

策略名称：该策略组的名称。

类型：该数据库的类型。

勾选 “授权”、“系统” 两个大的策略组中需要添加的策略，点击保存，完成对该策略组的添加。如下图所示：



授权

当前访问量

风险描述：连接量过大可能导致服务运行缓慢甚至崩溃，也有可能是恶意攻击，管理员需及时查看原因。

产生原因：同一时间访问数据库量过多

系统

cat_cache 溢出

风险描述：检测 cat_cache 是否溢出。cat_cache 溢出将可能导致信息丢失并加大被攻击的风险。

产生原因：缓冲区太小或被恶意操作。

cat_cache 堆溢出

风险描述：cat_cache 堆溢出将可能导致信息丢失并加大被攻击的风险。

产生原因：缓冲区太小或被恶意操作。

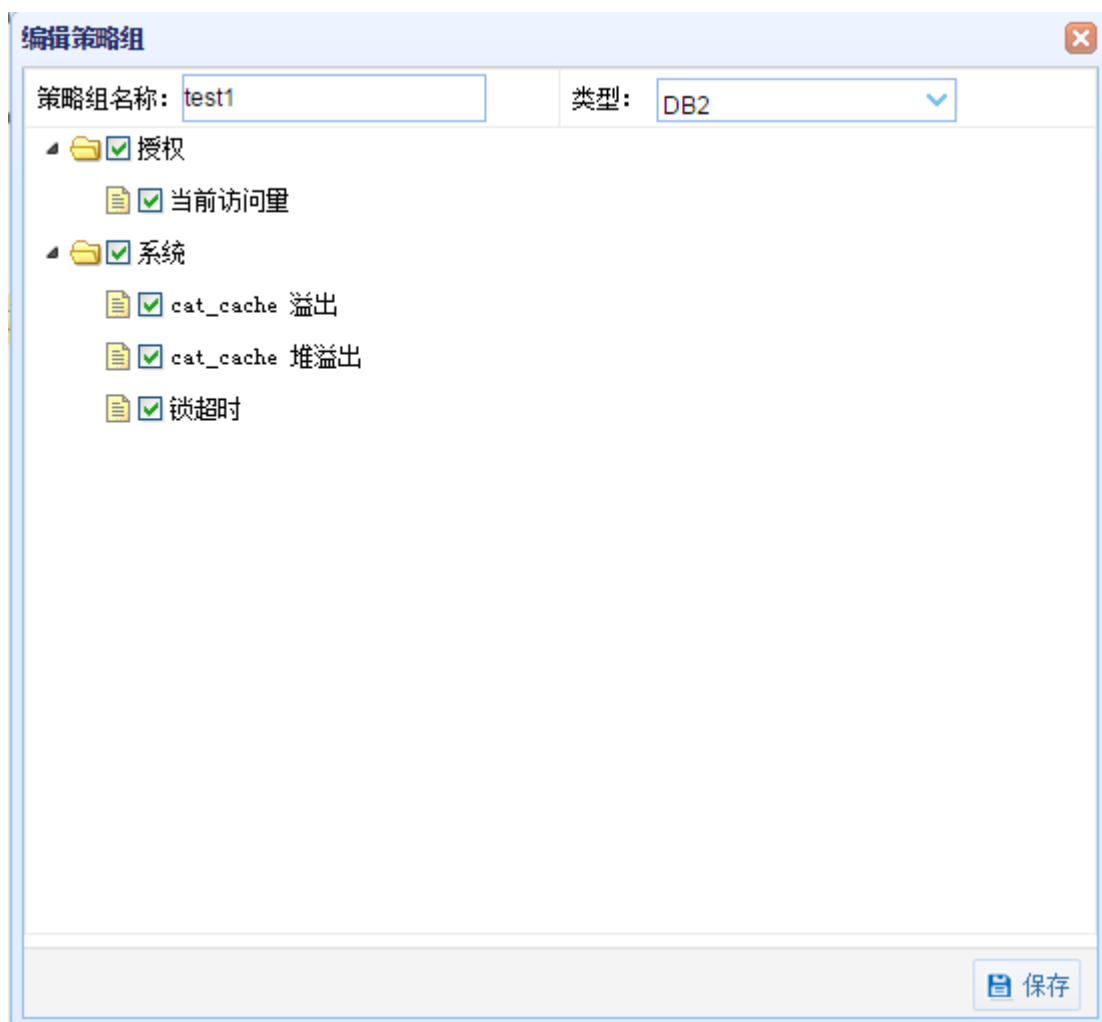
锁超时

风险描述：锁超时可能一直占用系统资源而导致无法返回结果。

产生原因：当一个进程访问数据库表或者字段的时候，另一个程序正在执行带锁的访问（比如修改数据），那么这个进程就会等待，当等待很久锁还没有解除就会锁超时，报告一个系统错误，拒绝执行相应 SQL 操作。

编辑策略组

编辑策略组：对已添加的策略组进行调整的操作，可以再进行策略的添加、删除操作以及对策略组名称的修改。如下图所示：



策略参数配置

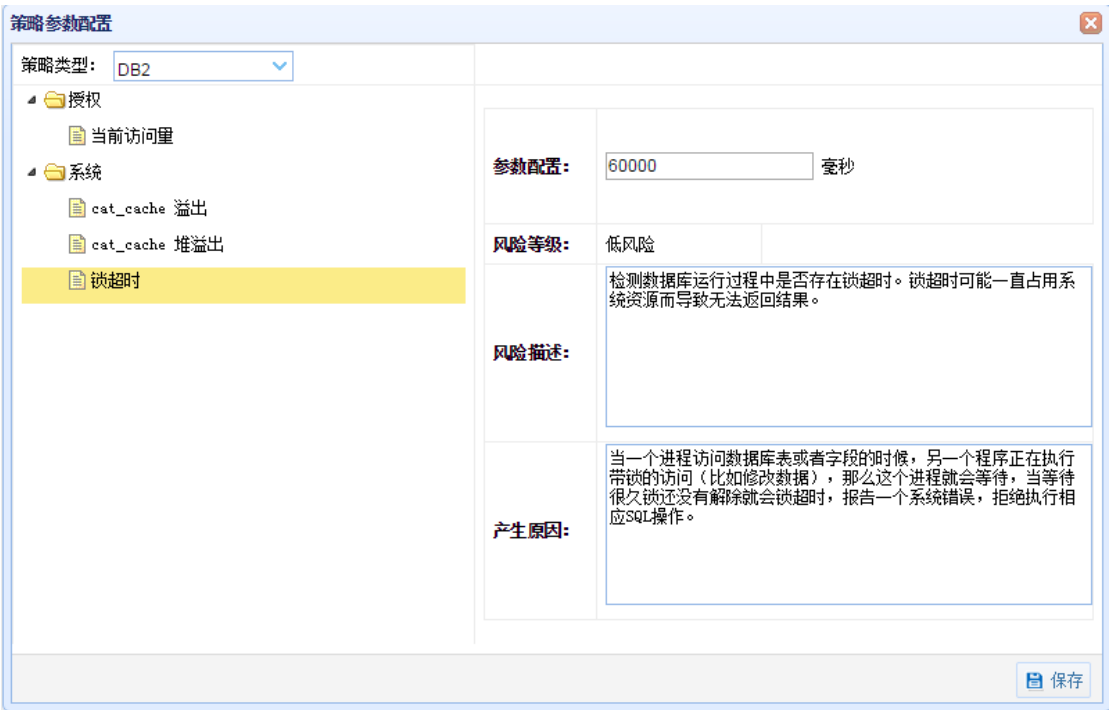
参数配置：对相应的策略进行参数配置，有的策略会显示无需参数配置。

风险等级：系统对该风险级别等级的评定。

风险描述：描述该风险的具体情况以及解决的一些建议。

产生原因：描述产生该风险的原因。

点击“保存”后，完成策略参数的配置。再此进行扫描，将会按照新的策略来扫描数据库，发现相应的风险。如下图所示：



风险扫描

这个模块是在前面策略组添加、策略组编辑以及策略组参数配置操作完成后，最终进行的最重要，也是本模块最核心的操作，即风险扫描。

用户：数据库管理员的用户名。

风险策略：即添加编辑后的策略组名称。

点击“扫描”弹出风险扫描窗口。如下图所示：



弱口令检测

弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，因此不推荐用户使用。

点击“开始检测，”将会显示出相应的弱口令。

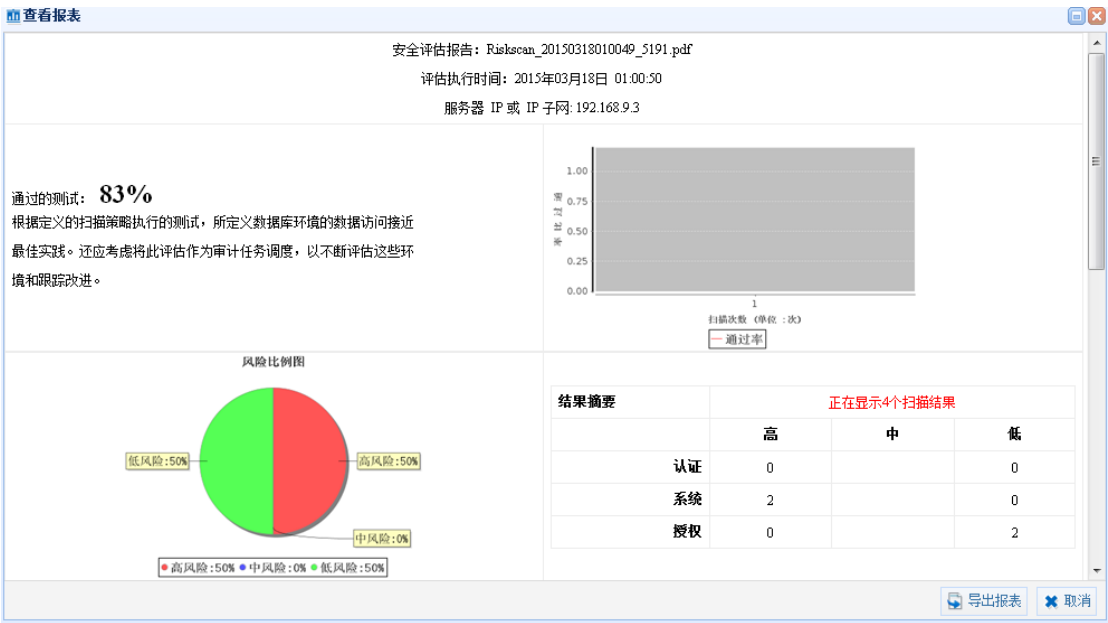
3.4.3.2 历史报表

报表就是用表格、图表等格式来动态显示数据，可以用公式表示为：“报表 = 多样的格式 + 动态的数据”。历史报表记录了风险扫描的详细信息。提供给查询的人更加详细的信息，以便对当时存在的风险有一个直观形象的了解。如下图所示：

| 扫描策略 | | | | |
|----------------------------------|-------------|--------|-----------|---------------------|
| 历史报表 | | | | |
| 查看报表 | 删除报表 | | | |
| 报表 | IP | 数据库名 | 数据库类型 | 生成时间 |
| Riskscan_20150318010049_5191.pdf | 192.168.9.3 | master | SQLSERVER | 2015-03-18 01:00:50 |
| Riskscan_20150304215648_6757.pdf | 192.168.1.3 | master | SQLSERVER | 2015-03-04 21:56:49 |
| Riskscan_20150304181634_4819.pdf | 192.168.1.3 | master | SQLSERVER | 2015-03-04 18:16:34 |

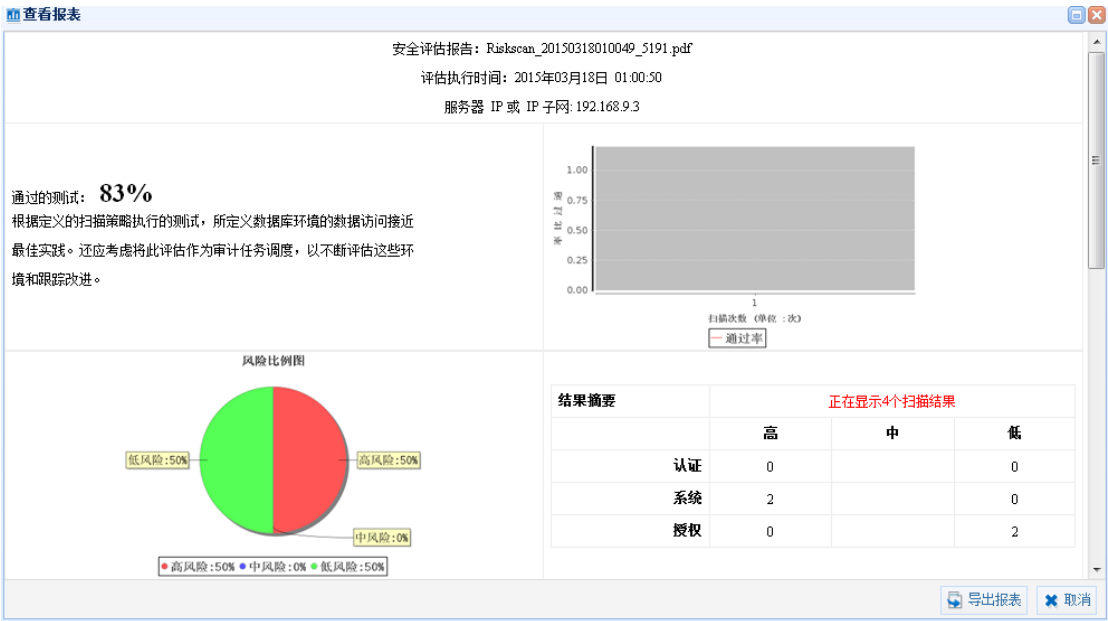
查看报表

选择需要查询的报表，点击 “查看报表”，将会显示该报表的所有详细信息。如下图所示：



导出报表

点击 “导出报表”，可将该报表下载保存起来，以便之后的查看。如下图所示：



删除报表

选择需要删除的报表, 点击 “删除报表”, 即可删除该报表。

3.5 数据库状态监控

所属用户: SecAdmin。

数据库状态监控可以看到数据库服务器当前的运行信息, 包括服务器的运行时间、内存及存储的使用情况等。从而及时发现服务器的异常情况, 更好的维护数据库服务器。

3.5.1 添加数据库状态监控

进入 “通用配置” > “选择引擎”, 点击状态监控的 “添加” 按钮。如下图所示:

| 名称 | 类型 | IP | 端口 | 缺省数据库 | 所属控制器 | 审计与防火墙 | 状态监控 |
|------------------------|-----------|--------------|------|--------|-----------|---------------------------------------|----------------------|
| 192.168.1.45:1521/orcl | ORACLE | 192.168.1.45 | 1521 | orcl | localhost | 详情 删除 | + 添加 |
| 192.168.1.9:1433/maste | SQLSERVER | 192.168.1.9 | 1433 | master | localhost | + 添加 | + 添加 |

点击“添加”按钮后，需输入如下信息：

名称：该状态监控的名称。

用户名：该数据库管理员的用户名。

密码：该数据库管理员的密码。

缺省数据库：系统默认的数据库。

已下信息输入完成后，点击“确定”后，完成数据库状态监控的添加。如下图所示：

添加数据库监控

名称

192.168.1.11:1433/master

用户名

密码

缺省数据库

master

确定

3.5.2 引擎列表

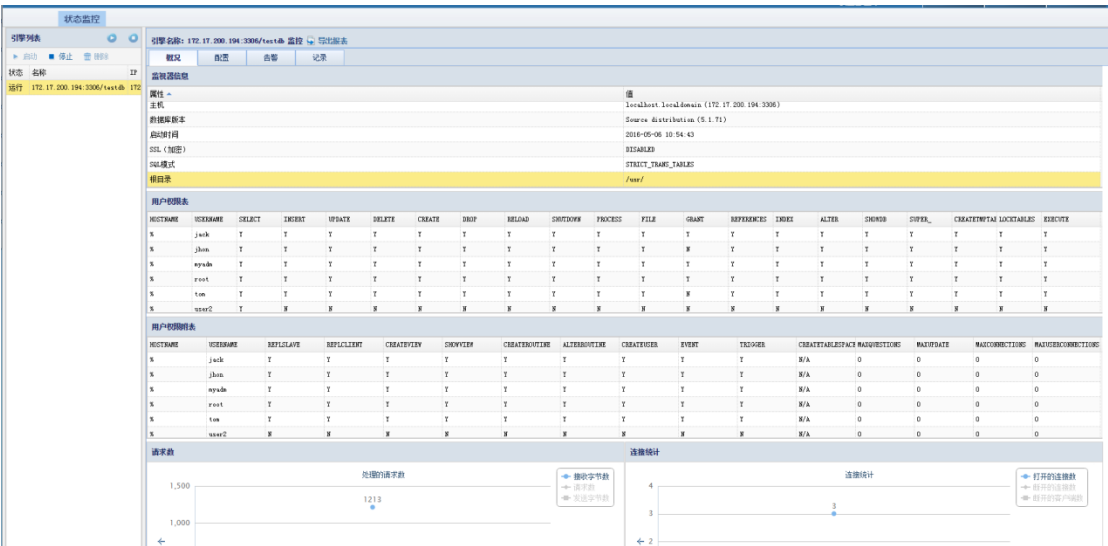
点击选择相应引擎可，对该引擎进行开启、停止和删除操作如下图所示：



提示：引擎只有在停止状态下才能被删除

3.5.3 概况

该页面包括监视器信息、用户权限、用户权限附表、请求数等信息，用户可以快速从该页面了解到对应数据库的运行概况，如下图所示：



3.5.3.1 监视器信息

监视器信模块，主要包含了如下信息，该模块显示的信息以使用户更清晰的了解数据库的详细信息。

- 主机：主机名。
 - 数据库版本：数据库的版本。
 - 启动时间：该引擎启用的时间。
 - SSL（加密）：是否启用了 ssl 加密。
 - SQL 模式：数据库所使用的 SQL 模式。
 - 根目录：数据库的根目录。
- 如下图所示：

| 概况 | 配置 | 告警 | 记录 |
|---------|---|----|----|
| 监视器信息 | | | |
| 属性 | 值 | | |
| 主机 | localhost.localdomain (172.17.200.194:3306) | | |
| 数据库版本 | Source distribution (5.1.71) | | |
| 启动时间 | 2016-05-06 10:54:43 | | |
| SSL（加密） | DISABLED | | |
| SQL模式 | STRICT_TRANS_TABLES | | |
| 根目录 | /usr/ | | |

3.5.3.2 用户权限表

用户权限表模块，主要包含数据用户名（USERNAME）以及对应用户可以登录数据库的主机（HOSTNAME），用户对数据库所具有的权限（select、insert、update……）等信息。

如下图所示：

| 用户权限表 | | | | | | | | |
|--------------|----------|--------|--------|--------|--------|--------|------|--------|
| HOSTNAME | USERNAME | SELECT | INSERT | UPDATE | DELETE | CREATE | DROP | RELOAD |
| % | tom | Y | Y | Y | Y | Y | Y | Y |
| % | user2 | Y | N | N | N | N | N | N |
| % | zim | Y | Y | Y | Y | Y | Y | Y |
| 127.0.0.1 | root | Y | Y | Y | Y | Y | Y | Y |
| 172.16.0.126 | lisa | Y | N | N | N | N | N | N |
| localhost | | N | N | N | N | N | N | N |

3.5.3.3 用户权限附表

用户权限附表模块，主要包含数据用户名（USERNAME）以及对应用户可以登录数据库的主机（HOSTNAME），用户对数据库所具有的权限（replslave、replclient、createview……）等信息。如下图所示：

| 用户权限附表 | | | | | | |
|--------------|----------|-----------|------------|--------------|----------|---------------|
| HOSTNAME | USERNAME | REPLSLAVE | REPLCLIENT | CREATEVIEW ▲ | SHOWVIEW | CREATEROUTINE |
| % | tom | Y | Y | Y | Y | Y |
| % | user2 | N | N | N | N | N |
| % | zim | Y | Y | Y | Y | Y |
| 127.0.0.1 | root | Y | Y | Y | Y | Y |
| 172.16.0.126 | lisa | N | N | N | N | N |
| localhost | | N | N | N | N | N |

3.5.3.4 请求数

请求数模块，主要包含接收字节数、请求数、发送字节数三方面的信息如下图所示：



提示：“请求数”和“发送字节数”默认为灰色未显示折线图状态，用户点选上图中右上角的相应名称后，相应折线图会加以显示。

3.5.3.5 连接统计

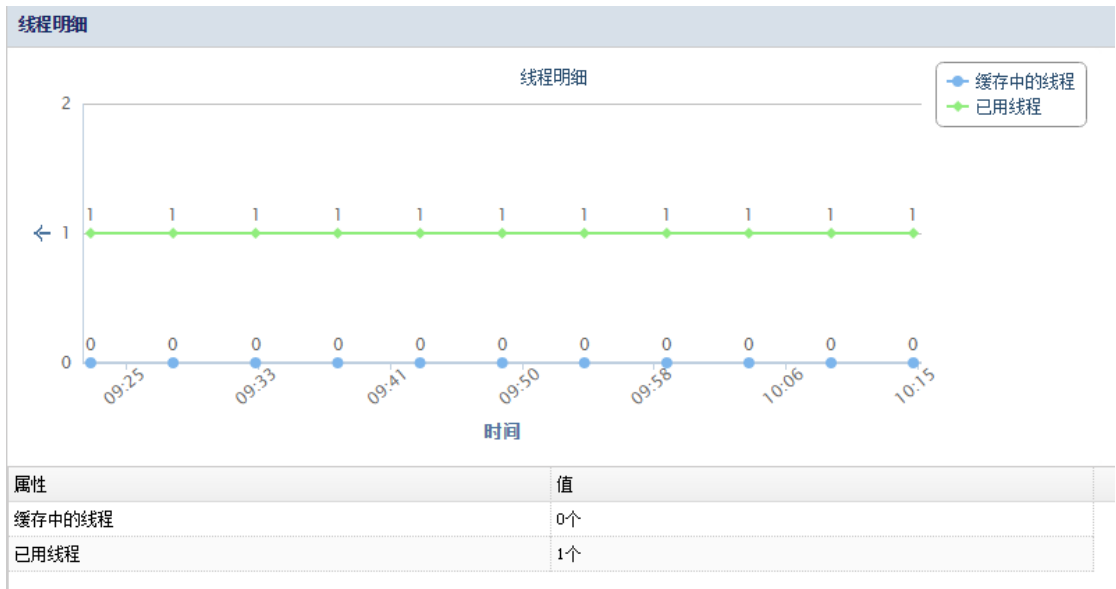
连接统计模块，主要包含打开的连接数、断开的连接数、断开的客户端数三方面的信息，如下图所示：



提示：“断开的连接数”和“断开的客户端数”默认为灰色未显示折线图状态，用户点选上图中右上角的相应名称后，相应折线图会加以显示。

3.5.3.6 线程明细

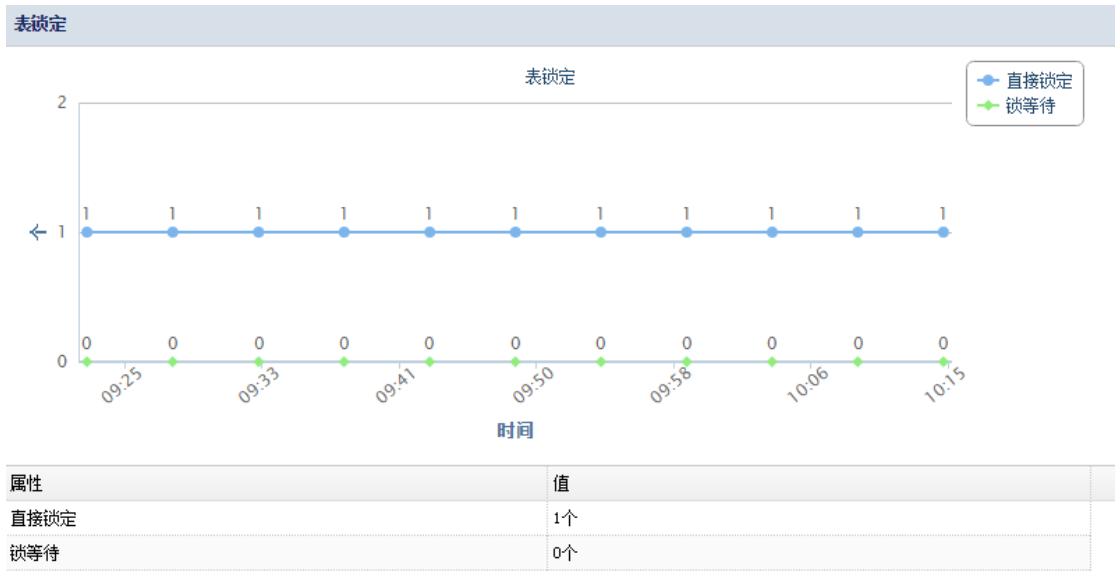
线程明细模块，主要包含缓存中的线程、已用线程两方面的信息，如下图所示：



提示：“已用线程”默认为灰色未显示折线图状态，用户点选上图中右上角的相应名称后，相应折线图会加以显示。

3.5.3.7 表锁定

表锁定模块，主要包含直接锁定、锁等待两方面的信息，如下图所示：



提示：“锁等待”默认为灰色未显示折线图状态，用户点选上图中右上角的相应名称后，相应折线图会加以显示。

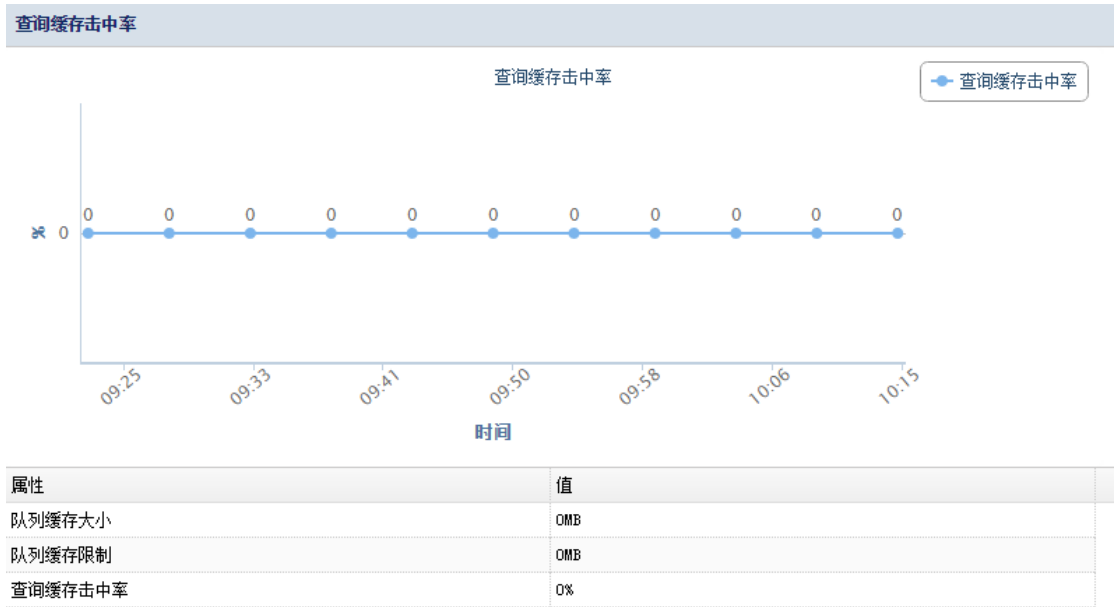
3.5.3.8 主键击中率

主键击中率模块，主要包含主键击中率、已用主键缓冲区、主键缓冲区大小三方面的信息，如下图所示：



3.5.3.9 查询缓存命中率

查询缓存命中率模块，主要包含查询缓存命中率、队列缓存大小、队列缓存限制三方面的信息，如下图所示：



3.5.3.10 查询统计

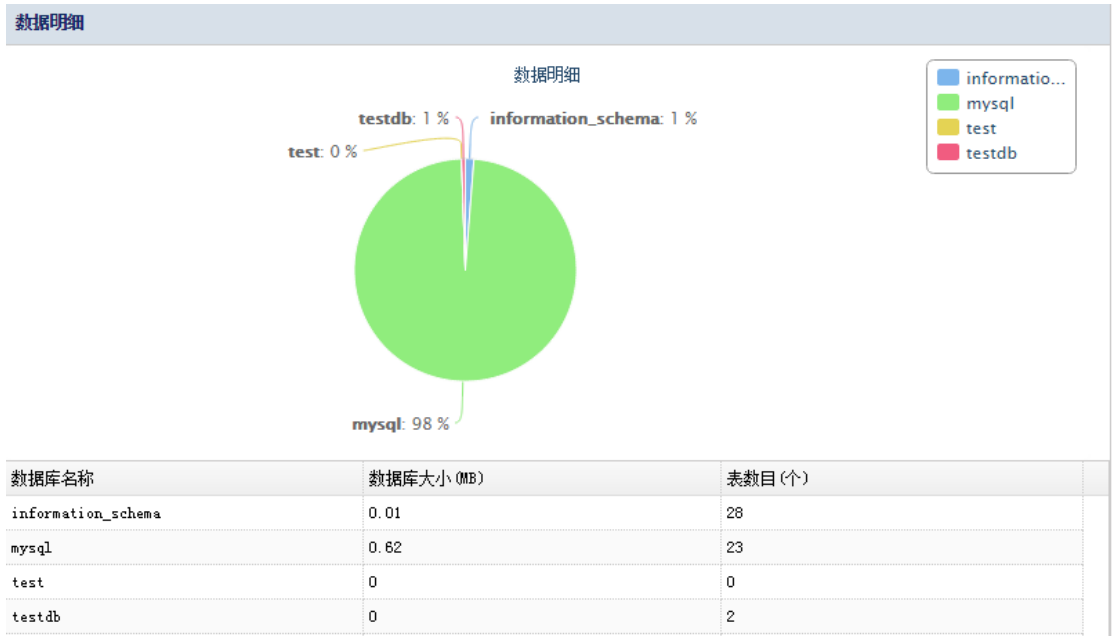
查询统计模块，主要包含插入的查询、更新的查询、删除的查询、选择的查询四方面的信息，如下图所示：



提示：“更新的查询”、“删除的查询”、“选择的查询”默认为灰色未显示折线图状态，用户点选上图中右上角的相应名称后，相应折线图会加以显示。

3.5.3.11 数据明细

数据模块，主要包含数据库名称、数据库大小、数据目（个）三方面的信息，如下图所示：

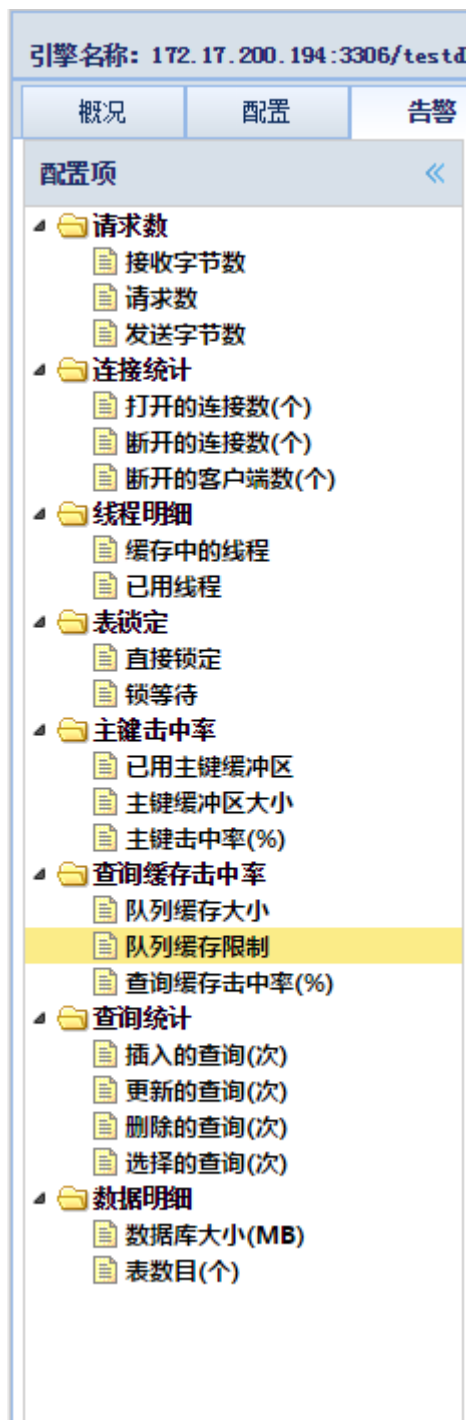


3.5.4 配置

从配置页面，用户可以快速的浏览到相应数据库的配置信息如下图所示：

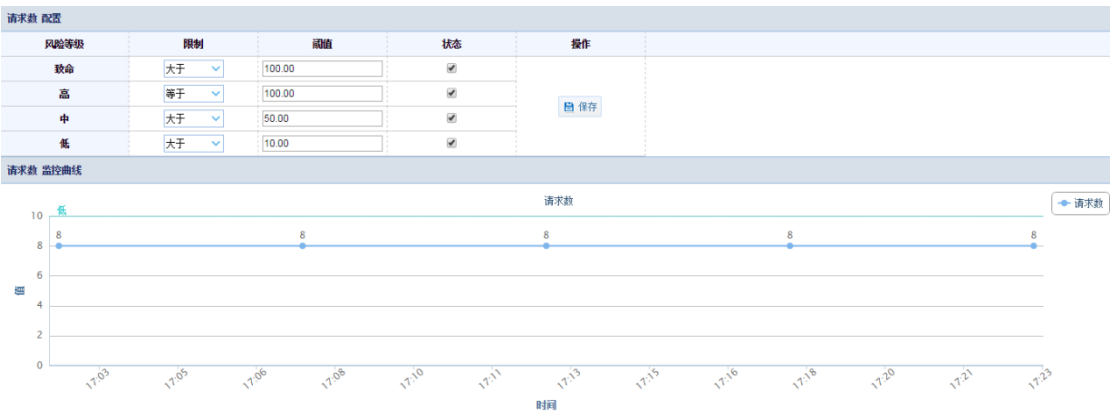
3.5.5.1 配置项

在该模块主要显示了一些告警规则，可根据需要选择配置项，其中主要有几大项分别是：请求数、连接统计、线程明细、表锁定、主键击中率、查询缓存击中率、查询统计以及数据明细。如下图所示：



3.5.5.2 编辑告警配置

该模块是针对左侧所选取的具体的配置项，进行阈值编辑的，根据需要设定阈值，点击保存后即可生效，当偏离阈值时将会告警。如下图所示：



3.5.6 记录

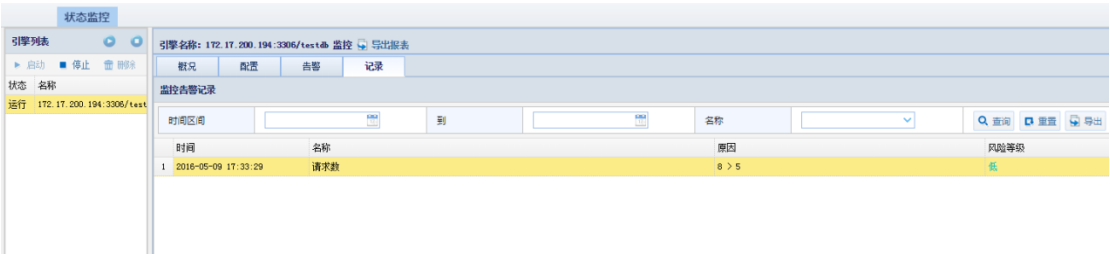
该模块主要是针对告警模块，记录的是告警，在该模块可以查询到告警的表，还可以根据时间来筛选告警，可以进行查询、重置与导出三项操作，导出的格式支持 WORD、EXCELE、PDF。如下图所示：

监控告警记录

时间区间 到 名称

查询 重置 导出

同时还会显示该告警记录的时间、名称、原因以及风险等级。



3.6 运维审计

所属用户：SecAdmin。

通过运维审计模块可对 FTP 服务器进行审计。

3.6.1 FTP 引擎列表

在 FTP 引擎列表中可以查看到已添加的 FTP 引擎，包括其 IP 地址、端口、网口名、过滤记录保存天数等信息；通过“添加”、“编辑”等按钮进行相应操作

| FTP审计 | | | | | | |
|-----------------------------|----|-------|----------|-------------|-----|----|
| FTP引擎列表 | | | | | | |
| <div>添加 编辑 默认设置 启动 停止</div> | | | | | | |
| IP | 端口 | 网口名 | 过滤记录保存天数 | 连续登录失败~次后告警 | 状态 | 操作 |
| 172.17.200.190 | 21 | ensg1 | 3 | 3 | 运行中 | |

3.6.1.1 添加

点击“添加”，弹出新建引擎窗口，输入 IP 端口网口，选择网口名称（审计接口），设置记录天数、连续失败多少次的风险等级，点击“确定”进行保存。

新建引擎

IP

端口

21

网口名称

记录天数

3

连接失败

5

次

无风险

确定

3.6.1.2 编辑

点选已添加的 FTP 引擎，点击“编辑”按钮，弹出编辑引擎窗口，除 IP 地址外其它参数均可修改。点击“确定”保存修改。

编辑引擎

IP

172.17.200.190

端口

21

网口名称

enp1

记录天数

3

连接失败

3

次

中风险

确定

提示：引擎审计在停止状态下方可编辑。

3.6.1.3 默认设置

通过默认设置可配置记录参数和连续失败多少次的风险等级。点选相应引擎，点击“默认设置”，弹出默认设置窗口，修改相应参数，点击“确定”。

默认设置

记录天数

3

连接失败

5

次

无风险

确定

3.6.1.4 启动和停止

点选相应引擎，点击“启动”或“停止”，开启或关闭相应引擎的审计功能。

| FTP引擎列表 | | | | | | |
|--------------------|----|-------|----------|-------------|-----|----|
| + 添加 编辑 默认设置 启动 停止 | | | | | | |
| IP | 端口 | 网口名 | 过滤记录保存天数 | 连续登录失败n次后告警 | 状态 | 操作 |
| 172.17.200.190 | 21 | ensg1 | 3 | 3 | 运行中 | |

3.6.2 规则列表

在规则列表中可以查看到已添加的规则；通过“添加”、“编辑”、“删除”等按钮进行相应操作

示例：添加

点击“添加”，添加/编辑规则窗口，输入规则名称；选择风险等级；针对客户端 IP、服务器 IP、文件名、文件类型、敏感词、正则匹配、文件大小等条目进行规则配置，点击“保存”进行保存。

添加/编辑规则

规则名称

test

设为默认规则

风险等级

中风险

客户端IP

172.16.0.126

包含 不包含

服务器IP

172.17.200.190

包含 不包含

文件名

1.txt

包含 不包含

文件类型

txt

包含 不包含

敏感词

1

正则匹配

*

文件大小

大于等于

0.00

MB

保存

四、 检索和报表

4.1 审计检索（检索）

所属用户：SecAdmin。

审计检索模块中包含了数据库审计检索（检索）和 FTP 检索两个大的模块，通过检索模块，用户能够按条件筛选审计日志。

可以生成检索中不同时间段的报表。

在检索中实时生成不同维度的报表。所谓不同维度就是对不同条件的组合查询。

服务器维度： 被监测服务器、受监测数据库、数据库服务器性能。

源分析维度： 源应用程序、数据库用户、源主机、源 IP、登录分析、源就用的性能。

数据的访问模式： 最多查询、查询类型分析、敏感数据查询、查询记录、数据修改分析。

特权操作： 特权查询概述、表删除与截断、存储过程的更改、数据库与 Schemar 的更改、DCL 命令、DDL 命令、本机审计更改、新创建的用户。

其它信息： 失败的登录、SQL 错误、未检测的加密登录。

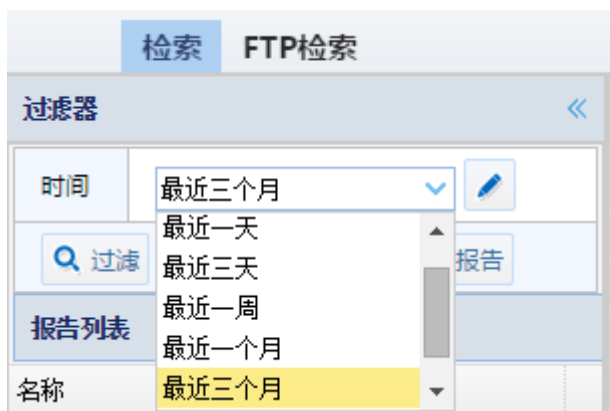
基于时间的分析： 每天、每周、每时。

4.1.1.1 数据库审计检索

4.1.1.1.1 过滤器

时间

1. 默认选择从下拉菜单选择一天、三天、一周、一个月、三个月。如下图所示：



2. 第二种为自定义时，从某一时间点另一时间点。如下图所示：

自定义时间范围

开始时间

该输入项为必填项

结束时间

整点设置

确定

取消

过滤

过滤包括的可选条目有：引擎、策略、数据库类型、数据库 IP、数据库 MAC、数据库实例、数据库用户、操作、操作类型、操作对象、字段、客户端 IP、客户端 MAC、客户端端口、主机名、操作系统用户、客户端程序、执行时长、动作、风险等级、影响行数、SQL 语句、SQL 结果、响应状态、SQL 模型。



更新

“更新”按钮可以刷新右侧显示，当更改过滤条件时，需用“更新”刷新右侧数据。

检索FTP检索

过滤器

时间最近三个月

过滤更新导出报告

报告列表

名称

视图

概要

数据

服务器分析

数据库服务器分析

数据库服务器性能

来源分析

源数据库用户

源应用程序

源主机

源IP

登录分析

源应用程序性能

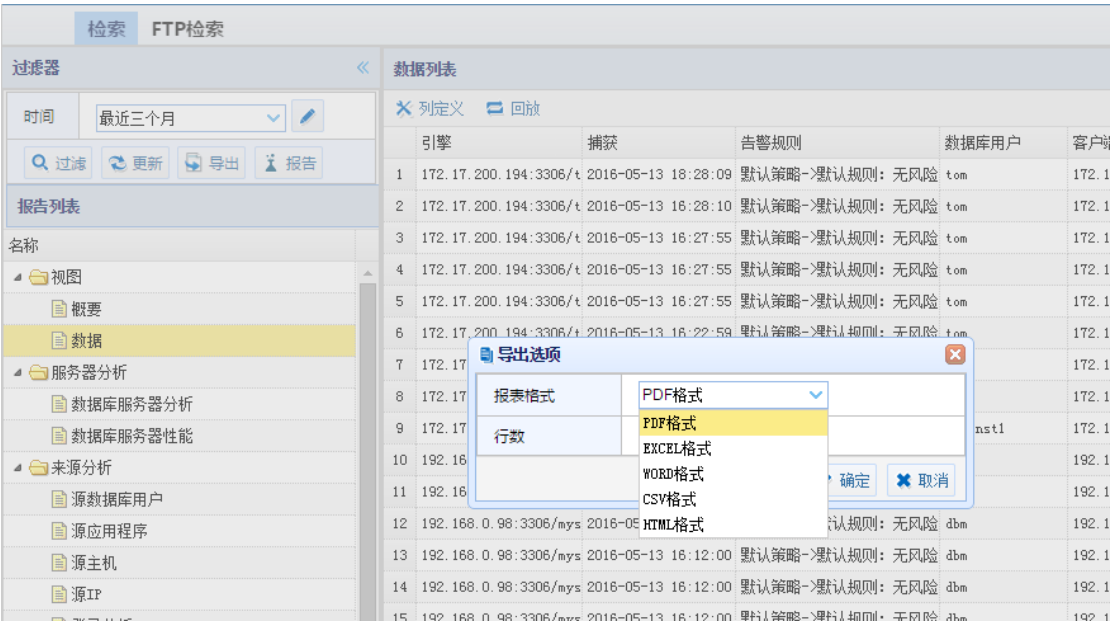
数据列表

列定义回放

| | 引擎 | 捕获 | 告警规则 | 数据库用户 | 客户端 |
|----|-----------------------|---------------------|-----------------|----------|--------|
| 1 | 172.17.200.194:3306/t | 2016-05-13 18:28:09 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 2 | 172.17.200.194:3306/t | 2016-05-13 16:28:10 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 3 | 172.17.200.194:3306/t | 2016-05-13 16:27:55 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 4 | 172.17.200.194:3306/t | 2016-05-13 16:27:55 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 5 | 172.17.200.194:3306/t | 2016-05-13 16:27:55 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 6 | 172.17.200.194:3306/t | 2016-05-13 16:22:59 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 7 | 172.17.200.194:3306/t | 2016-05-13 16:22:59 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 8 | 172.17.200.194:3306/t | 2016-05-13 16:22:59 | 默认策略->默认规则: 无风险 | tom | 172.11 |
| 9 | 172.17.200.190:60000/ | 2016-05-13 16:22:44 | 默认策略->默认规则: 无风险 | db2inst1 | 172.11 |
| 10 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |
| 11 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |
| 12 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |
| 13 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |
| 14 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |
| 15 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |
| 16 | 192.168.0.98:3306/mys | 2016-05-13 16:12:00 | 默认策略->默认规则: 无风险 | dbm | 192.11 |

导出

“导出”按钮可以将筛选的数据以 PDF、WORD、EXCEL 等格式导出，便于用户查看与分析。



报告

点击“报告”按钮，弹出添加报告的窗口，点击“确定”会将报告列表中选中的条目导入到报表模块中。



| 报告 报告结果 | | | | | |
|---|--------|---------------------|----|------|--|
| 报告列表 | | | | | |
| <div>+ 添加</div> <div>删除</div> <div>时间排序</div> <div>分类排序</div> | | | | | |
| 名称 | 类型 | 修改时间 | 计划 | 来源 | |
| 检索-来源分析 | | | | | |
| 源数据库用户 | 源数据库用户 | 2016-05-13 18:52:14 | | 模块导入 | |
| 检索-视图 | | | | | |
| 数据 | 数据 | 2016-05-13 18:41:36 | | 模块导入 | |

4.1.1.2 报告列表

报告列表包含视图、服务器分析、来源分析、数据访问模式、特权操作、其他视图、基于时间的分析，几个大条目。

| 报告列表 | |
|---------|--|
| 名称 | |
| 视图 | |
| 服务器分析 | |
| 来源分析 | |
| 数据访问模式 | |
| 特权操作 | |
| 其他视图 | |
| 基于时间的分析 | |

视图



视图为检索策略的结果呈现，分为“概要”与“数据”视图。还可以基于“过滤”来查看所需要的查看内容。

视图的“概要”信息主要是通过用户点击情况，按天、周、小时、来进行统计，可以形成表格及柱状图进行输出。

如下图所示：



如下图所示：

数据列表

列定义 回放

| | 引擎 | 捕获 | 告警规则 | 数据库用户 | 客户端IP | 风险等级 | 操作 |
|----|-----------------------|---------------------|-----------------|--------|---------------|------|----|
| 1 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 2 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | SI |
| 3 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | UI |
| 4 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 5 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | LI |
| 6 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | LI |
| 7 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 8 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | SI |
| 9 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | UI |
| 10 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 11 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | LI |
| 12 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | LI |
| 13 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 14 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | SI |
| 15 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | UI |
| 16 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 17 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | LI |
| 18 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | LI |
| 19 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | DI |
| 20 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | SI |
| 21 | 192.168.0.97:1521/orc | 2016-04-27 15:05:46 | 默认策略->默认规则: 无风险 | SYSTEM | 192.168.0.168 | 无风险 | UI |

服务器分析

数据库服务器分析

被监测数据库由两个柱状图及一个表格够成，分别为数库名称及数据库用户数柱状图及访问数据库来源 IP 柱状图（同源多 IP），表格名称为数据库登录及点击统计报表分别由数据名、引擎、登录-数量、事件累计构成。

如下图所示：



数据库服务器性能

数据库的性能指标主要是通过对数据库的操作时间为维度来判断数据的性能。通过四个图与一个表格来体现数据库的性能。分别是请求响应时间（1 秒以下、1 秒以上 10 以下、10

秒以上)、SQL 类型时长累计（在一段时间内所有对数据库操作 SQL 用时累计）、服务的繁忙占比（基于源 IP 的平均响应时间占比）。表操作时长累计（数据库中表的响应时长的累计）。

如下图所示：





来源分析

来源分析是通过源应用程序、数据库用户、源主机、源 IP、登录分析、源应用程序的性能等进行不同角度的分析数据的点击率、登陆及相关统计。

如下图所示：



源数据库用户

源数据库用户分析，通过不同的数据库用户访问不同的数据库进行分析。主要构成为一个柱状图与表格。柱状图是数据库用户访问不同的库与事件数构成。表格是通过用户、引擎、数据库名称、登录-数量、事件-累计等项目进行统计的。

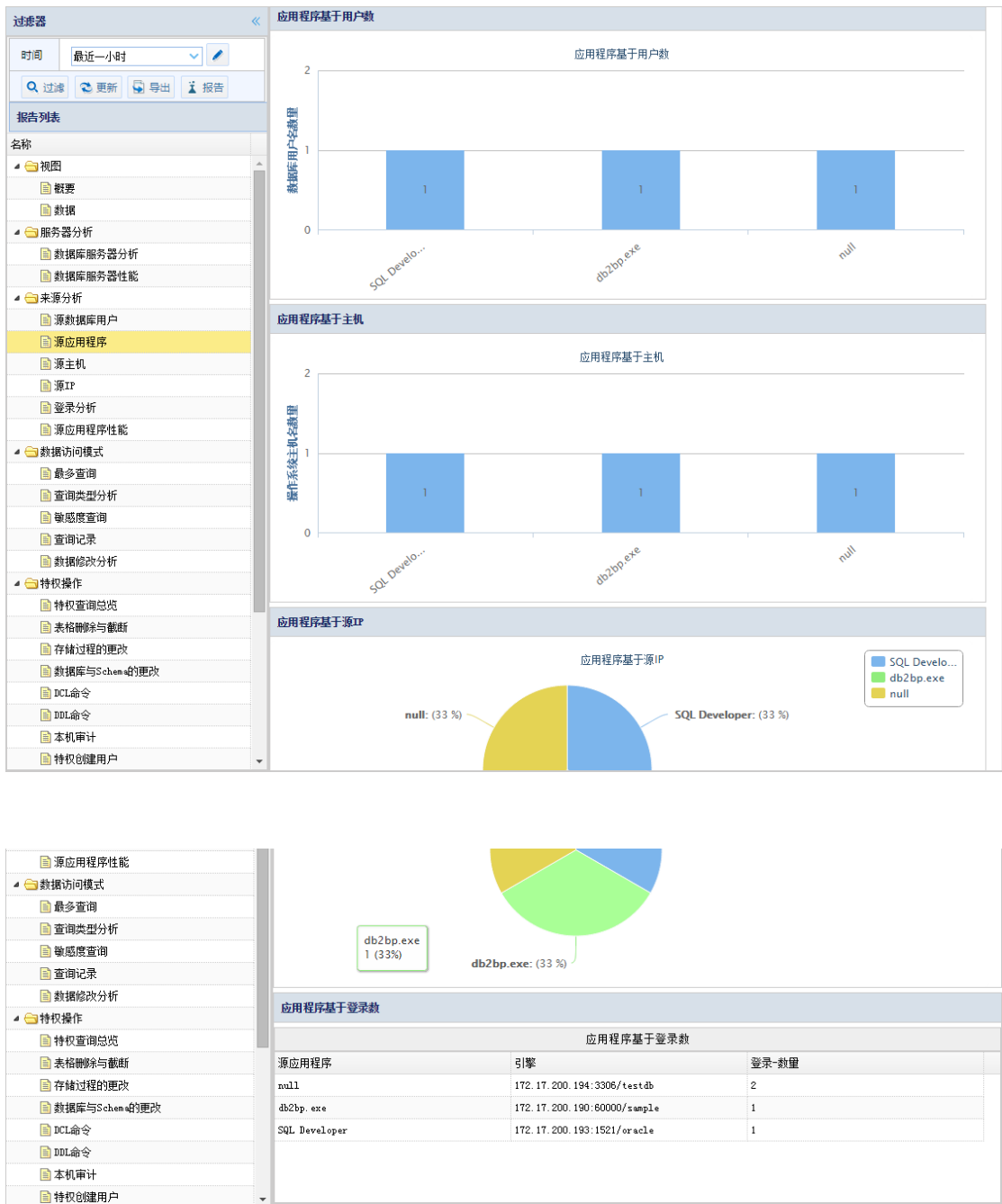
如下图所示：



源应用程序

通过源应用程序的用户、主机、IP、引擎等角度进行统计。通过三个图一个表格方式呈现。表格方式包括源应用程序、引擎、登录-数量。

如下图所示：



源应用程序性能

数据访问模式

最多查询

查询类型分析

敏感度查询

查询记录

数据修改分析

特权操作

特权查询总览

表格删除与截断

存储过程的更改

数据库与Schema的更改

DCL命令

DDL命令

本机审计

特权创建用户

db2bp.exe 1 (33%)

db2bp.exe: (33%)

应用程序基于登录数

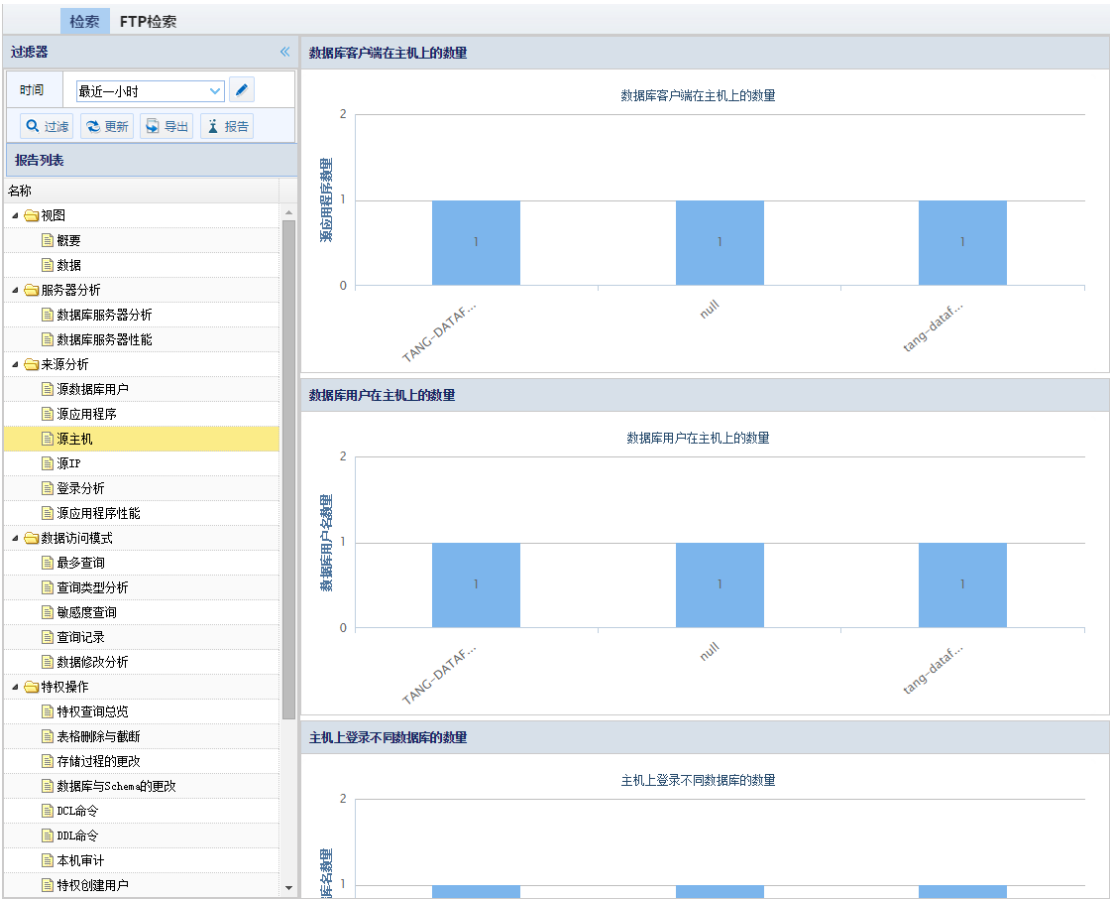
应用程序基于登录数

| 源应用程序 | 引擎 | 登录-数量 |
|---------------|-----------------------------|-------|
| null | 172.17.200.194:3306/testdb | 2 |
| db2bp.exe | 172.17.200.190:60000/sample | 1 |
| SQL Developer | 172.17.200.193:1521/oracle | 1 |

源主机

统计访问数据的主机相关信息，主要包括数据库客户端在主机上的数量、数据库用户在主机上的数量、主机上登录不同数据库的数量、主机综合信息等，通过三个柱状图一个图格来呈现。

如下图所示：

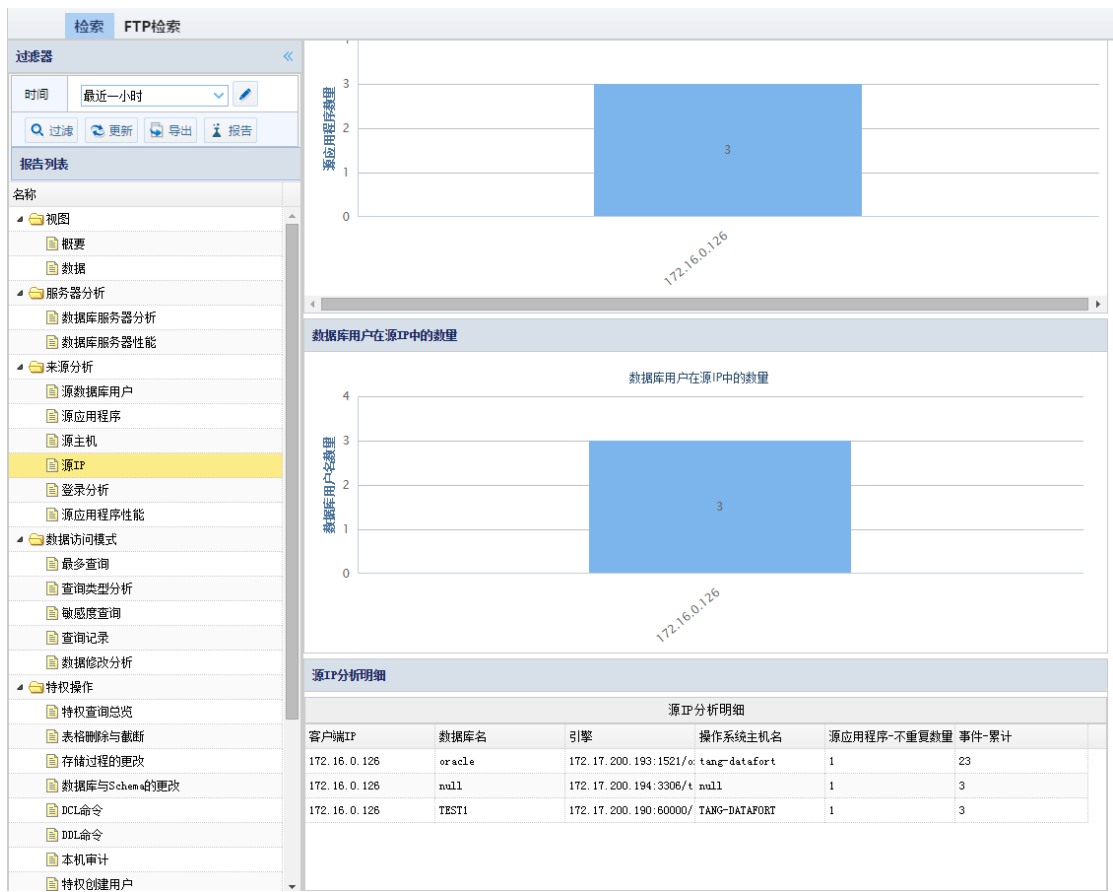




源 IP

统计源 IP 中数据库应用程序的数量、数据库用户数量，由两个柱状图和一个表格组成。

如下图所示：



登录分析

统计登陆数据库的用户、操作系统主机名、源应用程序、数据库用户、数据库引擎、数据库名、数据库 Schema、数据库 IP、登录-数量。以一个柱状图和一个表格显示。详见下图



源应用程序性能

分析源应用程序的性能，用户操作平均时间、过长时间、应用程序的时间占比、平均累计时间。通过柱状图及表的形式呈现。



数据访问模式

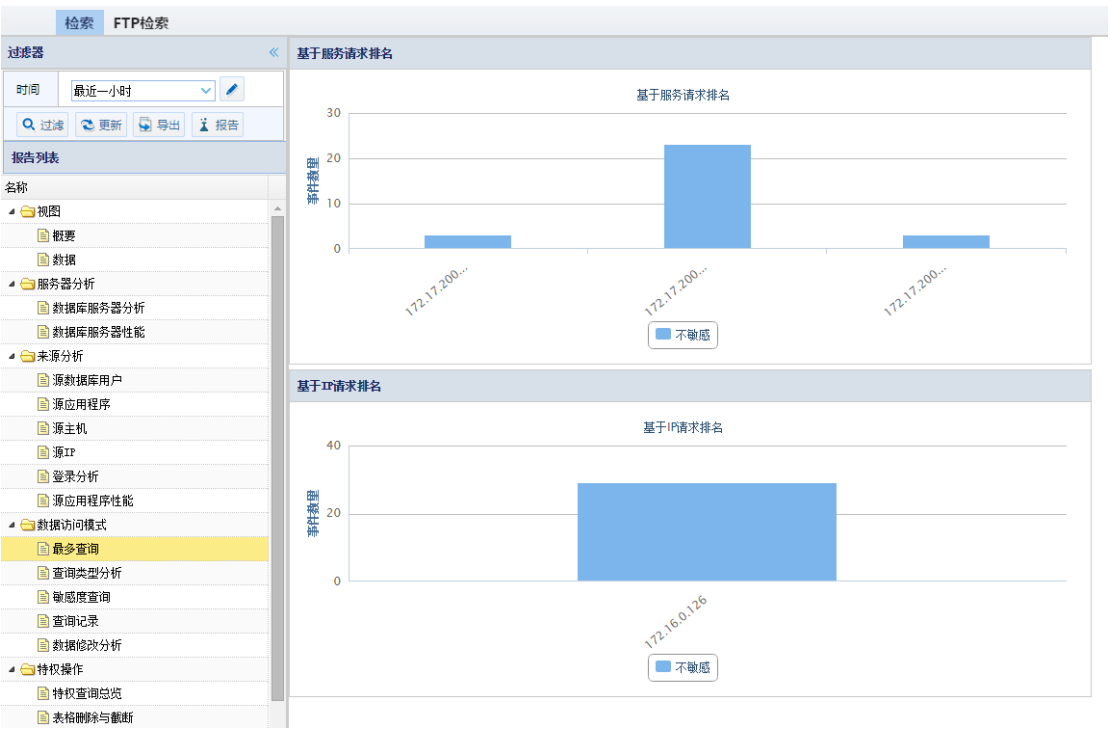
根据数据的查询类型、数量、及数据的修改来进行分析。包括最多查询、查询类型分析、敏感度查询、查询记录、数据修改分析。



最多查询

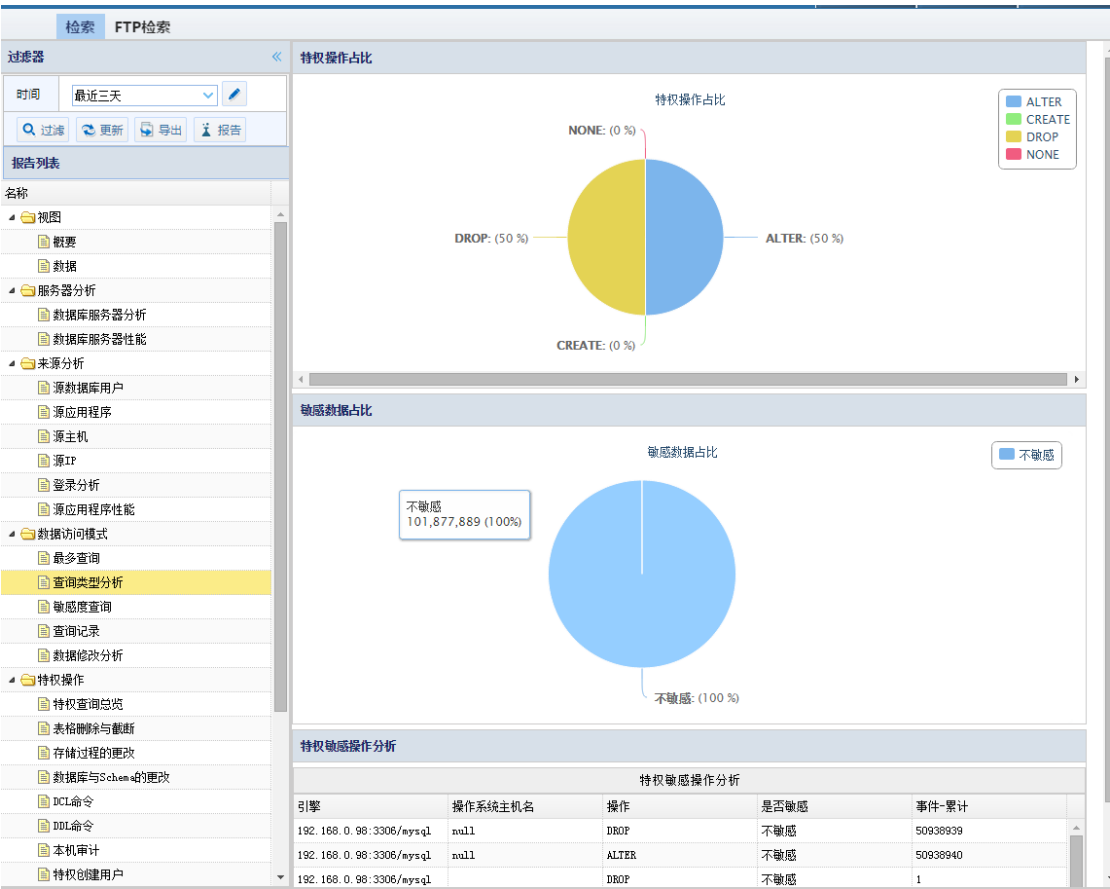
统计数据库的时间数量、客户端对应 IP 的请求数量，通过柱状图形式呈现。

如下图所示：



查询类型分析

统计分析数据中的特权操作、无特权操作、敏感数据、不敏感数据。通过饼状图及表格形式呈现。如下图所示：



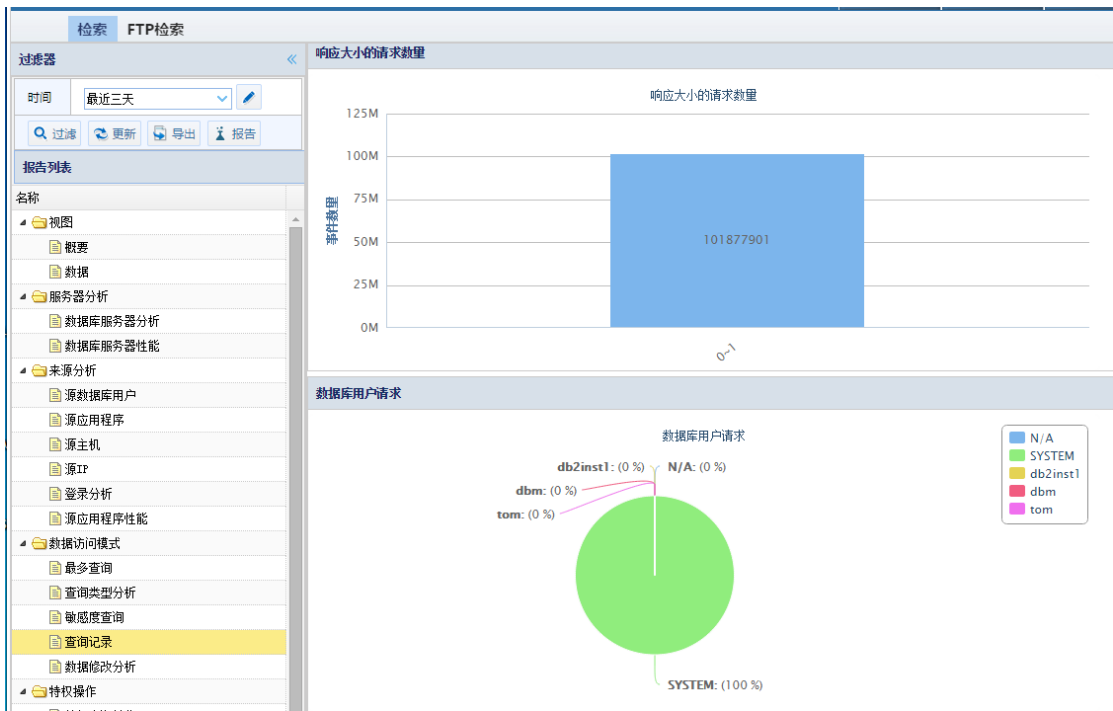
敏感数据查询

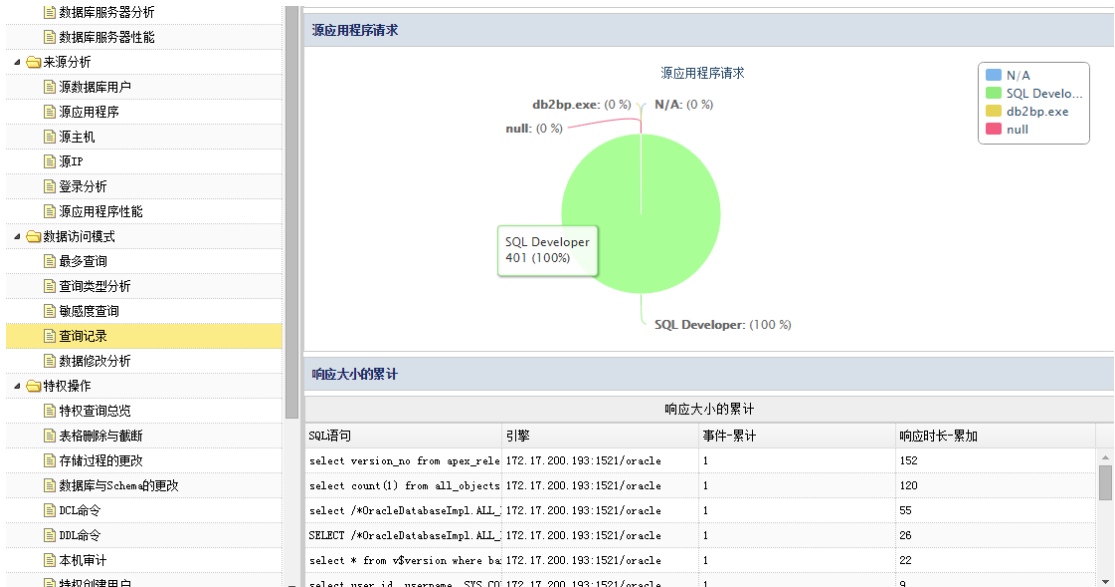
在数据库及表组中统计敏感信息。通过柱状图及综合表格来呈现。



查询记录

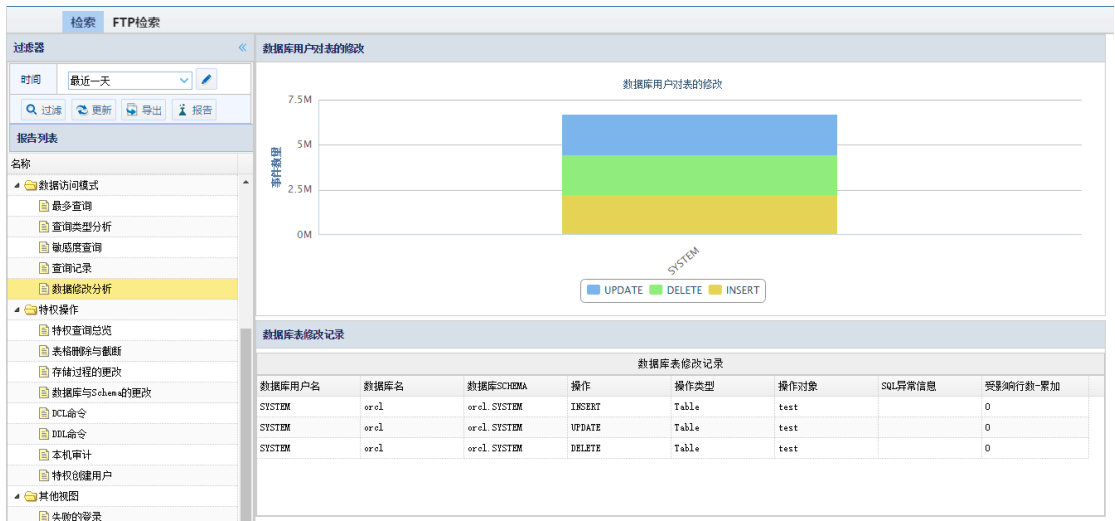
统计请求响应大小数量、应用程序请求占比、用户请求占比、响应大小累计。通过饼状图、柱状图以及表格形式呈现。如下图所示：





数据修改分析

统计数据访问中的 insert、updata、delete 等对数据库表修改的操作。通过柱状图与表格形式展现。如下图所示：

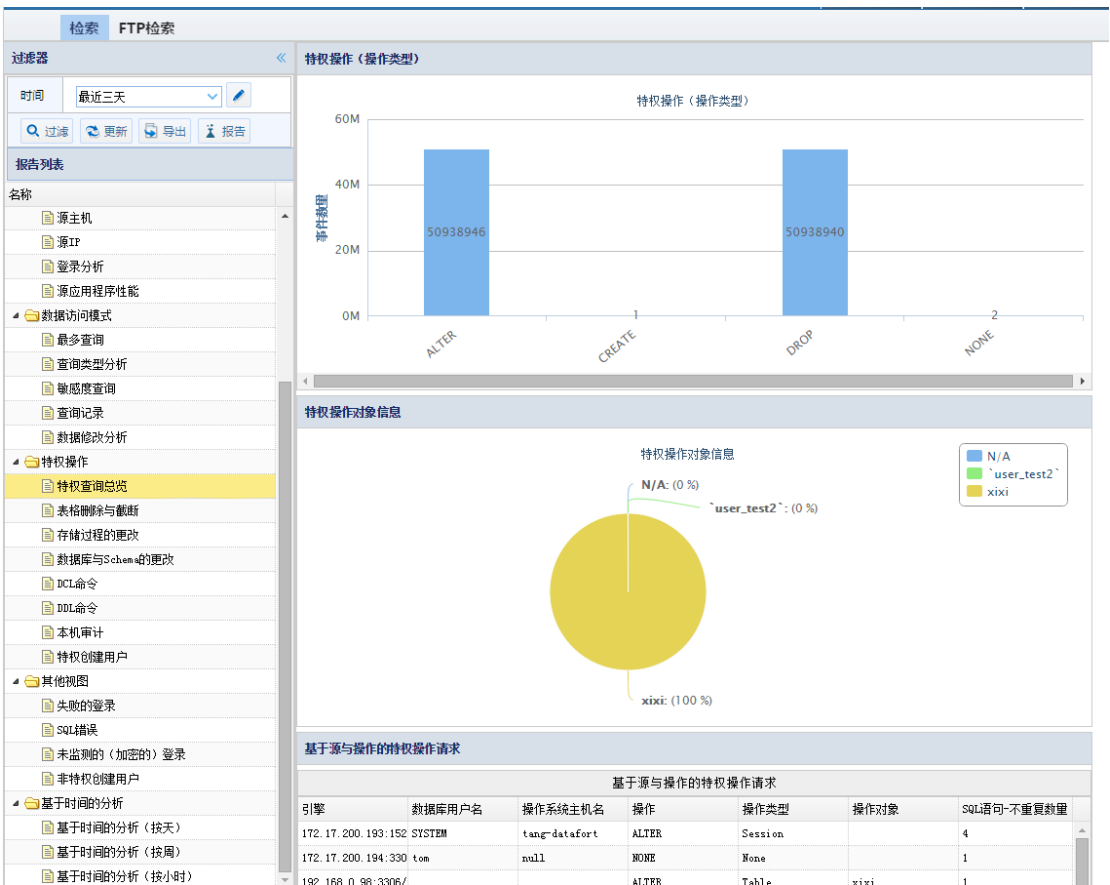


特权操作

统计特权操作相关信息包括特权查询总览、表删除与截断、存储过程的更改、数据库与 Schema 的更改、DCL 命令、DDL、本机审计、特权创建用户。通过柱状图饼状图及表格形式展现。

特权查询总览

统计特权操作相关信息，包括特权操作类型、特权操作对象信息、基于源与操作的特权操作请求。分别通过柱状图、饼状图、表格的形式展现。如下图所示：



表删除与截断

统计不同用户对表的删除与截断（drop、truncate）通过柱状图及表格的形式展现。如下图所示：



存储过程的更改

统计用户对表的操作，表的类型属于 Procedure、Function 并且操作属于特权操作。通过柱状图与表格方式展现。



数据库与 Schema 的更改

分析用户对数据库及 Schema 的特权操作，通过柱状图及表格的形式展现。



DCL 命令

通过 DCL 命令分析用户与特权操作,通过饼状图与表格展现。



DDL 命令

通过 DDL 命令分析用户与特权操作,通过饼状图、柱状图与表格展现。



本机审计

分析操作类型为 Audit Operation、Audit 特权操作，通过饼状图与表格形式展现。



特权创建用户

统计创建用户的方法的占比，包括 INSERT USER 表的方法、CREATE USER 的方法、GRANT 的方法。通过饼状图的形式展现。

统计创建用户的相关的CREATE USER方法和GRANT的方法。

创建用户方法



新用户分布



| 创建用户详细 | | | |
|--------|--------|---------|------|
| 创建用户详细 | | | |
| 引擎 | 数据库用户名 | 操作系统主机名 | 操作对象 |
| | | | |

其它视图

统计分析其它类别的视图包括失败的登录、SQL 错误、未监测的（加密的）登录、非特权创建用户，通过饼状图、柱状图等进行分析。

失败的登录

统计登录数据库失败的次数与数据库的类型。通过柱状图和表格的方式展示。详见下图。



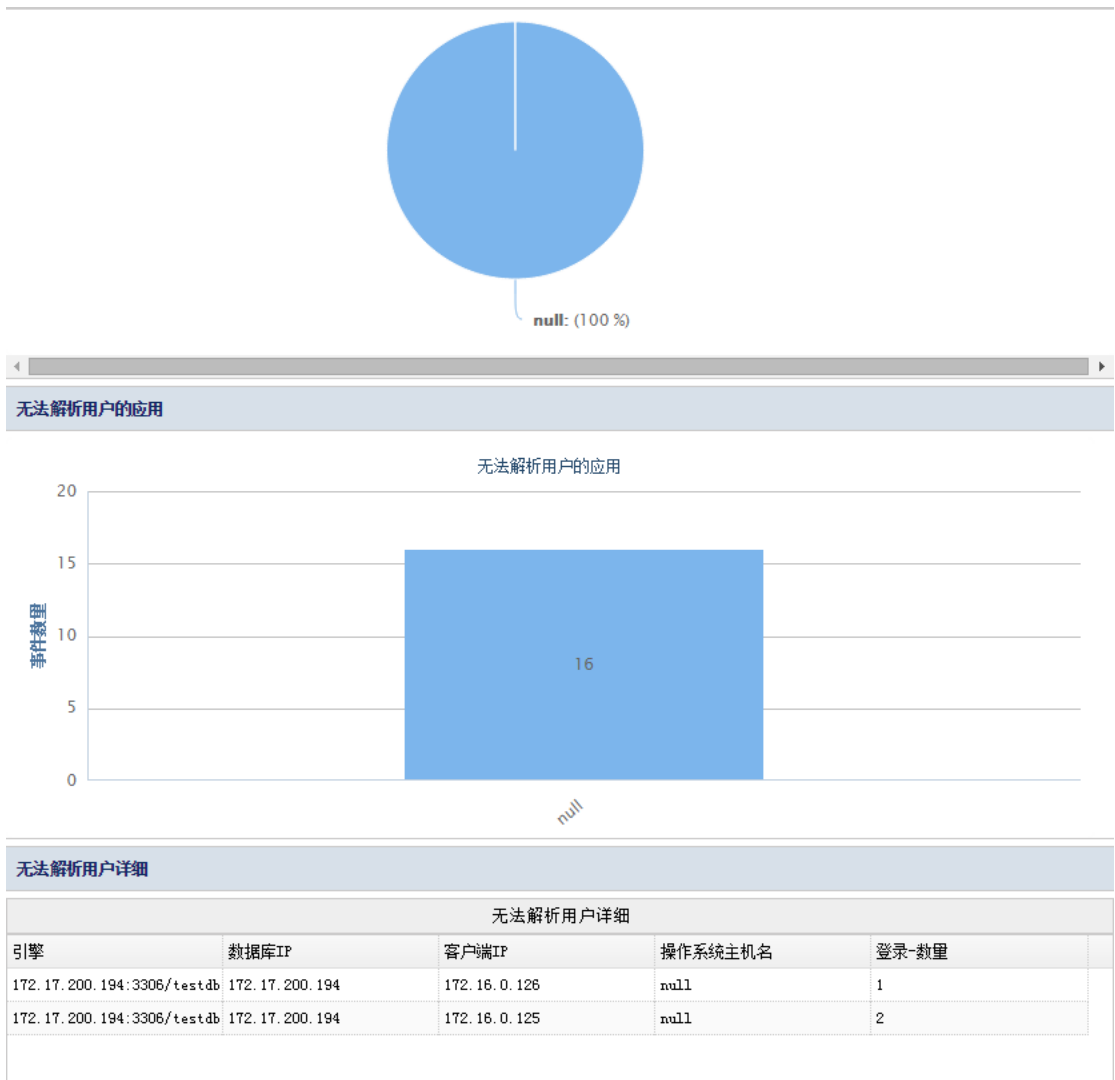
SQL 错误

统计每个引擎或服务器发生的 SQL 异常请求的数量，通柱状图与表格的方式展现。SQL 异常通常是请求的语句异常。例如：select I love you select*.8 phoneNum show tables use mysql show databases print “serverName………….” + sysuser exp select * from select*.*from select* select*from all tables 等。详见下图。



未监测的（加密的）登录

统计无法解析的用户名，在识别到验证流量已加密但却无法解密时，不论是出于何种原因无法解密，通过饼状图与柱状图及表格方式展现。如下图所示：



基于时间的分析

根据时间的维度来分析 SQL 请求数量，包括每天、每周中的某一天、每天的某一时刻。

通过柱状图与表格来展现。

基于天

统计每天的点击数量通过柱状图与表格的方式展现。



基于周

统计每周中的每天点击数量，通过柱状图与表格形式展现。如下图所示：



基于小时

统计每天中的每小时点击数量，通过柱状图与表格形式展现。如下图所示：



4.1.1.3 点击数按天细分（小时）

统计一天中小时的点击数通过柱状图展现,同时在表格中展现点击详细信息包括小时(24小时)、点击、登录、用户、引擎、主机。

4.1.2 FTP 检索

4.1.2.1 FTP 数据检索

查询结果

通过 FTP 数据检索页面可检索查看 FTP 客户端从服务器下载或上传文件的操作。可以时间、服务器 IP、客户端 IP、用户名、文件名、关键字为条件进行筛选查询。通过“重置”按钮，清除所设置的条件，点选相应文件，点击“批量下载”按钮可将文件下载到本地。通过“导出”按钮可将条目以文件的形式导出到本地。“生成报表”按钮，可生成 FTP 审计报表，并以文件形式导出下载到本地。

查询结果

| | | | | | | | | |
|-------------------------------------|-------------------------------------|---------------------------------|----------------------|-------------|----------------------|--|----------------------|--------|
| 时间 区间 | <input type="text"/> | 到 | <input type="text"/> | 服务器 IP | <input type="text"/> | 客 户 端 IP | <input type="text"/> | |
| 用 户 名 | <input type="text"/> | 文 件 名 | <input type="text"/> | 关 键 字 | <input type="text"/> | <div><div>查询</div><div>重置</div><div>批量下载</div><div>导出</div><div>生成报表</div></div> | | |
| <input checked="" type="checkbox"/> | 操作时间 | 服务器IP | 客户端IP | 用户名 | 文件名 | 文件大小 | 上传 / 下载 | 链接地址 |
| 1 | <input checked="" type="checkbox"/> | 2016-05-23 16:27:172.17.200.190 | 172.16.0.125 | ftpuser | 1.txt | 2.17K | 下载 | /1.txt |

概要

在概要中能够查看到相应文件的文件名和存放路径等信息。

概要

文件名: 1.txt

ftp路径: /1.txt

.....[查看更多内容](#)

4.1.2.2 FTP 指令检索

通过 FTP 指令检索页面可检索查看 FTP 客户端所执行的 FTP 指令。可以时间、服务器 IP、客户端 IP、指令、用户名为条件进行筛选查询。

检索

FTP检索

FTP数据检索

FTP指令检索

查询结果

时间区间

到

指令

服务器IP

客户端IP

用户名

用户名

查询

重置

| | 操作时间 | 服务器IP | 客户端IP | 用户名 | 指令 |
|---|---------------------|----------------|--------------|----------|---------------|
| 1 | 2016-05-23 15:37:22 | 172.17.200.190 | 172.16.0.125 | ftptuser | USER ftptuser |
| 2 | 2016-05-23 15:37:11 | 172.17.200.190 | 172.16.0.125 | 4 | QUIT |
| 3 | 2016-05-23 15:36:52 | 172.17.200.190 | 172.16.0.125 | 4 | USER 4 |
| 4 | 2016-05-23 15:36:47 | 172.17.200.190 | 172.16.0.125 | ftptuser | QUIT |
| 5 | 2016-05-23 15:36:25 | 172.17.200.190 | 172.16.0.125 | ftptuser | USER ftptuser |
| 6 | 2016-05-23 15:36:19 | 172.17.200.190 | 172.16.0.125 | ftptuser | QUIT |
| 7 | 2016-05-23 15:36:00 | 172.17.200.190 | 172.16.0.125 | ftptuser | USER ftptuser |
| 8 | 2016-05-23 15:35:55 | 172.17.200.190 | 172.16.0.125 | ftptuser | QUIT |
| 9 | 2016-05-23 15:35:21 | 172.17.200.190 | 172.16.0.125 | ftptuser | USER ftptuser |

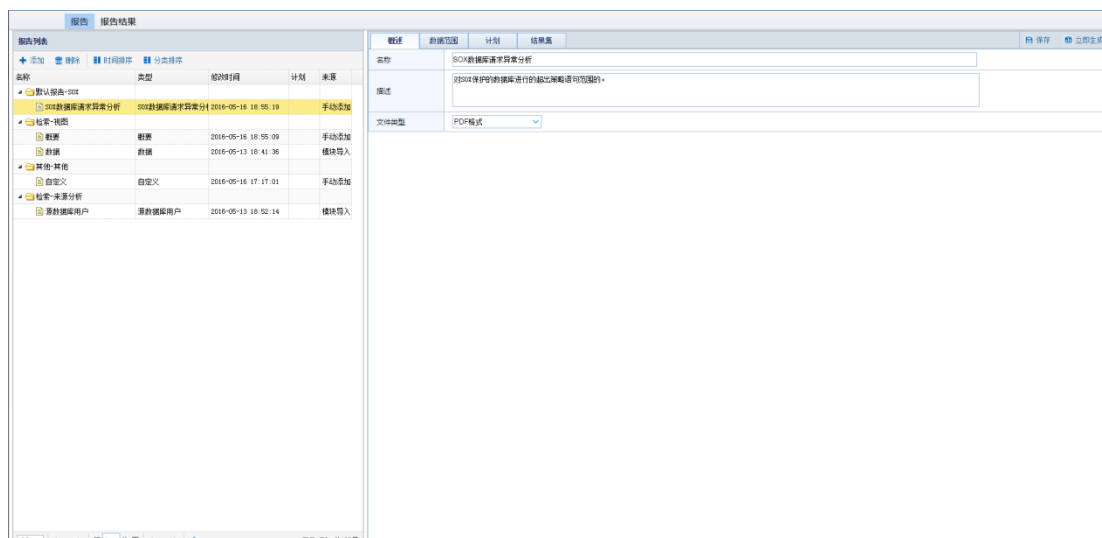
4.2 报表

所属用户：SecAdmin。

报表模块内置了报表模版，这些报告可以通过预定义模板来使用。也可以修改报告中预定义的参数，来满足不同需求。

4.2.1 报告

通过报告模块，用户可以进行添加配置报告模版，设置修改模版参数，导出报告等操作。



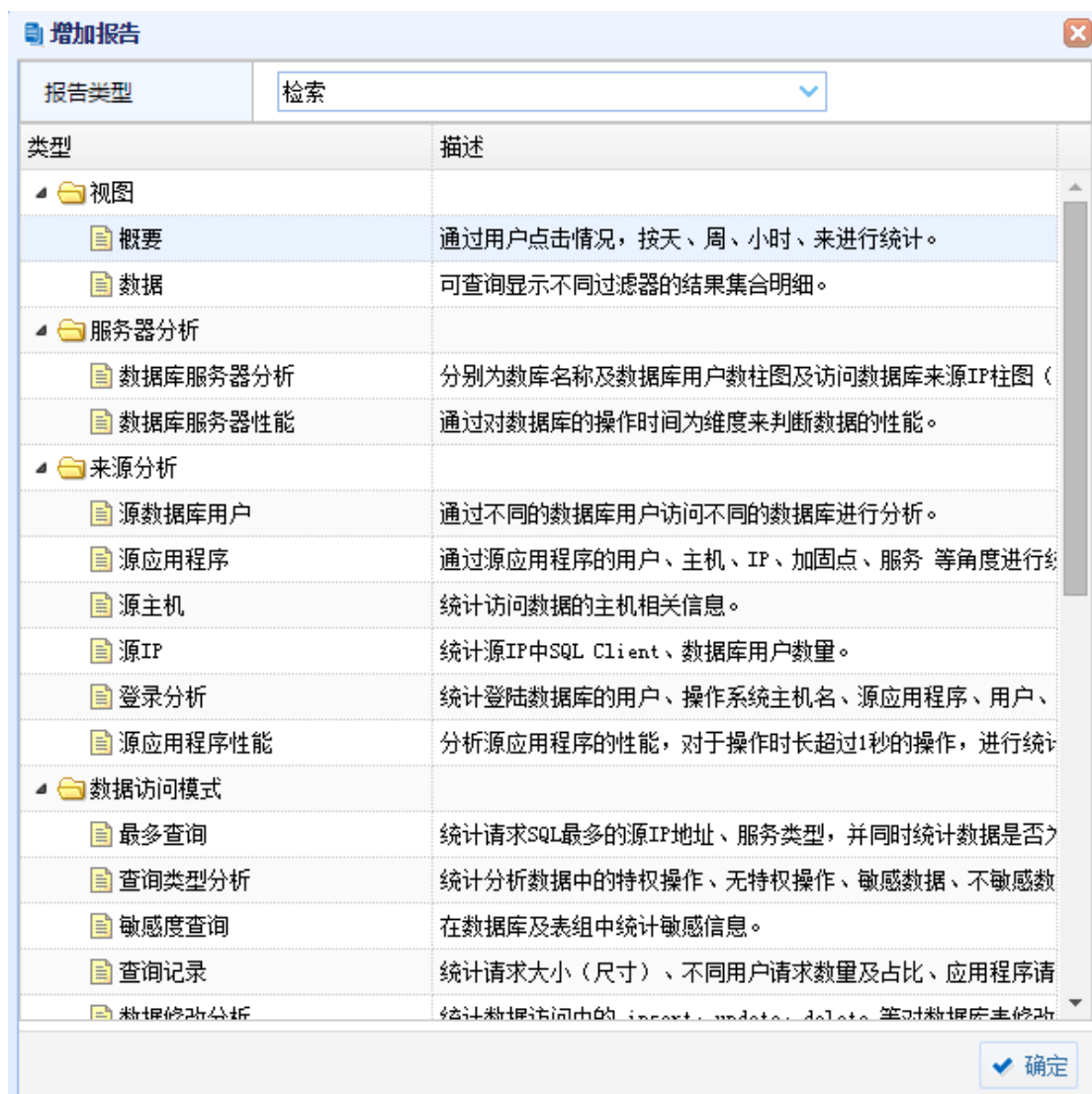
4.2.1.1 报告列表

在报告列表中，用户可进行模版添加、删除、排序。

| 报告列表 | | | | | |
|---|--------------|---------------------|----|------|--|
| <div><div><div><div><div></div><div>+</div></div><div>添加</div></div><div><div><div></div><div>删除</div></div><div>删除</div></div><div><div><div></div><div>时间排序</div></div><div>时间排序</div></div><div><div><div></div><div>分类排序</div></div><div>分类排序</div></div></div></div> | | | | | |
| 名称 | 类型 | 修改时间 | 计划 | 来源 | |
| 默认报告-SOX | | | | | |
| SOX数据库请求异常分析 | SOX数据库请求异常分析 | 2016-05-16 18:55:19 | | 手动添加 | |
| 检索-视图 | | | | | |
| 概要 | 概要 | 2016-05-16 18:55:09 | | 手动添加 | |
| 数据 | 数据 | 2016-05-13 18:41:36 | | 模块导入 | |
| 其他-其他 | | | | | |
| 自定义 | 自定义 | 2016-05-16 17:17:01 | | 手动添加 | |
| 检索-来源分析 | | | | | |
| 源数据库用户 | 源数据库用户 | 2016-05-13 18:52:14 | | 模块导入 | |

添加

点击“添加”按钮，弹出添加窗口。报告类型有“检索”、“默认报告”、“其他”三项可供选择；每项可供选择的详细条目在“类型”列表中显示，点击即可选中。通过“确定”按钮，保存选择和配置。



增加报告

报告类型默认报告

| 类型 | 描述 |
|-----------------|---------------------------------|
| 文件夹 DPA | |
| 报告 DPA数据库管理活动 | 对DPA保护的数据库进行的DDL和DCL访问。 |
| 报告 DPA数据库请求异常分析 | 对DPA保护的数据库进行的超出策略语句。 |
| 文件夹 SOX | |
| 报告 SOX数据库管理活动 | 对SOX保护的数据库进行的DDL和DCL访问。 |
| 报告 SOX数据库请求异常分析 | 对SOX保护的数据库进行的超出策略语句范围的。 |
| 报告 SOX活动用户 | 对SOX保护的数据库进行的活动状态的用户的访问情况统计。 |
| 报告 SOX活动用户（表格） | 对SOX保护的数据库进行的活动状态的用户的访问情况统计（表格） |
| 文件夹 等级保护 | |
| 报告 等保数据库管理活动 | 对等级保护的数据库进行的DDL和DCL访问。 |
| 报告 等保数据库请求异常分析 | 对等级保护的数据库进行的超出策略语句范围的。 |
| 报告 等保活动用户 | 对等级保护的数据库进行的活动状态的用户的访问情况统计。 |
| 报告 等保活动用户（表格） | 对等级保护的数据库进行的活动状态的用户的访问情况统计（表格） |
| 文件夹 医疗防统方 | |
| 报告 HIS数据库管理活动 | 对HIS保护的数据库进行的DDL和DCL访问。 |
| 报告 HIS数据库请求异常分析 | 对HIS保护的数据库进行的超出策略语句范围的。 |
| 报告 HIS活动用户 | 对HIS保护的数据库进行的活动状态的用户的访问情况统计。 |
| 报告 HIS活动用户（表格） | 对HIS保护的数据库进行的活动状态的用户的访问情况统计（表格） |

确定

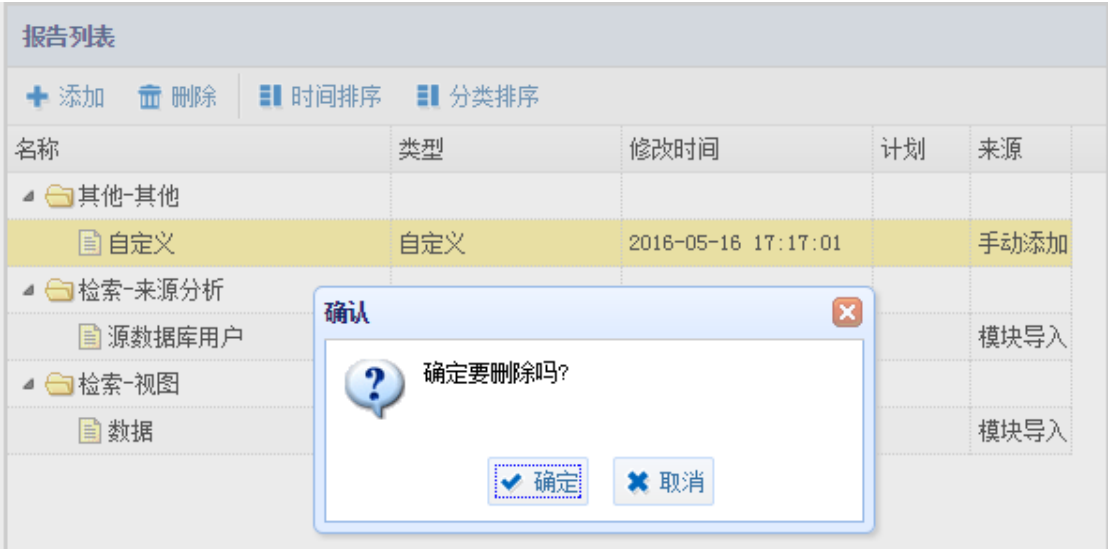
增加报告

报告类型其他

| 类型 | 描述 |
|--------|------------------------|
| 文件夹 其他 | |
| 报告 自定义 | 可自定义需要检索的数据，及所有的可显示样式。 |

删除

點選已添加的模版，点击“删除”按钮，弹出确认窗口，点击“确定”，即可成功删除。



时间排序

点击“时间排序”，系统将会把已添加的模版按照添加时间的倒序进行排序。

| 报告 报告结果 | | | | |
|---|--------|---------------------|----|------|
| 报告列表 | | | | |
| <div>+ 添加</div> <div>删除</div> <div>时间排序</div> <div>分类排序</div> | | | | |
| 名称 | 类型 | 修改时间 | 计划 | 来源 |
| 其他-其他 | | | | |
| 自定义 | 自定义 | 2016-05-16 17:17:01 | | 手动添加 |
| 检索-来源分析 | | | | |
| 源数据库用户 | 源数据库用户 | 2016-05-13 18:52:14 | | 模块导入 |
| 检索-视图 | | | | |
| 数据 | 数据 | 2016-05-13 18:41:36 | | 模块导入 |

分类排序

点击“分类排序”，系统将会把已添加的模版按类别进行排序。

| 报告 报告结果 | | | | | |
|--------------|--------------|---------------------|----|------|--|
| 报告列表 | | | | | |
| + 添加 删除 | | 时间排序 分类排序 | | | |
| 名称 | 类型 | 修改时间 | 计划 | 来源 | |
| 检索-视图 | | | | | |
| 概要 | 概要 | 2016-05-16 18:55:09 | | 手动添加 | |
| 数据 | 数据 | 2016-05-13 18:41:36 | | 模块导入 | |
| 检索-来源分析 | | | | | |
| 源数据库用户 | 源数据库用户 | 2016-05-13 18:52:14 | | 模块导入 | |
| 默认报告-SOX | | | | | |
| SOX数据库请求异常分析 | SOX数据库请求异常分析 | 2016-05-16 18:55:19 | | 手动添加 | |
| 其他-其他 | | | | | |
| 自定义 | 自定义 | 2016-05-16 17:17:01 | | 手动添加 | |

4.2.1.2 概述

概述包括名称、描述、和文件类型。名称指所生成报告的标题名称和文件命名，用户可进行手动修改配置。描述指生成文档中对内容的描述简介，用户同样可进行修改编辑。文件类型包括 PDF、EXCEL、WORD 等格式可供选择。

| | | | | |
|------|--|----|-----|---------|
| 概述 | 数据范围 | 计划 | 结果集 | 保存 立即生成 |
| 名称 | <input type="text" value="SOX数据库请求异常分析123"/> | | | |
| 描述 | <input type="text" value="对SOX保护的数据库进行的超出策略语句范围的。"/> | | | |
| 文件类型 | <div>PDF格式 PDF格式 EXCEL格式 WORD格式 CSV格式 HTML格式</div> | | | |

提示：修改配置后，需点“保存”按钮进行保存，否则不生效。

4.2.1.3 数据范围

“数据范围” 允许您将报告中包含的数据限制为选定“数据范围” 字段中的数据。配置数据范围不是必需的，但配置数据范围有助于集中关注数据的特定子集。

概述

数据范围

计划

结果集

保存

立即生成

时间范围

从：

时

到：

时

最后的：

最近一小时

过滤器

折叠

取消

操作

CHANGE
CLOSE
COMMENT
CHECKPOINT
DBCC
DEALLOCATE
DECLARE
DELETE
DENY
DISABLE

>>

<<

ALERT
CALL
COMMIT
CREATE
DROP
EXECUTE
GRANT
OTHERS
ROLLBACK
RPC

包括

不包括

展开

选取

数据库用户

展开

选取

操作对象

展开

选取

客户端IP

展开

选取

主机名

展开

选取

操作系统用户

展开

选取

客户端程序

展开

选取

SQL语句

展开

选取

SQL结果

展开

选取

SQL模型

展开

选取

引擎

展开

选取

策略

展开

选取

数据库IP

展开

选取

数据库MAC

展开

选取

客户端MAC

展开

选取

响应状态

展开

选取

字段

展开

选取

数据库类型

展开

选取

数据库实例

| 条件名称 | 操 作 | 可选元素 | 自定义 | 备注 |
|---------|---------|-------------------------------------|-----|-------|
| 时间范围 | 点选、自定义 | 最近一小时、最近一天、最近三天、最近一周、最近一个月 | 是 | |
| 客户端 IP | 点选、自定义 | 学习+IP 集 | 是 | |
| 客户端 MAC | 点选、自定义 | 自定义 | 是 | |
| 数据库 IP | 点选、自定义 | 通用配置中配置的引擎的 IP | 是 | |
| 数据库 MAC | 点选、自定义 | 自定义 | 是 | |
| 客户端程序 | 点选、自定义 | 学习+源应用程序集 | 是 | |
| 操作类型 | 点选 | None 、 Aggregate 、 BrokerPriority 等 | 否 | |
| 操作对象 | 点选、自定义 | 学习 | 是 | |
| 操作 | 点选 | 增删查改、特权操作、登入、登出。 | 否 | |
| 影响行数 | 点选+自定义值 | 大于、小于、等于、小于等于、大于等于 | 是 | |
| 字段 | 点选、自定义 | 学习+数据库列集 | 是 | 某表的某列 |
| 响应状态 | 点选 | 默认、未知、登录成功、登录失败、超时、等 | 否 | |
| 主机名 | 点选、自定义 | 学习+操作系统主机集 | 是 | |
| 操作系统用户 | 点选、自定义 | 学习+操作系统用户集 | 是 | |
| 数据库实例 | 点选、自定义 | 学习 | 是 | |
| 执行时长 | 点选+自定义值 | 大于、小于、等于、小于等于、大于等于 | 是 | 毫秒 |
| 数据库类型 | 点选 | ORACLE 、 MYSQL 、 SYBASE、CACHE 等 | 否 | |
| SQL 语句 | 点选、自定义 | 自定义 | 是 | |
| SQL 结果 | 点选、自定义 | 自定义 | 是 | |
| 数据库用户 | 点选、自定义 | 学习+数据库用户集 | 是 | |
| SQL 模型 | 点选、自定义 | 自定义 | 是 | |
| 引擎 | 点选 | 通用配置中添加的引擎 | 否 | |
| 策略 | 点选 | 策略中心中的策略 | 否 | |
| 动作 | 点选 | 通过、报警、阻断 | 否 | |

| | | | | |
|-------|---------|--------------------|---|--|
| 风险等级 | 点选 | 无风险、低风险、中风险、高风险、致命 | 否 | |
| 客户端端口 | 点选+自定义值 | 大于、小于、等于、小于等于、大于等于 | 是 | |

提示：修改配置后，需点“保存”按钮进行保存，否则不生效。

4.2.1.4 计划

在“计划”中用户可以设定时间用以自动生成报告。可设置频率、时间及发送邮件的地址。

| 概述 | 数据范围 | 计划 | 结果集 | 保存 | 立即生成 |
|------|--|--|-----|----|------|
| 启用计划 | | <input checked="" type="checkbox"/> 启用计划 | | | |
| 计划设置 | | | | | |
| 频率设置 | <input checked="" type="radio"/> 执行一次 <input type="radio"/> 重复执行 <div> “执行一次”：按配置执行一次计划，在时间条件符合时执行计划，配置不再保存； “重复执行”：按配置循环检测计划，在时间条件符合时执行计划，配置不会清除。 </div> | | | | |
| 定时设置 | <input checked="" type="radio"/> 每日计划 <input type="radio"/> 每周计划 <input type="radio"/> 每月计划 设置 整点设置： <input type="text" value="0"/> 整点 | | | | |
| 开始日期 | <input type="text" value="2016-05-17"/> | | | | |
| 发送邮件 | <input type="text"/> | | | | |

启用计划

勾选“启用计划”启用生成报告的计划任务。

| | | | | | |
|------|------|--|-----|----|------|
| 概述 | 数据范围 | 计划 | 结果集 | 保存 | 立即生成 |
| 启用计划 | | <input checked="" type="checkbox"/> 启用计划 | | | |

计划设置

频率设置，可设定计划执行的频率；分为执行一次和重复执行两个选项。

| | |
|------|---|
| 频率设置 | <div><input checked="" type="radio"/> 执行一次 <input type="radio"/> 重复执行</div> <div><p>“执行一次”：按配置执行一次计划，在时间条件符合时执行计划，配置不再保存；</p><p>“重复执行”：按配置循环检测计划，在时间条件符合时执行计划，配置不会清除。</p></div> |
|------|---|

定时设置

定时设置，可设定生成报告周期任务的执行时间、分为每日计划、每周计划、每月计划；可设定计划执行的具体整点时间。

| | |
|------|---|
| 定时设置 | <div><input checked="" type="radio"/> 每日计划 <input type="radio"/> 每周计划 <input type="radio"/> 每月计划</div> <div>设置 整点设置：<input type="text" value="0"/> 整点</div> |
|------|---|

开始日期

开始日期，可设定计划开始执行的日期。

| | |
|------|---|
| 开始日期 | <input type="text" value="2016-05-17"/> |
|------|---|

发送邮件

设定接收报告的邮箱地址

发送邮件

提示：修改配置后，需点“保存”按钮进行保存，否则不生效。

4.2.1.5 结果集

通过结果集，用户能查看到对应模版已生成的报告，并能够进行重新发送、下载和删除操作。重新发送会将报告发送到设定的邮箱中，下载会将报告下载到本地，删除则将报告从列表中删除。

| 概述 | 数据范围 | 计划 | 结果集 | 保存 立即生成 | | |
|--|---------------------|----|------|------------|--|--|
| 名称 | 生成时间 | | 发送状态 | 操作 | | |
| 1 SOX数据库请求异常分析-SOX数据库请求异常分析123_20160517C | 2016-05-17 09:22:42 | | 立即生成 | 重新发送 下载 删除 | | |
| 2 SOX数据库请求异常分析-SOX数据库请求异常分析_20160517092C | 2016-05-17 09:20:48 | | 立即生成 | 重新发送 下载 删除 | | |

4.2.1.6 “保存”按钮

在概述、数据范围、计划中修改配置后，需点“保存”按钮进行保存，否则不生效，且修改的参数会丢失。

| 概述 | 数据范围 | 计划 | 结果集 | 保存 立即生成 | | |
|----|------|----|-----|---------|--|--|
|----|------|----|-----|---------|--|--|

4.2.1.7 “立即生成”按钮

点击立即生成按钮，会根据选中的模版，和在概述、数据范围中修改的参数生成报告。并在结果集中显示。

4.2.2 报告结果

通过报告结果，用户可以浏览到所有生成的报告，包括报告的名称、生成时间、发送状态等。并能够按照类型进行筛选。通过每条报告后的重新发送、下载、删除按钮，可进行重新发送、下载和删除操作。重新发送会将报告发送到设定的邮箱中，下载会将报告下载到本地，删除则将报告从列表中删除。

| 报告 | | 报告结果 | |
|--------------------|----------------------|-----------------------------------|--|
| 类型 | <input type="text"/> | <input type="button" value="筛选"/> | |
| 报告结果 | | | |
| 名称 | 生成时间 | 发送状态 | 操作 |
| 1 SOX数据库请求异常分析-SOX | 2016-05-17 09:22:42 | 立即生成 | 重新发送 ↓ 下载 ✕ 删除 |
| 2 SOX数据库请求异常分析-SOX | 2016-05-17 09:20:48 | 立即生成 | 重新发送 ↓ 下载 ✕ 删除 |

五、 其他模块和配置

5.1 监控

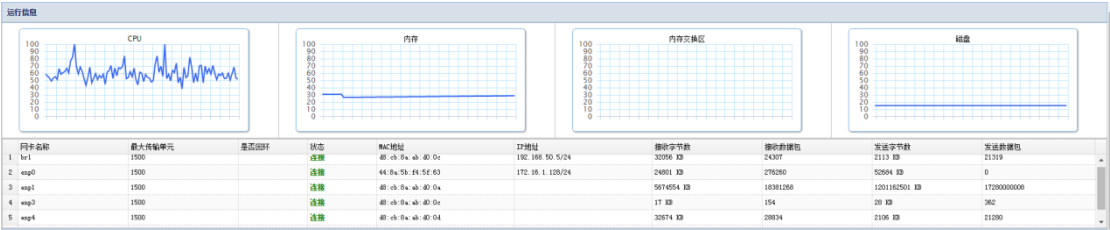
所属用户：SysAdmin、SecAdmin、Auditor。

监控这个模块，主要用检测设备的运行状态，主要包括运行信息、访问趋势、引擎列表、高风险告警列表、系统告警列表这几个模块。通过“监控”模块用户能够及时发现和解决设备存在的问题，如 CPU 占用率高，磁盘空间不足等。

5.1.1 运行信息

所属用户：SysAdmin、SecAdmin、Auditor。

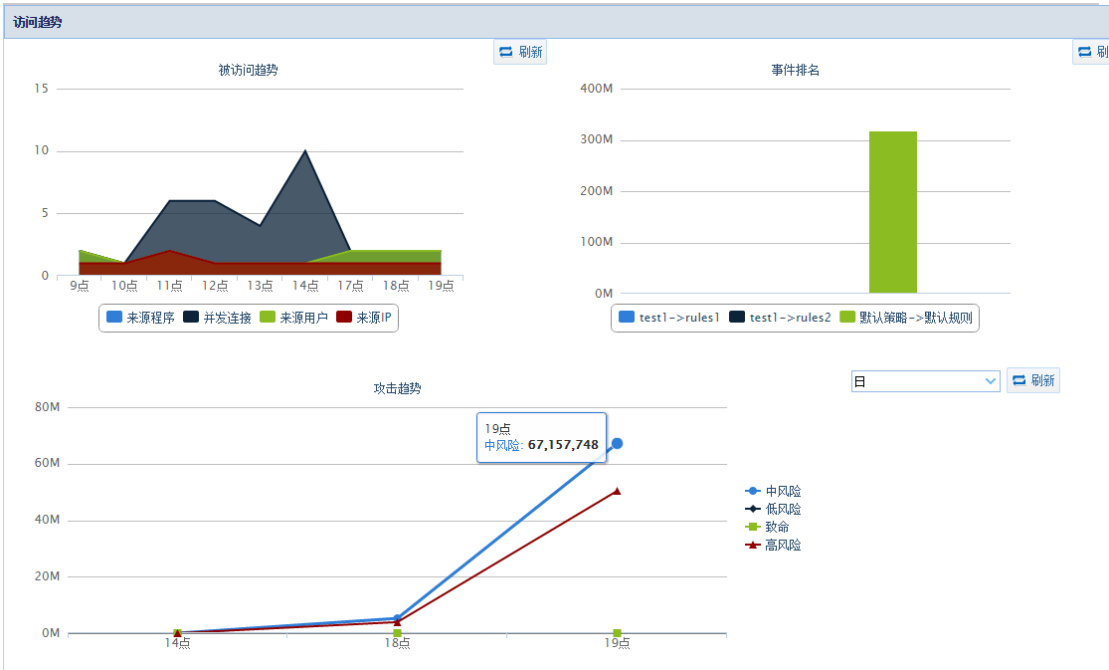
运行信息模块，包括设备的 CPU、内存、交换分区、磁盘四者的监控曲线图，以及网卡的信息（如网卡名称、最大传输单元、是否回环、状态等）。通过此模块，用户能够快速的了解设备的运行状态。如下图所示：



5.1.2 访问趋势

所属用户：SecAdmin。

访问趋势模块，包括被访问趋势、事件排名、攻击趋势三者的监控曲线图，通过此模块，用户能够快速的了解设备的访问状态。如下图所示：



5.1.3 引擎列表

所属用户：SecAdmin。

引擎列表模块，包括以下几个方面的信息，

名称：该引擎的名称。

类型：数据库的类型。

IP：该数据库引擎的 IP。

端口：数据库服务使用的连接端口。

缺省数据库：默认数据库。

如下图所示：

| 引擎列表 | | |
|---|---|---|
| 172.17.200.190:60000/test1 | 172.17.200.194:3306/testdb | 192.168.0.98:3306/mysql |
|  |  |  |
| 名称: 172.17.200.190:60000/test1 | 名称: 172.17.200.194:3306/testdb | 名称: 192.168.0.98:3306/mysql |
| 类型: DB2 | 类型: MYSQL | 类型: MYSQL |
| IP: 172.17.200.190 | IP: 172.17.200.194 | IP: 192.168.0.98 |
| 端口: 60000 | 端口: 3306 | 端口: 3306 |
| 缺省数据库: test1 | 缺省数据库: testdb | 缺省数据库: mysql |

5.1.4 高风险告警列表

- 所属用户: SecAdmin。
- 高风险告警列表模块, 主要包含以下信息,
- 审计防火墙: 引擎的类型。
- 告警规则: 设计的规则。
- 捕获时间: 捕获该 SQL 语句的具体时间。
- 数据库: 被保护的数据库。
- 数据库用户: 数据库的用户名。
- 客户端 IP: 访问该数据库的 IP。
- 处理状态: 处理的状态。
- 处理人: 具体的处理人。
- SQL 类别: 该 SQL 语句的类别。
- SQL 语句: 该 SQL 语句的具体内容。

如下图所示：

| 高风险告警列表 | | | | | | | | | | |
|---------|--------------------|----------------|-----------------|-------|----------|-----------|------|-----|--------|--------------------------------------|
| | 审计防火墙 | 告警规则 | 捕获时间 | 数据库 | 数据库用户 | 客户端IP | 处理状态 | 处理人 | SQL类别 | SQL语句 |
| 5 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Create | create table haha (name varchar(10)) |
| 6 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Delete | delete from haha where name='jack' |
| 7 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Delete | delete from haha where name='tom' |
| 8 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Create | create table haha (name varchar(10)) |
| 9 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Delete | delete from haha where name='jack' |
| 10 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Delete | delete from haha where name='tom' |
| 11 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Create | create table haha (name varchar(10)) |
| 12 | 192.168.0.99:60000 | test1->rules2: | 高 2016-05-24 19 | TEST1 | db2inst1 | 192.168.0 | | | Delete | delete from haha where name='jack' |

5.1.5 系统告警列表

所属用户：SysAdmin、SecAdmin、Auditor。

系统告警列表模块，主要有发生时间、日志类型、状态、事件级别、事件内容、处理备注几项内容，方便用户及时发现高危的报警。及时发现可能危险。

如下图所示：

| 系统告警列表 | | | | | | |
|--------|---------------------|------|-----|------|-----------------|------|
| | 发生时间 | 日志类型 | 状态 | 事件级别 | 事件内容 | 处理备注 |
| 15 | 2016-05-06 10:58:49 | 应用 | 已处理 | 警告 | 数据库审计防火墙停止完成。。。 | 12 |
| 16 | 2016-05-05 16:52:52 | 应用 | 未处理 | 警告 | 数据库审计防火墙启动完成。。。 | |
| 17 | 2016-05-05 16:51:44 | 应用 | 未处理 | 警告 | 数据库审计防火墙停止完成。。。 | |
| 18 | 2016-05-05 16:41:43 | 应用 | 未处理 | 警告 | 数据库审计防火墙启动完成。。。 | |
| 19 | 2016-05-05 16:41:25 | 应用 | 未处理 | 警告 | 数据库审计防火墙停止完成。。。 | |
| 20 | 2016-05-05 15:22:10 | 应用 | 未处理 | 警告 | 数据库审计防火墙启动完成。。。 | |

5.2 通用配置

所属用户：SysAdmin、SecAdmin、Auditor。

本模块主要进行数据库引擎添加和管理以及用户管理，

SysAdmin 用户可用此模块尽心用户的添加和管理

SecAdmin 用户可用此模块进行用户授权管理；在使用数据库审计、数据库状态监控、风险扫描等功能前都要首先在此模块添加配置相应的引擎及引擎。

Auditor 用户可用此模块进行用户授权管理。

5.2.1 SysAdmin 用户管理

SysAdmin 用户通过通用配置模块可以添加用户，并对用户授权

提示：未授权的用户只对监控模块有权限，授权后的用户对监控和系统管理两个模块有权限

5.2.1.1 用户添加

1.SysAdmin 用户进入通用配置模块在用户管理页面点击 “添加”

| 用户管理 | |
|---|-------|
| 用户列表 | |
| <div><div>+ 添加</div><div>删除</div><div>修改密码</div><div>授权</div></div> | |
| 用户名 | 角色名 |
| admin | 系统操作员 |
| admin1 | 默认管理员 |

2.弹出添加用户窗口，输入用户名和密码然后点击 “确定”

添加用户

用户名

admin2

输入密码

.....

确认密码

.....

💡 密码需以字母开头,并要包含数字,长度在8和30之间.

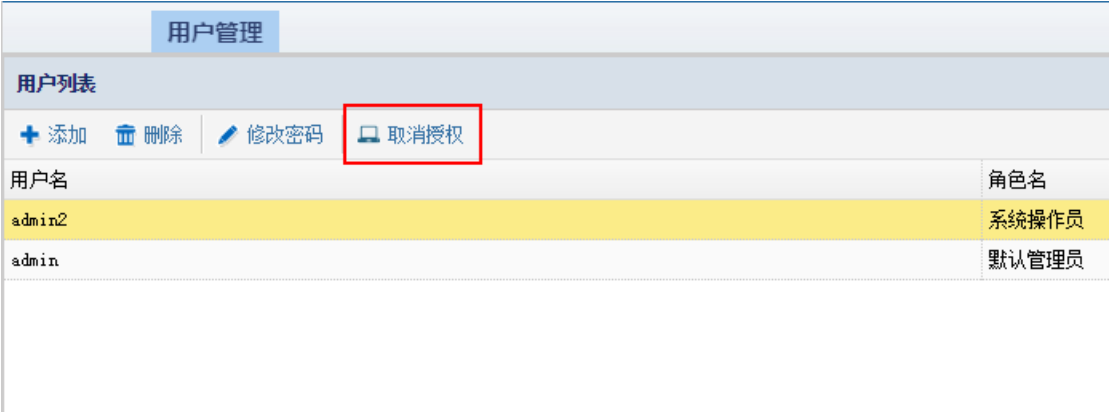
✓ 确定

5.2.1.2 授权管理

3.点选添加的用户，点击 “授权” 按钮即可对该用户授权

| 用户列表 | |
|--|-------|
| <div><div>+ 添加</div><div>🗑 删除</div><div>✎ 修改密码</div><div><div>🔑 授权</div></div></div> | |
| 用户名 | 角色名 |
| admin | 系统操作员 |
| admin2 | 系统操作员 |
| admin1 | 默认管理员 |

4.点选已授权的用户，点击 “取消授权” 按钮即可取消对该用户的授权



提示：已授权的用户“角色名”显示为系统管理员，未授权的用户“角色名”显示为默认管理员。

5.2.1.3 用户删除

點選需要删除的用户，点击 “删除” 按钮，弹出确认窗口，单击 “确定” 即可删除用户，如下图所示：



5.2.1.4 修改密码

点选需要修改密码的用户，点击 “修改密码” 按钮，弹出修改密码窗口，输入原始密码及新密码单击 “确定” 即可完成密码的修改，如下图所示：




5.2.2 Auditor 用户管理

Auditor 用户通过通用配置模块可以对 SysAdmin 用户添加但未进行授权的用户，进行授权。


提示：授权后该用户对 “系统审计” 和 “监控” 两个模块具有权限

5.2.2.1 授权管理

1.点选需要授权的用户，点击 “授权” 按钮即可对该用户授权

| 用户管理 | |
|---|-------|
| 用户列表 | |
|  | |
| 用户名 | 角色名 |
| admin | 审计操作员 |
| admin1 | 默认管理员 |

2.点选已授权的用户，点击 “取消授权” 按钮即可取消对该用户的授权

| 用户管理 | |
|---|-------|
| 用户列表 | |
|  | |
| 用户名 | 角色名 |
| admin | 审计操作员 |
| admin1 | 默认管理员 |

提示：已授权的用户“角色名”显示为审计操作员，未授权的用户“角色名”显示为默认管理员。

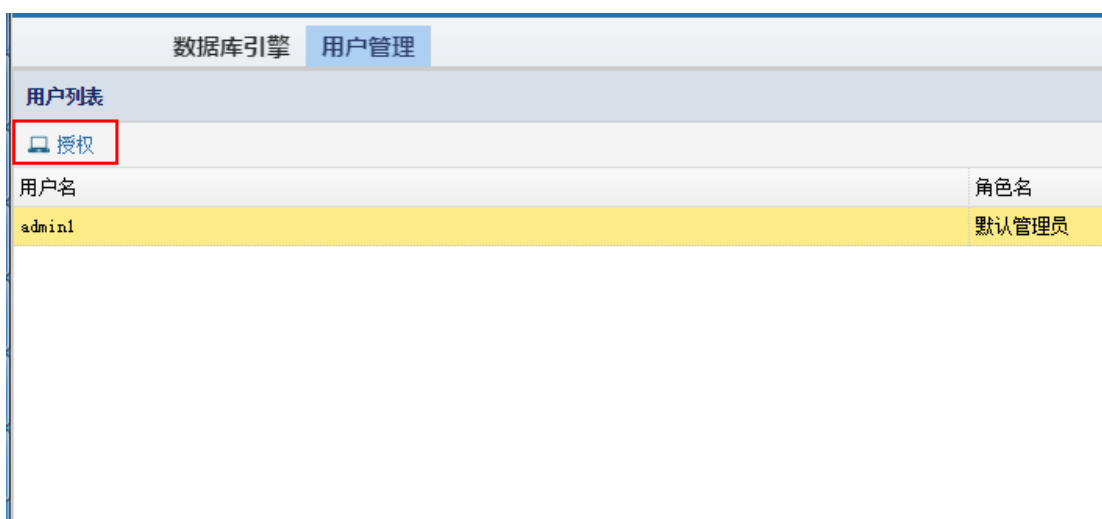
5.2.3 SecAdmin 用户管理

SecAdmin 用户通过通用配置模块可以对 SysAdmin 用户添加但未进行授权的用户, 进行授权。

提示：授权后该用户继承 Secadmin 用户除“用户管理”以外的所有权限。

5.2.3.1 授权管理

1. 点选需要授权的用户，点击“授权”按钮即可对该用户授权



2. 点选已授权的用户，点击“取消授权”按钮即可取消对该用户的授权

| 数据库引擎 用户管理 | |
|-----------------|-------|
| 用户列表 | |
| <div>取消授权</div> | |
| 用户名 | 角色名 |
| admin1 | 安全操作员 |

提示：已授权的用户“角色名”显示为安全操作员，未授权的用户“角色名”显示为默认管理员。

5.3 告警

所属用户：SecAdmin。

该模块用于显示数据库审计、防火墙的告警信息，以及对告警信息进行处理。

5.3.1 数据库告警

5.3.1.1 高风险告警

进入告警功能模块，点击 “数据库告警” > “数据库高风险”，显示风险级别为高和致命的告警信息。



告警信息按照时间倒序显示，具体功能如下：

更新

重新检索告警信息，操作方法如下：

点击“更新”按钮，则将新检索告警信息并显示。

5.3.1.2 Sql 注入风险列表

显示所有的 sql 注入风险。



具体功能如下：

更新

操作方法如下：

点击“更新”按钮，则将会重新检索告警信息并显示。

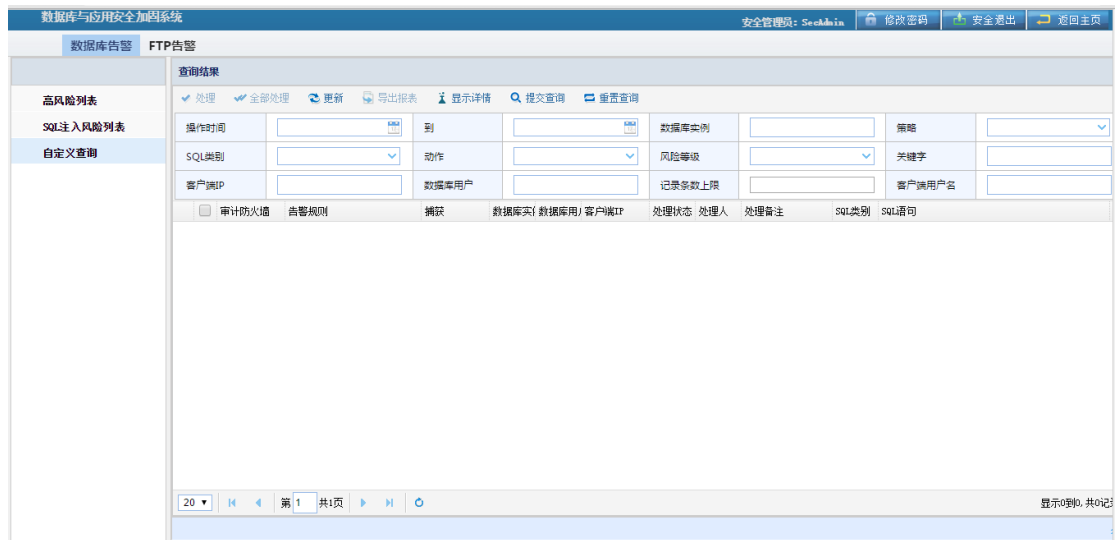
5.3.1.3 自定义查询

显示所有风险级别的告警信息，操作方法如下：

首先选择告警信息的过滤条件，条件包括操作时间、数据库实例、策略、SQL 类别、动作、风险等级、关键字、客户端 IP、数据库用户、客户端用户名；

设置好条件后，点击提交查询，则显示按照条件过滤后的告警信息。

告警信息的详情缺省不显示，如要显示，则点击页面右下角的向上的箭头，或点击显示详情按钮。



具体功能如下

处理/全部处理

对告警信息进行备注，标识已处理过此告警，操作方法如下：

1. 选中某一条或几条告警信息，选中“处理”或“全部处理”；
2. 在显示的对话框中，填写处理备注；
3. 选则确定。系统将记录处理备注，处理人和处理时间。

更新

重新检索告警信息，操作方法如下：

点击更新按钮，则将会按照当前过滤条件，重新检索告警信息并显示。

导出报表

将当前的告警信息导出为报表文件，操作方法如下：

1. 点击导出报表，显示导出条件的对话框；
2. 填写或选中导出条件，并选择确定；
3. 系统将生成报表文件，并下载。

显示详情

点击则显示告警信息的详情；

提交查询

点击则按照当前过滤条件提交查询，并显示新的告警信息；

重置查询

点击则把查询条件置为缺省值。

5.3.2 FTP 告警

查询结果

通过 FTP 告警页面可检索查看 FTP 告警信息。可以时间、服务器 IP、客户端 IP、用户名、文件名、关键字和风险等级为条件进行筛选查询。通过“重置”按钮，清楚所设置的条
件，点选相应文件，点击“批量下载”按钮可将文件下载到本地。通过“导出”按钮可将条
目以文件的形式导出到本地。

| | | | | | | | | | |
|--------------------------|-----------------------|----------------|----------------------|---------|----------------------|-------|----------------------|-----------------------------------|-----------------------------------|
| 时间范围 | <input type="text"/> | 到 | <input type="text"/> | 服务器IP | <input type="text"/> | 客户端IP | <input type="text"/> | | |
| 用户名 | <input type="text"/> | 文件名 | <input type="text"/> | 关键字 | <input type="text"/> | 风险等级 | <input type="text"/> | <input type="button" value="查询"/> | <input type="button" value="重置"/> |
| <input type="checkbox"/> | 操作时间 | 服务器IP | 客户端IP | 用户名 | 文件名 | 文件大小 | 访问 | 链接地址 | 等级 |
| 1 | 2018-05-23 15:36:40.0 | 172.17.208.190 | 172.16.0.125 | ftptest | ***** | ***** | 连接登录失败 | ***** | 警告 |

概要

在概要中能够查看到相应文件的文件名和存放路径等信息。

概要

连续登录失败！

5.4 系统审计

所属用户：Auditor。

系统审计模块记录了用户登录、登出系统，更改网卡接口设置、导出报告、等操作。

5.4.1 审计防火墙操作日志管理

通过管理模块，用户可对系统日志进行过滤筛选，可操作的条件包括：操作时间、IP、用户名、功能点、动作。用户可通过“查询”按钮按照设置的条件尽行查询，通过“重置”按钮可将查询条件恢复为缺省值（空）。

| | | | | | |
|-------------|---------------------------------------|----------|---------------------|-------------------------|--|
| 审计防火墙操作日志 | | | | | |
| 审计防火墙操作日志管理 | | | | | |
| 操作时间(开始) | 2016-05-10 17:51:52 | 操作时间(结束) | 2016-05-17 17:51:56 | IP | |
| 用户名 | | 功能点 | | 动作 | |
| 操作 | 查询 重置 | | 管理 | 以当前条件导出 | |

通过“以当前条件导出”用户可将日志的详细信息以 PDF、WORD 等文件的形式导出，以方便查阅，在弹出中可设置导出行数。

当前条件导出文件

| | |
|--|---|
| 行数 | <input type="radio"/> 全部(最多20000行) |
| | <input checked="" type="radio"/> 指定行数： <input type="text" value="500"/> (1~20000) |
| 报表格式 | <div>PDF格式</div> <div>PDF格式</div> <div>EXCEL格式</div> <div>WORD格式</div> |
| <div>确定 取消</div> | |

5.4.2 日志

日志模块显示了用户名、IP、操作时间、功能点、动作、详细信息。方便用户查看。

| 日志 | | | | | | |
|-------|----------|--------------|---------------------|-------|------|--------------------------------------|
| 序号 | 用户名 | IP | 操作时间 | 功能点 | 动作 | 详细信息 |
| 1 94 | Audi tor | 172.16.1.126 | 2016-05-16 17:33:17 | 登录系统 | 登录系统 | 登录成功! |
| 2 93 | Seckdin | 172.16.1.126 | 2016-05-16 17:33:10 | 登录系统 | 退出系统 | 退出成功! |
| 3 92 | Seckdin | 172.16.1.126 | 2016-05-16 17:17:01 | 报警 | 增加报警 | 增加报警成功, 类型: 自定义 |
| 4 91 | Seckdin | 172.16.1.126 | 2016-05-16 16:44:46 | 风险评估 | 告警处理 | 处理成功, 内容: 已处理 |
| 5 90 | Seckdin | 172.16.1.126 | 2016-05-16 15:53:03 | 登录系统 | 登录系统 | 登录成功! |
| 6 89 | Audi tor | 172.16.1.126 | 2016-05-16 15:52:57 | 登录系统 | 退出系统 | 退出成功! |
| 7 88 | Audi tor | 172.16.1.126 | 2016-05-16 15:52:55 | 登录系统 | 登录系统 | 登录成功! |
| 8 87 | Syskdm | 172.16.1.126 | 2016-05-16 15:52:46 | 登录系统 | 退出系统 | 退出成功! |
| 9 86 | Syskdm | 172.16.1.126 | 2016-05-16 15:52:44 | 登录系统 | 登录系统 | 登录成功! |
| 10 85 | Seckdin | 172.16.1.126 | 2016-05-16 15:52:40 | 登录系统 | 退出系统 | 退出成功! |
| 11 84 | Seckdin | 172.16.1.126 | 2016-05-16 14:27:02 | 登录系统 | 登录系统 | 登录成功! |
| 12 83 | Seckdin | 172.16.1.126 | 2016-05-16 14:26:55 | 登录系统 | 退出系统 | 退出成功! |
| 13 82 | Seckdin | 172.16.1.126 | 2016-05-16 14:12:17 | 登录系统 | 登录系统 | 登录成功! |
| 14 81 | Seckdin | 172.16.1.126 | 2016-05-16 13:14:19 | 登录系统 | 登录系统 | 登录成功! |
| 15 80 | Seckdin | 172.16.1.126 | 2016-05-16 10:15:55 | 审计防火墙 | 引擎控制 | 启动成功, 名称: 172.17.200.194:3306/testdb |
| 16 79 | Seckdin | 172.16.1.126 | 2016-05-16 10:15:54 | 审计防火墙 | 引擎控制 | 停止成功, 名称: 172.17.200.194:3306/testdb |
| 17 78 | Seckdin | 172.16.1.126 | 2016-05-16 10:08:02 | 登录系统 | 登录系统 | 登录成功! |
| 18 77 | Syskdm | 172.16.1.126 | 2016-05-16 10:07:57 | 登录系统 | 退出系统 | 退出成功! |
| 19 76 | Syskdm | 172.16.1.126 | 2016-05-16 10:07:45 | 登录系统 | 登录系统 | 登录成功! |
| 20 75 | Syskdm | 172.16.1.126 | 2016-05-16 10:06:33 | 登录系统 | 登录系统 | 密码错误, 帐号已被锁定, ---!---后再登录! |