明御数据库审计及风险控制系统 V4.6

—用户使用手册

杭州安恒信息技术有限公司

二〇一六年一月

目录

1 产品简介

1.1 产品概述

明御®数据库审计与风险控制系统（简称：DAS-DBAuditor）是安恒信息在多年数据库安全理论研究与实践的基础上，结合各类法令法规（如等级保护、分级保护、企业内控、SOX、PCI 等）对数据库安全的要求，自主研发的业界首创细粒度审计、双向审计、全方位风险控制的数据库安全审计产品。可帮助用户带来如下价值点：

- 全面记录数据库访问行为，识别越权操作等违规行为，并完成追踪溯源
- 提供细粒度、灵活的规则和查询条件，对违规行为进行告警（通过邮件、短信、SYSLOG 等方式）
- 跟踪敏感数据访问行为轨迹，建立访问行为模型，及时发现敏感数据泄漏
- 检测数据库配置弱点、发现 SQL 注入等漏洞、提供解决建议
- 为数据库安全管理与性能优化提供决策依据
- 提供符合法律法规的报告，满足等级保护、企业内控等审计要求

本系统采用目前业界最流行的 B/S 架构，用户可以方便的通过网络对系统的运行状况、数据库的受攻击程度进行操作、监控。同时在很大程度上减少用户对系统成本的投入，减少维护成本。

1.2 产品功能

DAS-DBAuditor 产品功能分成原始信息收集、审计信息标准化、审计信息筛选、预警与报表共四大模块。

1. 原始信息收集

- 通过旁路镜像的模式部署
- 不改变用户现有网络结构
- 不占用数据库服务器资源
- 不影响数据库性能
- 支持分布式部署
- 实现配置与报表的集中管理
- 并发流量采集与处理、多点存储、多级管理
- 自动定期发现功能，及时发现一些未知数据库

2. 审计信息标准化

- 支持国内外主流数据库，包括 Oracle、SQL server、DB2、MySQL、Informix、Sybase、PostgreSQL 、神通 OSCAR、达梦 DM、人大金仓、南大通用 Gbase、CACHé 、Teradata 共 13 种协议
- 将不同数据库协议按照标准化的格式进行展示，方便管理人员阅读和分析

3. 审计信息筛选

- 根据 5W1H(WHAT，WHERE，WHEN，WHO，WHY，HOW)分析模型进行规制设计，提供丰富的规则条件和向导式的规则配置方法
- 内置了 300 多条安全相关的审计分析规则
- 根据采集到的数据进行数据分析和产生行为模型
- 审计结果综合查询、WEB 查询、会话回放功能；还有针对历史数据的旧版本数据查询、恢复内容查询

4. 预警与报表

- 提供 SYSLOG、短信、邮件、SNMP、FTP 等丰富的告警通知方式，可第一时间通知管理人员
- 可与 SOC、安管平台等进行日志的整合
- 内置了 40 多种高价值、符合法律法规的分析报表，可从数据库账号增删、密码修改、权限变更、高危操作、违规告警、账号复用、数据库性能分析等角度进行分析
- 支持自定义的方式定制更多报表

1.3 产品特点

1. 采用多核、多线程并行处理技术，处理性能遥遥领先

该产品选用国际领先的、最适合审计产品特性的硬件平台，通过 intel 多核 CPU 的强大计算能力，以及安恒信息独有的多线程分布式处理技术，使得安恒数据库审计系统的处理能力大大提升，真正领先于国内同类型产品。

2. 数据库安全配置分析和漏洞评估

该产品继承了安恒信息数据库安全漏洞扫描技术优势，形成了从漏洞扫描、安全审计为一体的解决方案。可通过定制化任务方式实现周期性的自动扫描，发现数据库的配置不合理项、弱口令、安全漏洞。并可根据漏洞情况提供合理的安全建议和审计规则，生成安全漏洞扫描报告。

3. 智能关联分析

通过同时提取WEB业务端和数据库端的协议流量，提取出具体业务操作请求URL、POST/GET值、业务账号、原始客户端 IP、MAC 地址、提交参数等。通过智能自动多层关联，关联出每条 SQL 语句所对应 URL，以及其原始客户端 IP 地址等信息，实现追踪溯源。

4. 独有的双向审计

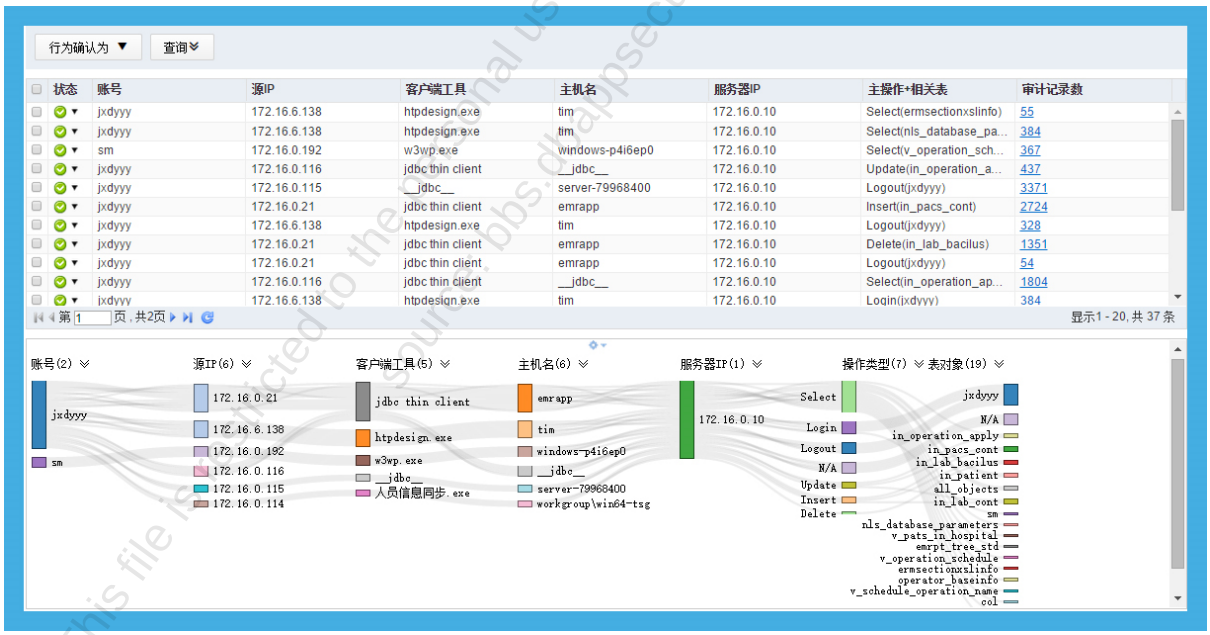
该产品可以实现真正的双向审计。双向审计不但包含了 SQL 语句执行状态、返回行数、返回时间等基本信息，最为关键是包含了数据库的返回结果内容。如图 1-1 所示。

图1-1 双向审计

5. 数据库行为轨迹分析

该产品通过创新的行为轨迹分析方法，使得审计员摆脱了从成千上万条日志进行枯燥分析的烦恼，大大提高了分析效率，提高了审计的易读性和价值。如图 1-2 所示。

图1-2 行为轨迹分析



6. 数据库行为模型分析

该产品通过自动学习建立数据库行为模型，行为模型是基于“总—分”逻辑分析思维，一层一层展示整个数据库的行为状态。通过行为模型的变更分析，可方便用户掌握最新访问动态。通过行为模型的对比分析则可以分析出两个不同时间段的模型差异，可以非常方便的发现数据库账号、源 IP、访问工具类型、权限的增删变更情况，方便进一步追踪分析。如图 1-3 所示。

图1-3 对比分析

2 WEB 概述

2.1 功能简介

通过 WEB 方式管理数据库审计系统。

2.2 WEB登录

2.2.1 通用版本

(1) 在浏览器中输入 *https://Admin 管理 IP*，进入登录窗口。如图 2-1 所示。

(2) 在登录窗口中输入用户名、密码。

图2-1 登录

(3) 单击<登录>后即可登录到整体概况页面，如图 3-1 所示。

说明

出厂默认 Admin 管理 IP 为：192.168.1.100

出厂默认用户名/密码为：admin/Dbapp@2013

2.2.2 医疗防统方专业版

登录步骤和通用版本一样，登录窗口有医疗防统方专版标识，如图 2-2 所示。

图2-2 医疗防统方专版

2.3 退出WEB登录

在数据库审计系统页面上点击(如图 2-3)，退出 WEB 登录。

退出系统时，系统不会自动保存当前配置。因此建议用户在退出系统前先设置保存当前配置。

注意

通过直接关闭浏览器标签的方式，已登录到设备上的用户不能自动退出登录。

2.4 WEB页面布局

WEB 页面布局共分为：功能页签、管理链接、导航树和操作区四部分。如图 2-3 所示。

图2-3 WEB 页面布局

WEB 页面布局序号说明参见表 2-1。

表2-1 WEB 页面布局序号说明

序号	名称	说明
(1)	功能页签	以不同的角度提供了各类管理功能的配置入口，方便管理员根据实际需要进行切换
(2)	管理链接	显示了当前登录的操作员信息以及退出等相关功能链接
(3)	导航树	列出了当前功能页签对应的操作链接
(4)	操作区	该区域主要用于信息展示以及相关功能的操作

3 主页

3.1 数据分析

3.1.1 整体概况

1. 功能简介

整体概况可以帮助用户了解被审计服务器的整体情况和状态，具体包括以下几个方面的内容：

- 当前数据库核心指标
- 审计记录数对比

- 最新告警
- 行为模型

用户 WEB 登录后，默认进入[整体概况]菜单的页面。如图 3-1 所示。

图3-1 整体概况

2. 当前数据库核心指标

在数据库 IP 列表中，选择 IP，查看对应数据库核心指标。指标说明参见表 3-1。

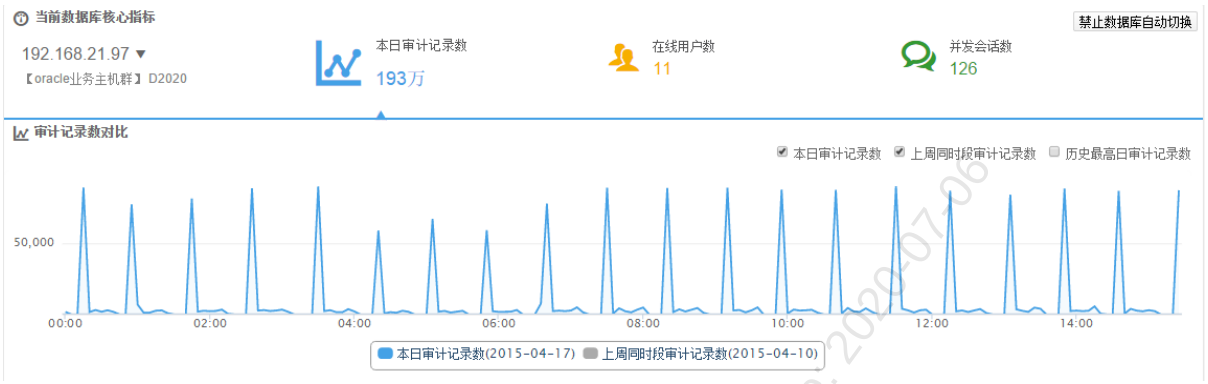
表3-1 数据库核心指标

指标	说明
本日审计记录数	统计本日审计的总记录数
在线用户数	显示当前的在线用户数
并发会话数	显示在线的并发会话数

3. 审计记录数对比

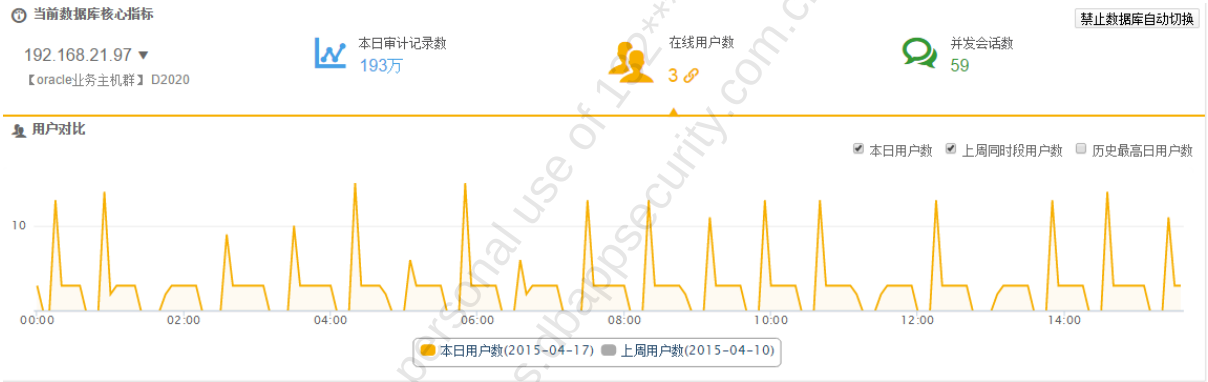
(1) 单击本日审计记录数，查看本日与本周及历史最高日审计记录数对比曲线图。如图 3-2 所示。

图3-2 本日审计记录数对比



(2) 单击在线用户数，查看本日与本周及历史最高日用户数对比曲线图。如图 3-3 所示。

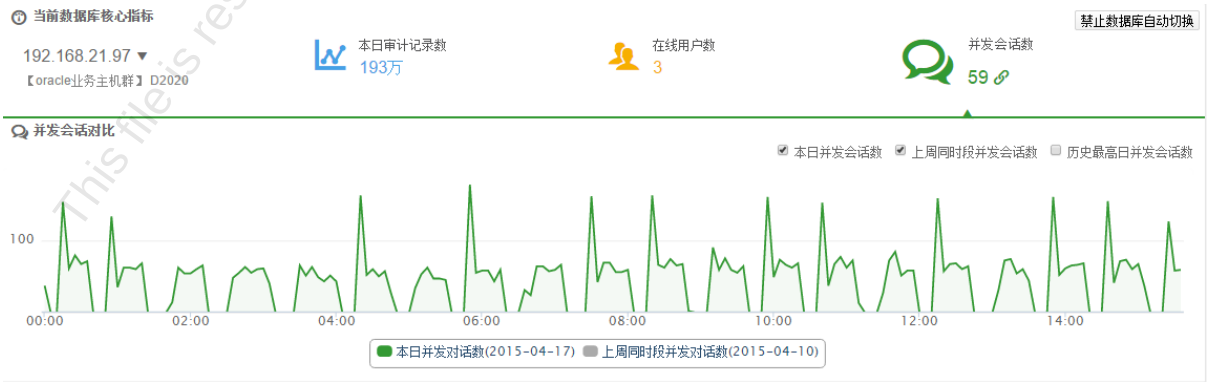
图3-3 用户数对比



(3) 并发会话数

单击并发会话数，查看本日与本周及历史最高日并发会话数对比曲线图。如图 3-4 所示。

图3-4 并发会话数对比



4. 最新告警

显示当日未处理的告警。包括高、中、低和关注行为四种告警，并循环显示每一条告警。如图 3-5 所示。

图3-5 最新告警

图中序号说明参见表 3-2。

表3-2 最新告警序号说明

序号	说明
(1)	单击报警数，查看对应的告警列表
(2)	单击此图标，链接到[风险/告警/查询]页面
(3)	单击每一条告警，查看告警的详细信息

5. 行为模型

显示当前数据库用户行为模型。如图 3-6 所示。

图3-6 行为模型

行为模型显示信息说明参见表 3-3。

表3-3 行为模型显示信息

标题项	说明
服务器IP	数据库服务器IP
账号/应用账号	统计分析登录数据库账号情况
源IP/应用源IP	统计分析源IP/应用源IP情况
客户端工具	统计分析登录数据库服务器使用的客户端工具情况
表对象	统计分析操作数据库中表对象情况
操作类型	统计分析对数据库进行的操作类型

说明

行为模型标题项后面的红色小球里面的数字表示新增行为。

3.1.2 趋势分析

1. 功能简介

对不同数据库的审计数据进行趋势分析和对同一数据库不同源 IP 数据进行趋势分析。

2. 趋势分析配置

(1) 通过[主页/数据分析/趋势分析]，进入趋势分析页面。如图 3-7 所示。

图3-7 趋势分析

(2) 趋势分析配置。选项说明参见表 3-4。

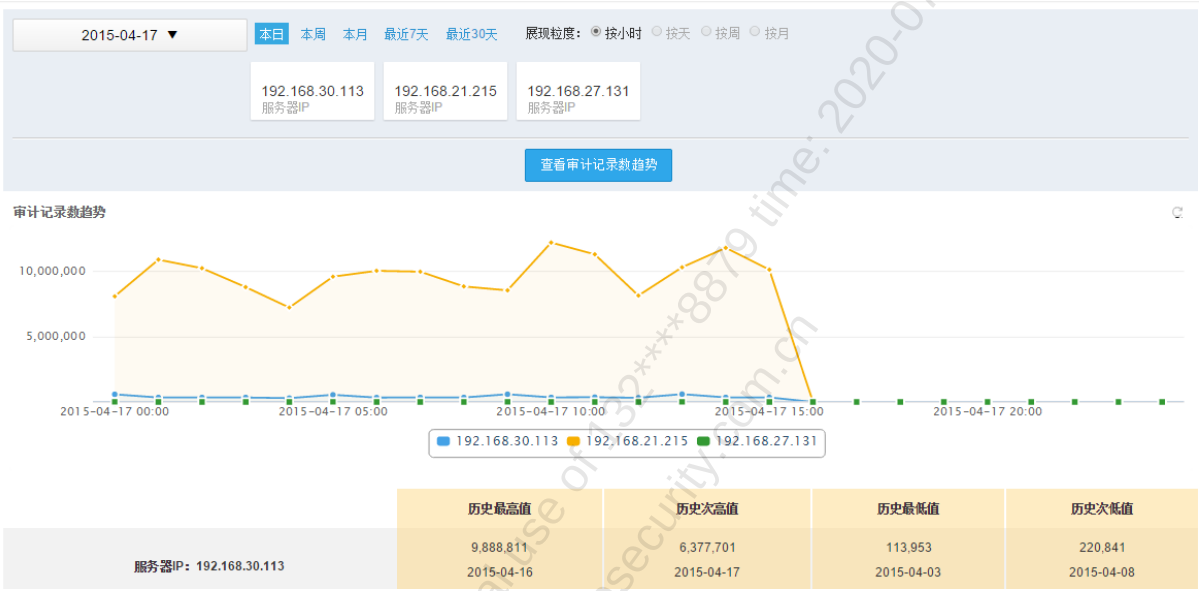
表3-4 趋势分析选项说明

选项		说明
时间段		可以快速选择本日、本周、本月、最近7天或最近30天，同时单击日期，支持自定义时间段。范围：1~365天
展现粒度		按小时、按天、按周或按月
添加服务器IP	不同服务器之	分析不同数据库服务器的趋势，最多支持3个服务器

	间分析	
	同一服务器不同来源IP分析	分析同一服务器不同来源IP的趋势， (1) 先选择一个服务器 IP (2) 再添加来源 IP，最多支持 3 个来源 IP

(3) 单击<查看审计记录数趋势>，查看趋势分析结果。如图 3-8 所示。

图3-8 趋势分析结果图



3.1.3 对比分析

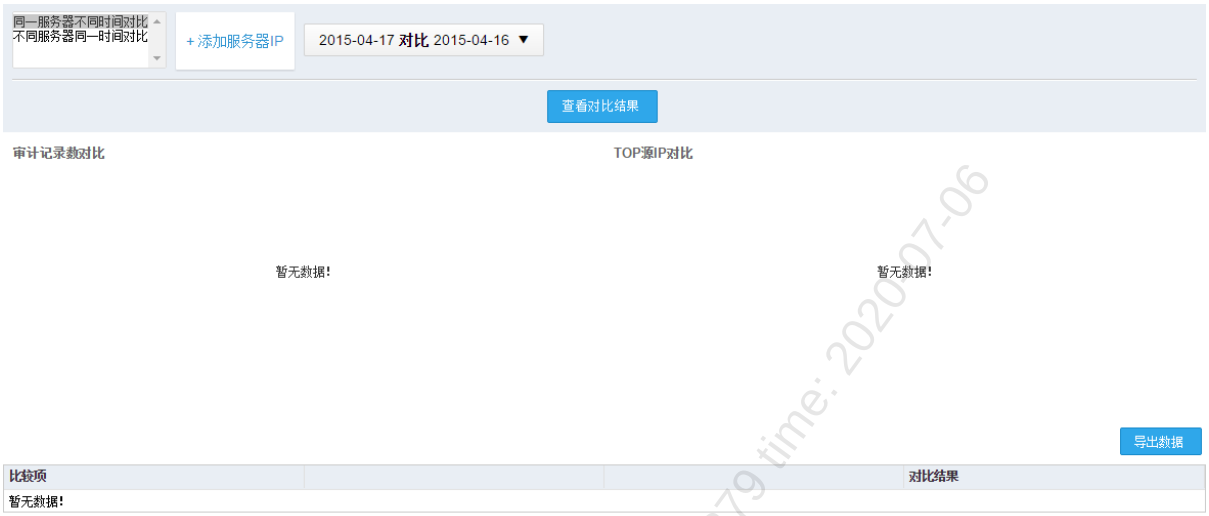
1. 功能简介

对同一服务器不同时间审计情况对比分析和对不同服务器同一时间审计情况对比分析。

2. 对比分析配置

(1) 通过[主页/数据分析/对比分析]，进入对比分析页面。如图 3-9 所示。

图3-9 对比分析



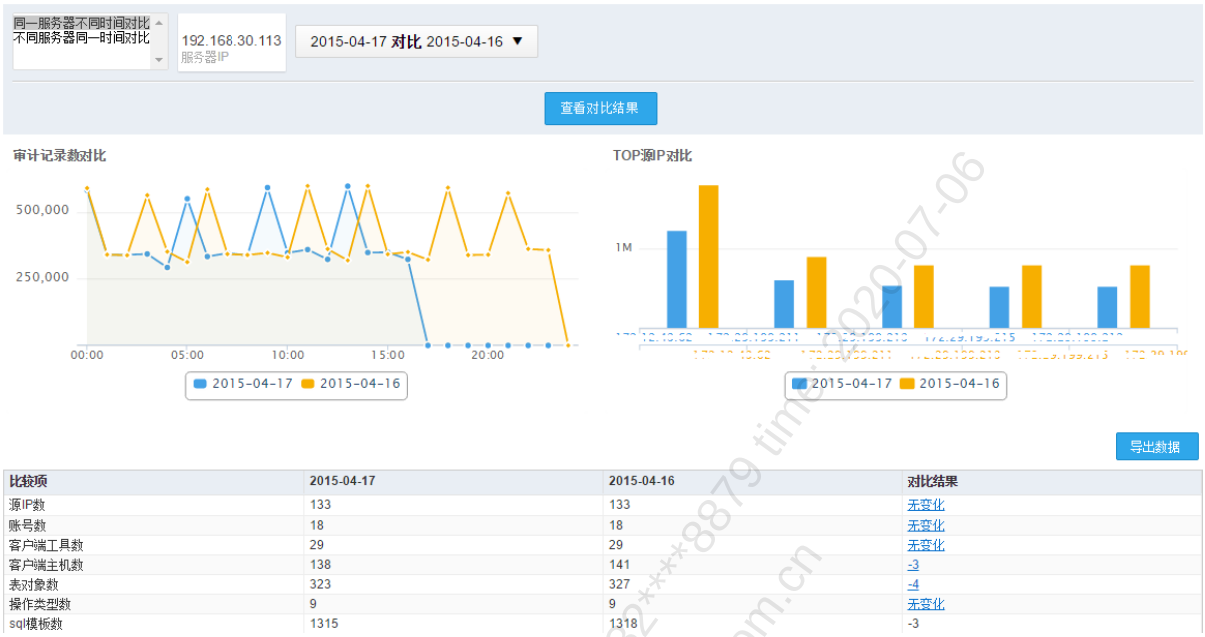
(2) 选择对比分析类型、服务器和对比分析时间段。选项说明参见表 3-5。

表3-5 对比分析选项说明

选项		说明
对比类型	同一服务器不同时间对比	针对同一服务器，不同时间段对比分析
	不同服务器同一时间对比	针对不同服务器，相同时间段对比分析
服务器IP		选择对比分析的服务器IP • 对比类型为同一服务器不同时间对比时，选择一个服务器 IP • 对比类型为不同服务器同一时间对比时，选择两个服务器 IP
时间段		按天、月、季度或自定义

(3) 单击<查看对比结果>，查看对比分析的结果。如图 3-10 所示。

图3-10 对比分析结果图



比较项	2015-04-17	2015-04-16	对比结果
源IP数	133	133	无变化
账号数	18	18	无变化
客户端工具数	29	29	无变化
客户端主机数	138	141	-3
表对象数	323	327	-4
操作类型数	9	9	无变化
sql模板数	1315	1318	-3

3.2 行为模型

3.2.1 新增行为

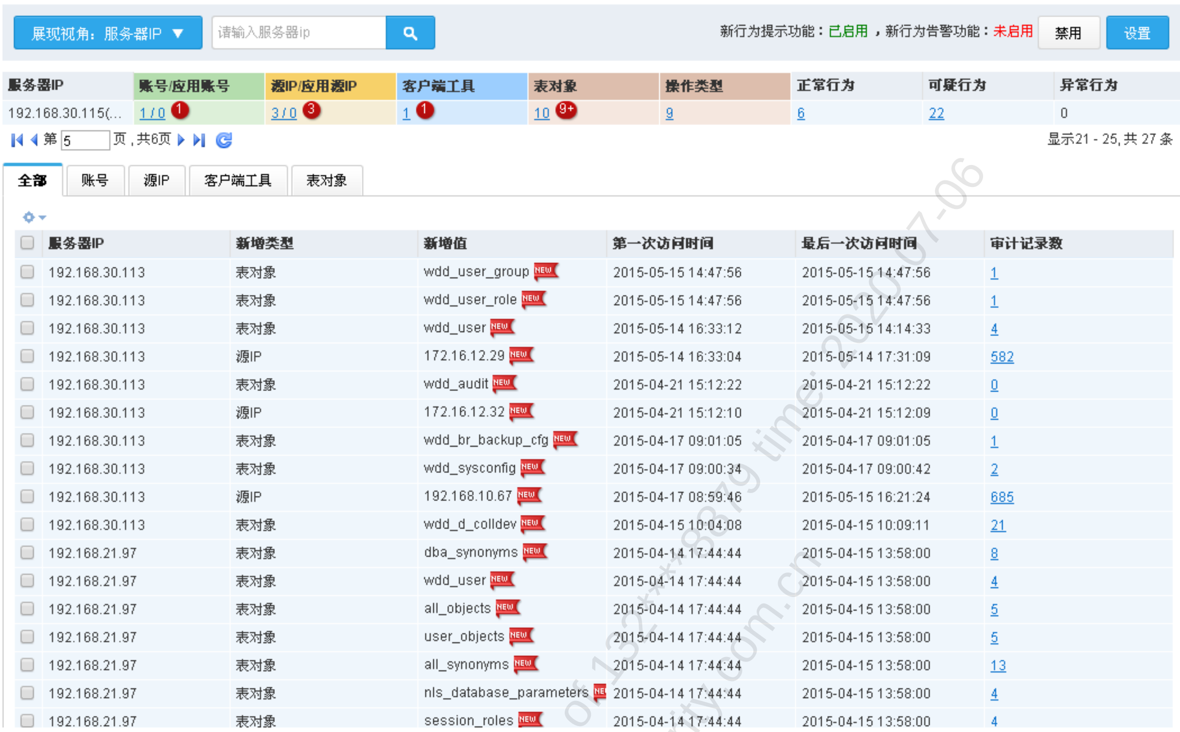
1. 功能简介

新增行为页面主要是针对用户行为对服务器访问账号、源 IP、客户端工具行为进行汇总统计。

2. 新增行为配置

通过[主页/行为模型/新增行为]进入新增行为页面。如图 3-11 所示。

图3-11 行为模型



新增行为列表内容说明参见表 3-6。

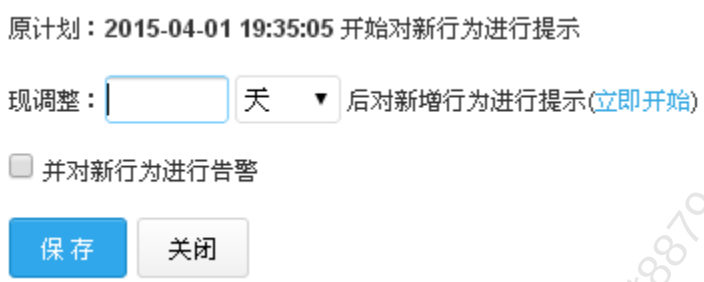
表3-6 新增行为列表说明

选项	说明
服务器IP	对应服务器IP，可通过输入服务器IP过滤查看某一具体的服务器统计信息
账号/应用账号	对应账号统计值，点击具体数字，可查看详细账号信息
源IP/应用源IP	对应访问IP统计值，点击具体数字，可查看详细各个访问IP信息量
客户端工具	对应访问使用客户端工具统计值，点击具体数字，可查看详细客户端工具
表对象	对应表对象统计值，点击具体数字，可查看具体的对象信息
操作类型	对应数据库操作类型统计值，点击具体数字，可查看详细操作类型
正常行为	指用户访问的正常行为统计值，点击具体数字，切换到详细查询页面，查看详细正常行为
可疑行为	指用户访问的可疑行为统计值，点击具体数字，切换到详细查询页面，查看详细可疑行为
异常行为	指用户访问的异常行为统计值，点击具体数字，切换到详细查询页面，查看详细异常行为
新增类型	指新增类型，包括账号、源IP、客户端工具、表对象
新增值	指具体的新增内容
第一次访问时间	指第一次访问的时间

最后一次访问时间	指最近一次访问的时间
审计记录数	记录对应的审计数，点击具体数字，切换到详细查询页面，查看详细行为

点击<设置>按钮，可以在打开的页面中设置新行为提示时间及是否对新行为进行告警，如图 3-12 所示。

图3-12 行为提示设置



3.2.2 账号视图

1. 功能简介

账号视图页面主要是显示具体的账号信息及各个账号对应的各维度的统计信息。

2. 账号视图配置

单击[主页/行为模型/账号视图]，进入账号视图页面，如图 3-13 所示。具体的信息说明可参见表 3-6。

图3-13 账号视图

3.2.3 源 IP 视图

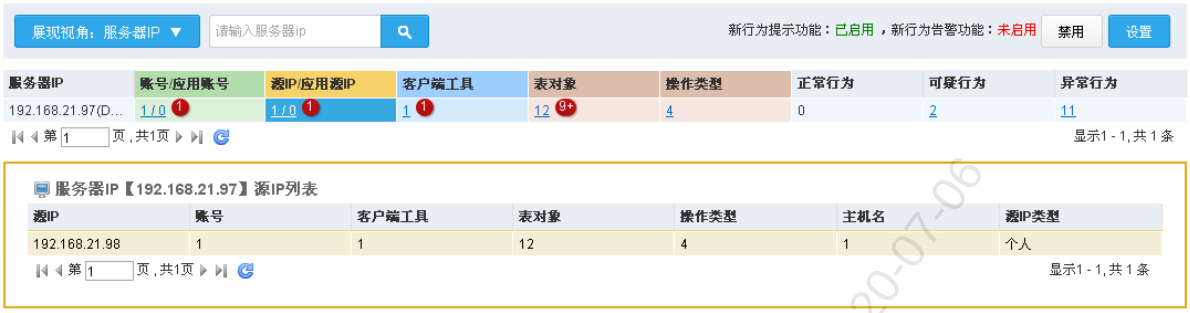
1. 功能简介

源 IP 视图页面主要是显示具体的源 IP 信息及各个源 IP 对应的各维度的统计信息。

2. 源 IP 视图配置

单击[主页/行为模型/源 IP 视图]，进入源 IP 视图页面，如图 3-14 所示。具体的信息说明可参见表 3-6。

图3-14 源 IP 视图



3.2.4 工具视图

1. 功能简介

工具视图页面主要是显示具体的工具信息及各个工具对应的各维度的统计信息。

2. 工具视图配置

单击[主页/行为模型/工具视图]，进入工具视图页面，如图 3-15 所示。具体的信息说明可参见表 3-6。

图3-15 工具视图

3.2.5 权限视图

1. 功能简介

权限视图页面主要是显示具体的权限信息及各个权限对应的各维度的统计信息。

2. 权限视图配置

单击[主页/行为模型/权限视图]，进入权限视图页面，如图 3-16 所示。具体的信息说明可参见表 3-6。

图3-16 权限视图

3.2.6 详细查询

1. 功能简介

详细查询页面主要是对用户的具体行为进行查询，并产生模型图。

2. 详细查询配置

单击[主页/行为模型/详细查询]，进入详细查询页面，如图 3-17 所示。具体的信息说明可参见表 3-6。

图3-17 详细视图

点击<查询>按钮，配置过滤条件，查询后，会出对应的行为轨迹图，如图 3-18 所示：

图3-18 行为轨迹

说明

- 默认打开详细页面时，不会出行为轨迹图，只有通过查询或从其它页面跳转到详细页面时，才会出行为轨迹图。
- 行为轨迹图不支持 IE9 以下版本，使用 IE9 或 IE9 以上版本、Chrome、FireFox 才能绘制。

3.3 医疗防统方专业版

3.3.1 统方监控

1. 功能简介

统方监控在医疗防统方专业版特有页面，可以帮助用户统方告警情况，具体包括以下几个方面的内容：

- 本机运行状态
- 告警信息
- 统方告警

防统方专业版的用户 WEB 登录后，默认进入[统方监控]菜单的页面。如图 3-19 所示。

图3-19 统方监控

4 审计配置

4.1 基本步骤

首先介绍系统审计操作步骤。

(1) 部署系统后，登录系统。如图 4_1 所示。

图4-1 登录系统

(2) 增加保护对象。

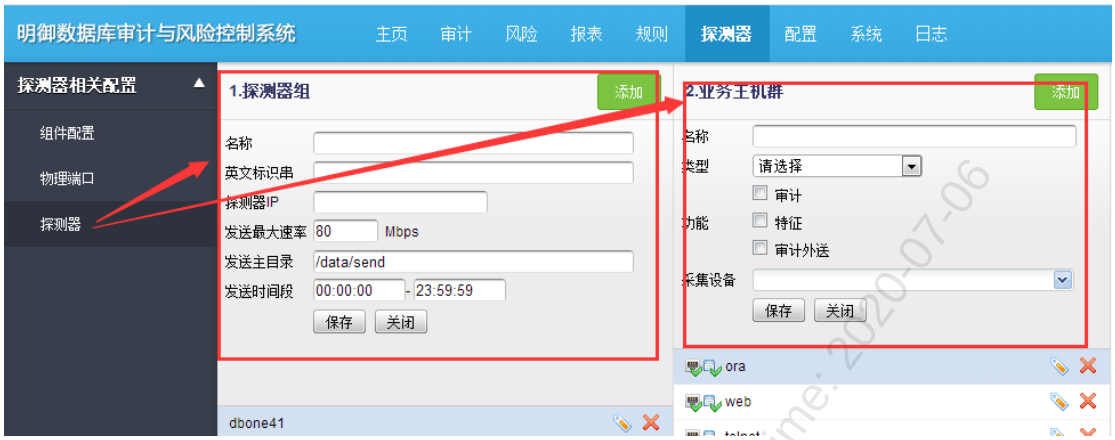
单击[探测器/物理端口/新增]，增加保护对象的 IP、业务类型、版本、端口、运行环境和流量方向。如图 4_2 所示。具体参见 4.2.2 物理端口。

图4-2 增加保护对象

(3) 增加探测器和业务主机群。

进入[探测器/探测器]页面，单击探测器组后面的<添加>，添加探测器。单击业务主机群后面的<添加>，为相应的探测器添加业务主机群。如图 4_3 所示。具体参见 4.2 探测器。

图4-3 增加探测器和业务主机群



(4) 挂载物理端口。

首先选择探测器组合业务主机群，之后选择需要挂载物理端口，单击<挂载>，将物理端口挂载到对应的业务主机群上。

图4-4 挂载端口

(5) 开启引擎。

进入[配置/常规/引擎管理]页面，开启审计引擎。如图 4_5 所示。

图4-5 开启引擎

(6) 查询审计数据。在镜像和端口挂载正常，并且挂载端口有 SQL 流量时，可以通过系统查询审计数据。

进入[审计/日常行为/综合查询]，打开查询页面，点击【查询】，进行审计数据查询。如图 4_6 所示。具体参见 4.3 审计查询。

图4-6 综合查询

4.2 探测器

4.2.1 组件配置

1. 配置准备

已经确认好此台设备数据接收的时间、速率等信息。

2. 配置组件信息

进入[探测器/探测器相关配置/组件配置]界面中进行配置，如图 4-7 所示。

图4-7 组件配置

配置项具体说明如表 4-1。

表4-1 配置组件

配置项	说明
服务组件选择	数据中心也可以作为探测器使用 当本机身份为探测器时，只能查看组件配置，不能修改组件配置
管理口配置	管理口配置只能连接到后台串口进行修改
数据中心配置	只有在本机身份为数据中心时才能看到此项配置 • 数据接收传输端口有效范围：1024 ~65535 • 数据接收最大速率有效范围：1~1000Mbps • 数据接收时间段参数 若本机身份为探测器时，无此项功能

4.2.2 物理端口

1. 配置准备

确认好是哪台数据库或 WEB 等需要配置成保护对象，如数据库还需要确认好版本等相关信息。

2. 配置物理端口

(1) 进入[探测器/探测器相关配置/物理端口]界面，显示物理端口列表。如图 4-8 所示。

图4-8 物理端口列表

IP	端口	业务类型	版本	运行环境	挂载次数	流量方向	来源	操作
192.168.21.67	3306	MYSQL	5.1	linux	1	双向	手工添加	编辑
192.168.21.74	*	ORACLE	9i	win	1	双向	手工添加	编辑
192.168.21.75	1521	ORACLE	10g	win	1	双向	手工添加	编辑
192.168.21.75	1522	ORACLE	10g	win	1	双向	手工添加	编辑
192.168.21.79	1433	SQLSERVER	2005	ucs-2	1	双向	手工添加	编辑
192.168.21.85	50000	DB2	v95	win	1	双向	手工添加	编辑
192.168.21.87	1433	SQLSERVER	2008	ucs-2	未挂载	双向	手工添加	编辑 删除
192.168.21.97	1521	ORACLE	11g	win	1	双向	手工添加	编辑
192.168.21.98	80	WEB	全部		未挂载	双向	手工添加	编辑 删除
192.168.21.98	1521	ORACLE	10g	win	1	双向	端口扫描	编辑
192.168.25.250	80	WEB	全部		1	双向	手工添加	编辑
192.168.25.45	8080	WEB	全部		1	双向	手工添加	编辑
192.168.27.49	1521	ORACLE	11g	win	1	双向	手工添加	编辑
192.168.27.51	80	WEB	全部		1	双向	手工添加	编辑
192.168.27.62	1521	ORACLE	10g	win	1	双向	手工添加	编辑
192.168.3.21	80	WEB	全部		1	双向	手工添加	编辑
192.168.30.10	1521	ORACLE	10g	aix	1	双向	手工添加	编辑
192.168.30.11	1521	ORACLE	10g	aix	1	双向	手工添加	编辑
192.168.30.12	1521	ORACLE	10g	aix	1	双向	手工添加	编辑
192.168.30.229	3306	MYSQL	5.1	linux	1	双向	手工添加	编辑

(2) 单击<新增>按钮，进入新增界面，输入相关的配置信息进行配置。如图 4-9 所示。

图4-9 新增物理端口

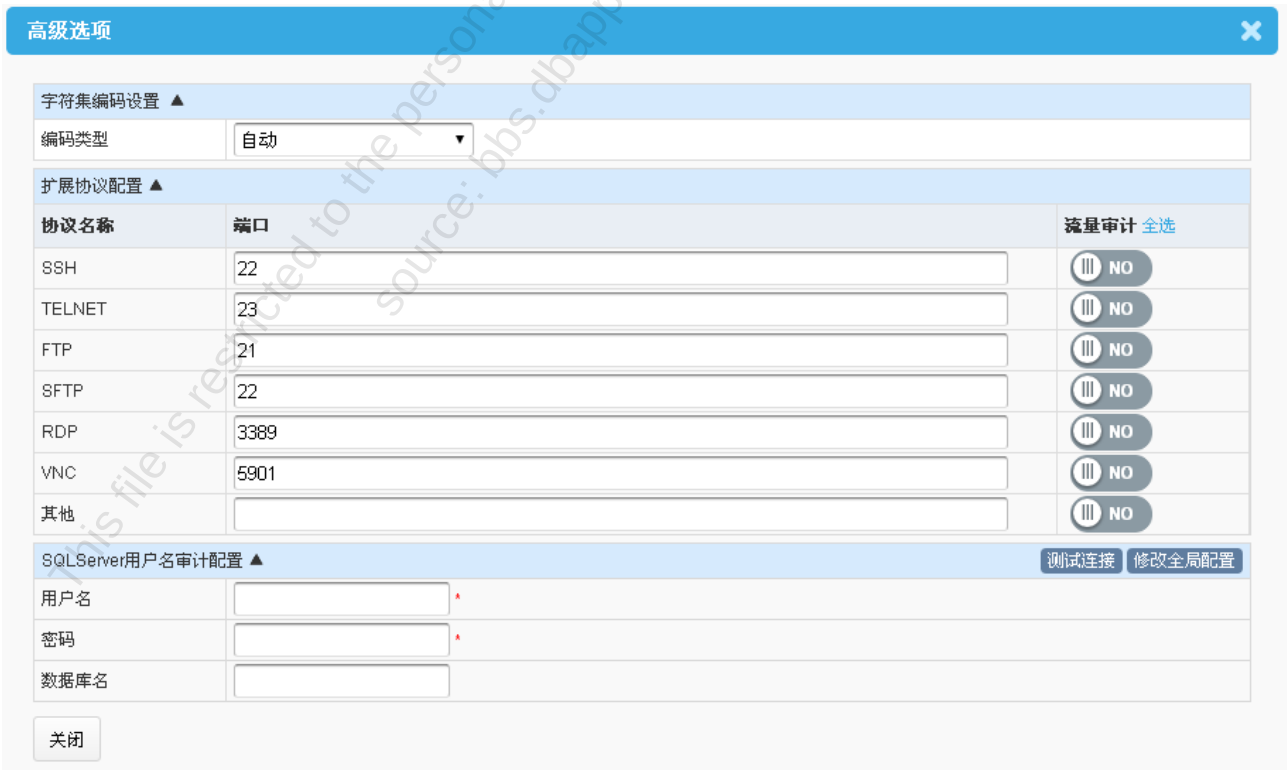
详细配置信息如表 4-2。

表4-2 配置物理端口

选项	说明
IP	IP要符合定义标准
业务类型	需要审计的业务类型
版本	保护对象的版本号
端口	保护对象的端口，如要审计全部端口，可填写*
运行环境	• 业务类型为以下类型时无【运行环境】选项。 WEB、达梦、CACHE、TERADATA、人金大仓、POSTGRESQL、SMTP、POP3、FTP和DCOM。 • 业务类型为以下类型时，【运行环境】变更为【字符集编码】，需要选择相应的字符集编码。 SQLSERVER和SYBASE。
流量方向	• 单向审计审计内容为：请求+客户端信息+服务端信息。不包括返回信息。 • 双向审计审计的内容为：请求+客户端信息+服务端信息+返回。对于 WEB、Oracle、Mysql、Sqlserver、Sybase、Db2、Informix、达梦数据库，返回内容可以选择是否保存，以及保存的长度和行数。 • Oracle、TELNET 默认为双向审计，其它默认为单向审计。

(3) 单击<高级选项>，打开高级选项页面。如图 4-10 所示。

图4-10 高级选项



高级选项说明参见表 4-3。

表4-3 高级选项说明

选项		说明
字符集编码设置	编码类型	对审计数据的编码类型。支持UTF-8、UTF-16等多种类型。默认为：“自动”。如果不清楚数据库的编码，可以先不作修改，选择默认值。当审计的内容不正确或包含乱码时，再使用其它编码类型。
扩展协议配置	协议名称	扩展协议名称。如SSH、TELNET等
	端口	协议对应的端口号。 SSH默认为：22 TELNET默认为：23 FTP默认为：21 SFTP默认为：22 RDP默认为：3389 VNC默认为：5901
	流量审计	开启流量审计。默认为“NO”
Sqlserver用户名审计配置	用户名相关配置	用户名和密码为必填项，sqlserver用户名审计配置只有在配置SQLSERVER数据库时才会显示出来，并且版本在2005以上

(4) 单击<保存>，保存新增物理端口。

4.2.3 物理端口配置举例

1. 配置要求

如要配置一台保护对象 IP 为 192.168.21.97，业务类型为 Oracle，版本为 10g，端口为 1521，运行在 linux 环境，并要求双向审计且不保存返回内容的数据库。

2. 配置步骤

(1) 进入[探测器/探测器相关配置/物理端口]界面，单击<新增>，进入配置页面，输入相关的信息。如图 4-11 所示。

图4-11 新增物理端口图

(2) 单击<保存>，配置成功，返回物理端口列表。如图 4-12 所示。

图4-12 物理端口列表图

IP	端口	业务类型	版本	运行环境	挂载次数	流量方向	来源	操作
192.168.21.67	3306	MYSQL	5.1	linux	1	双向	手工添加	编辑
192.168.21.74	*	ORACLE	9i	win	1	双向	手工添加	编辑
192.168.21.75	1521	ORACLE	10g	win	1	双向	手工添加	编辑
192.168.21.75	1522	ORACLE	10g	win	1	双向	手工添加	编辑
192.168.21.79	1433	SQLSERVER	2005	ucs-2	1	双向	手工添加	编辑
192.168.21.85	50000	DB2	v95	win	1	双向	手工添加	编辑
192.168.21.87	1433	SQLSERVER	2008	ucs-2	未挂载	双向	手工添加	编辑 删除
192.168.21.97	1521	ORACLE	10g	linux	未挂载	双向	手工添加	编辑 删除
192.168.21.98	80	WEB	全部		未挂载	双向	手工添加	编辑 删除
192.168.21.98	1521	ORACLE	10g	win	1	双向	端口扫描	编辑
192.168.25.250	80	WEB	全部		1	双向	手工添加	编辑
192.168.25.45	8080	WEB	全部		1	双向	手工添加	编辑
192.168.27.49	1521	ORACLE	11g	win	1	双向	手工添加	编辑
192.168.27.51	80	WEB	全部		1	双向	手工添加	编辑
192.168.27.62	1521	ORACLE	10g	win	1	双向	手工添加	编辑
192.168.3.21	80	WEB	全部		1	双向	手工添加	编辑
192.168.30.10	1521	ORACLE	10g	aix	1	双向	手工添加	编辑
192.168.30.11	1521	ORACLE	10g	aix	1	双向	手工添加	编辑
192.168.30.12	1521	ORACLE	10g	aix	1	双向	手工添加	编辑
192.168.30.229	3306	MYSQL	5.1	linux	1	双向	手工添加	编辑

4.2.4 探测器

1. 配置准备

需要确认好采集设备所在 IP，以及采集口。

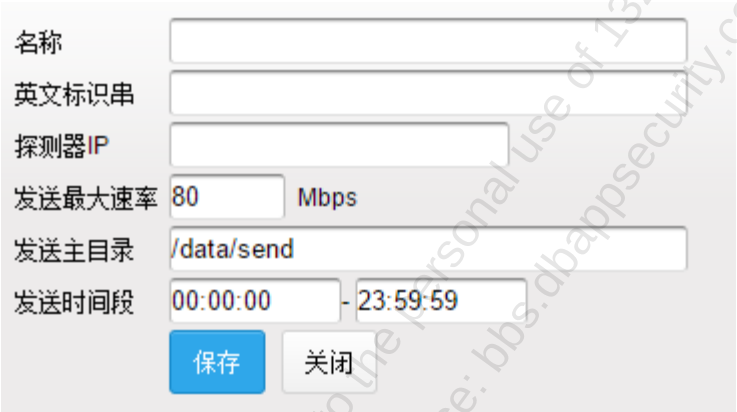
2. 配置探测器

(1) 进入[探测器/探测器相关配置/探测器]界面。如图 4-13 所示。

图4-13 探测器列表图

(2) 单击“探测器组”中<添加>，打开“添加探测器”页面，添加探测器。如图 4-14 所示。

图4-14 添加探测器图



详细配置信息如表 4-4。

表4-4 配置探测器

配置项	说明
名称	必填项。采集设备的名称
英文标识串	必填项。由字母、数字及下划线组成，首字母必须是字母 当填入名称时，会自动以中文首字母生成，可修改
探测器IP	必填项。采集设备IP
发送最大速率	必填项。范围为：1~1000Mbps，默认为80Mbps
发送主目录	必填项。向数据中心发送审计数据的暂存目录
发送时间段	必填项。审计数据发送的时间段

(3) 选择添加好的探测器，在“业务主机群”中单击<添加>，打开“添加业务主机群”页面，添加业务主机群。如图 4-15 所示。

图4-15 添加业务主机群

详细配置信息如表 4-5。

表4-5 配置业务主机群

配置项	说明
名称	必填项。业务主机群的名称
类型	必填项。业务类型
功能	可选项。需要实现的功能，添加时可先不选，使用时再去选也可以 系统默认提供的功能有：审计、特征和审计外送功能
采集设备	可选项。采集数据网口，添加时可先不选，使用时再去选也可以

(4) 选择添加好的业务主机群，在“端口挂载”中单击“挂载”，选择物理端口，进行挂载即可。如图 4-16 所示。

图4-16 挂载物理端口

说明

可直接挂载已经配置好的物理端口，也可以单击<新增物理端口>新增物理端口进行挂载

4.2.5 探测器配置举例

1. 配置要求

要求配置一台探测器名称为“D2020”，业务主机群名称为“财务 Ora”，在 eth0 采集口挂载一台 Oracle 数据库。

2. 配置步骤

(1) 进入[探测器/探测器相关配置/探测器]界面，点击“探测器”<添加>，输入名称为“D2020”相关信息。如图 4-17 所示。

图4-17 添加探测器图

(2) 选择创建好的“D2020”，单击“业务主机群”中的<添加>，添加“财务 Ora”业务主机群。如图 4-18 所示。

图4-18 添加业务主机群

(3) 选择创建好的“财务 Ora”业务主机群，单击“端口挂载”中<挂载>。如图 4-19 所示。

图4-19 挂载物理端口图

(4) 选择配置好的物理端口，单击<挂载>。如图 4-20 所示。

图4-20 物理端口挂载图

(5) 至此探测器相关信息配置完成，即可审计数据。

4.3 审计查询

主机及帐户及目标服务器的信息管理，如 IP、主机名、网络协议、端口号、帐户、密码等信息。主机及帐户配置既能单个手工添加，又能批量表格导入。

4.3.1 查询参数

1. 功能简介

对审计查询参数、查询结果显示列和查询结果显示视图进行设置。

2. 配置查询参数

(1) 进入[配置/常规/查询参数]，打开查询参数配置界面。如图 4-21 所示。

图4-21 查询参数

(2) 设置相应参数。参见表 4-6。

表4-6 查询参数信息

选项		用途说明
审计查询参数	查询结果每页显示	每页显示审计数据记录的条数。可进行数值调整，最小值20条，最大值1000条。默认值为20 提示 不建议选用太大，否则显示时间会比较长。
	查询结果总记录数	显示审计数据记录的条数。可进行数值调整，最小值200条，最大值100000条。默认值为600
	查询缺省时间范围	缺省值300秒，显示审计数据记录。可进行数值调整，最小值60秒，最大值86400秒
	查询结果导出最大记	结果导出最大记录数为100000

	录数	
	报文最大显示长度	报文最大显示长度为10000
审计查询结果设置	显示列设置	设置后，在审计查询结果列表中只显示选中列
	视图设置	设置后，在审计查询结果页面根据设置显示视图
风险查询结果设置	显示列设置	设置后，在风险查询结果列表中只显示选中列。具体参见5.2 告警查询

4.3.2 综合查询

1. 功能简介

对审计的结果进行查询，此页面可以查询所有的审计数据。

2. 查询步骤

(1) 打开[审计/日常行为/综合查询]，打开综合查询页面。如图 4-22 所示。

图4-22 审计查询图

查询选项说明如表 4-7。

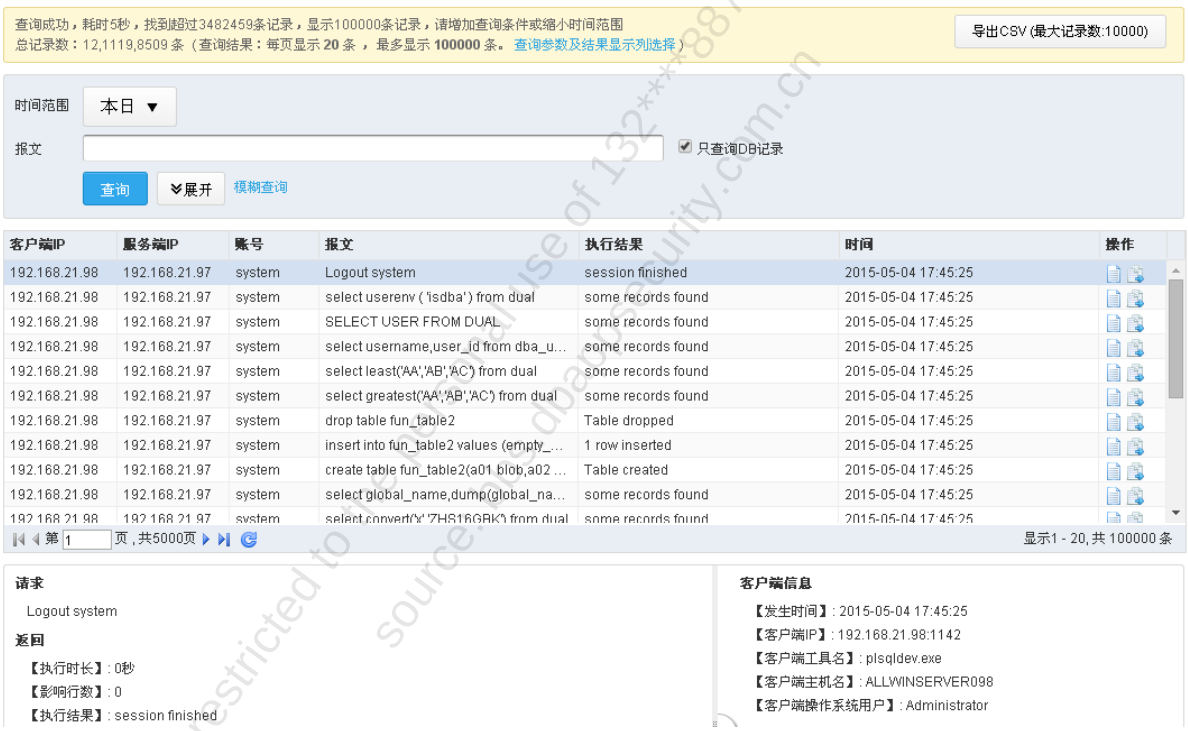
表4-7 配置审计查询表

选项	用途说明
时间范围	可选项。查询在指定时间内对数据库进行的所有操作。默认搜索最近五分钟的数据
报文	可填项。查询审计内容。多个关键字用空格分隔，字符个数2~255，特殊字符用空格代替查询条件
只查询DB记录	可选项。默认搜索结果只查询DB的审计记录。去掉选项，可以搜索到所有的审计记录。
业务主机群	可选项。选择查询相关的业务主机群
操作类型	可选项。操作数据库的类型，如select等
关联账号	可填项。按指定的关联账号查询
客户端IP	可填项。按指定的客户端IP查询。如填入192.168.3.25，则查询客户端IP为192.168.3.25的所有操作

账号	可填项。按指定的用户名查询。如填入sa，则可以查询到sa用户登录的所有操作
客户端工具	可选项。默认为”全部”。其中的选项可通过[配置/常规/客户端工具]页面进行管理，也可以直接点击“客户端工具”下拉框后面的“管理”链接直接打开管理页面。具体参见13.1.2 客户端工具
服务端IP	可填项。按指定的服务端IP查询。如填入192.168.21.2，则查询服务端IP为192.168.21.2 的所有操作
SID	可填项。按指定的数据库SID查询
来访客户网络	可选项。默认为”全部”。其中的选项可通过[配置/常规/来访客户网络]页面进行管理。具体参见13.1.3 来访客户网络

(2) 输入查询条件，单击<查询>，显示查询结果列表。如图 4-23 所示。

图4-23 审计查询结果图



说明

默认是只查询 600 条，如想查询更多可以到[配置/常规/查询参数]配置，最多一次只能查询 100000

4.3.3 WEB 查询

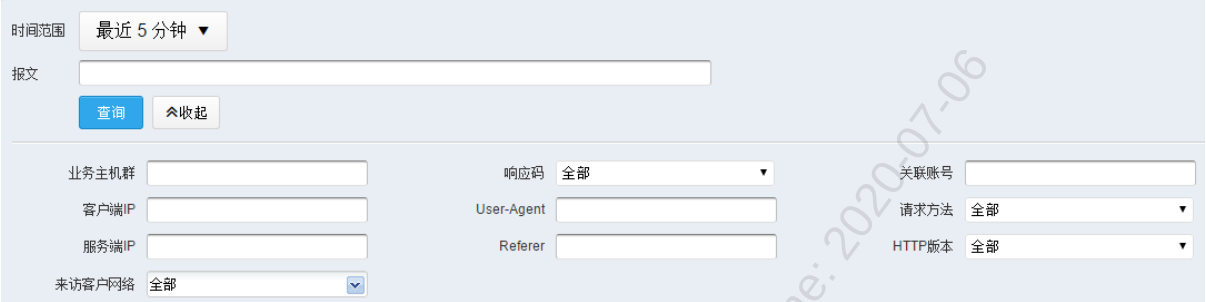
1. 功能简介

此页面只能对 WEB 审计结果进行查询。

2. 查询步骤

(1) 打开[审计/日常行为/WEB 查询]，打开 WEB 查询页面。如图 4-24 所示。

图4-24 WEB 查询图



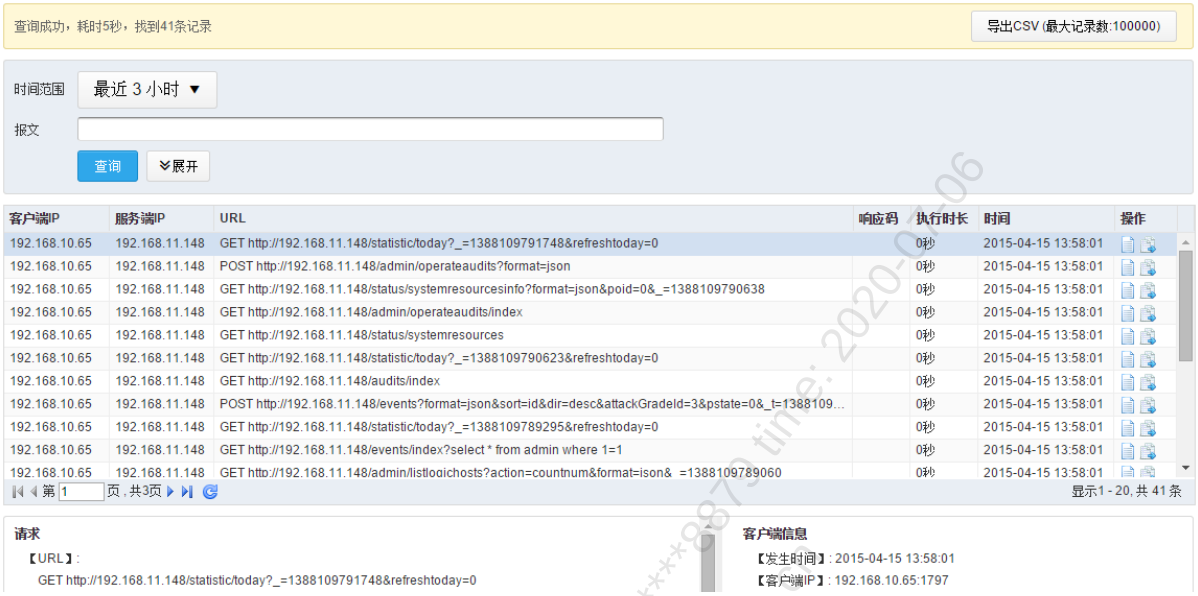
详细选项说明如表 4-8。

表4-8 配置 WEB 查询表

选项	用途说明
时间范围	可选项。查询在指定时间内对数据库进行的所有操作。默认搜索最近五分钟的数据
报文	可填项。查询审计内容。多个关键字用空格分隔，字符个数2~255，特殊字符用空格代替查询条件
业务主机群	可填项。选择作用对象。如用户(oracle)、包、表等对象
响应码	可选项。服务器响应返回值，由3位十进制数字组成，出现在由HTTP服务器发送的响应的第一行。默认为“全部”
关联账号	可填项。按指定的关联账号查询
客户端IP	可填项。按指定的客户端IP查询。如填入192.168.3.25，则查询客户端IP为192.168.3.25的所有操作
User-Agent	可填项。使用的用户代理，它是一个特殊字符串头，使得服务器能够识别客户端使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等
请求方法	可选项。HTTP协议中的请求方法，如GET，POST等
服务器端IP	可填项。按指定的服务端IP查询。如填入192.168.21.2 ，则查询服务端IP为192.168.21.2 的所有操作
Referer	可填项。header的一部分，告诉服务器，客户机是从哪个页面来的（防盗链）。当浏览器发送请求的时候，一般会带上Referer
HTTP版本	可填项。HTTP的版本号，默认选择“全部”
来访客户网络	可填项。其中的选项可通过[配置/常规/来访客户网络]页面进行管理。默认为”全部”。具体参见13.1.3 来访客户网络

(2) 输入查询条件，单击<查询>，显示查询结果列表。如图 4-25 所示。

图4-25 WEB 查询列表



4.3.4 会话查询

1. 基本会话查询

查询客户端与服务器端之间建立的会话信息。查询步骤如下：

(1) 进入[审计/日常行为/会话查询]，打开会话查询页面。如图 4-26 所示。

图4-26 会话查询

(2) 输入相关的查询信息。选项说明。

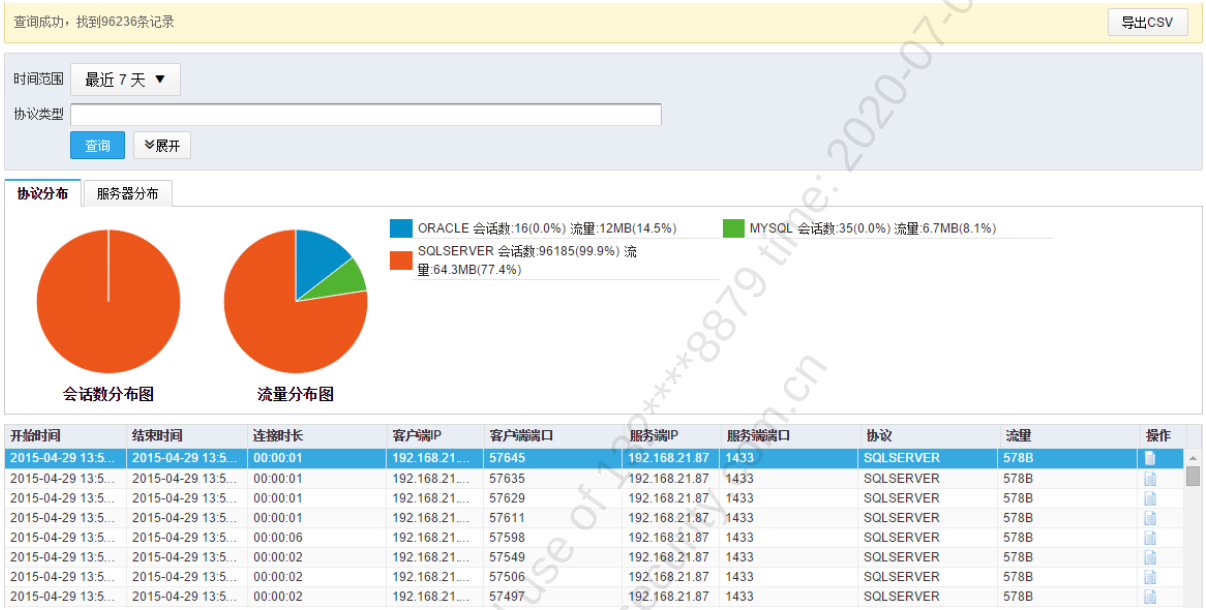
表4-9 会话查询选项说明

选项	用途说明
时间范围	可选项。查询在指定时间内发起的会话。默认为“最近五分钟”
协议类型	可选项。会话使用的协议类型。如“ORACLE”等
服务端IP	可填项。服务端IP地址
服务端端口	可填项。服务端端口号

客户端IP	可填项。客户端IP地址

(3) 点击<查询>，进行会话查询。如果有配置关联堡垒机则会显示对应的堡垒关联信息，如下页面为没有配置堡垒关联信息的情况，如图 4-27 所示。

图4-27 会话查询结果



查询结果信息说明参见表 4-10。

表4-10 查询结果信息说明

选项	用途说明
导出CSV	将查询结果导出为CSV格式文件。 下载到本地计算机默认的下载目录 名称为：auditlist.zip。
协议分布	按协议类型，以饼图的方式统计显示会话数分布情况和流量分布情况
服务器分布	按服务器类型，以饼图的方式统计显示会话数分布情况和流量分布情况
开始时间	会话的开始时间
结束时间	会话的结束时间
连接时长	会话的连接时长
客户端IP	会话发生的客户端IP地址
客户端端口	会话发生的客户端端口号
服务器IP	会话发生的服务器IP地址
服务器端口	会话发生的服务器端口号
协议	会话的协议类型
流量	会话产生的流量

操作	单击，查看告警分析的详细信息

2. 堡垒联动查询

目前支持的协议有：SSH、TELNET、RDP、FTP、SFTP、VNC

目前对这些协议除了基本的信息审计外，另外审计的内容如下：

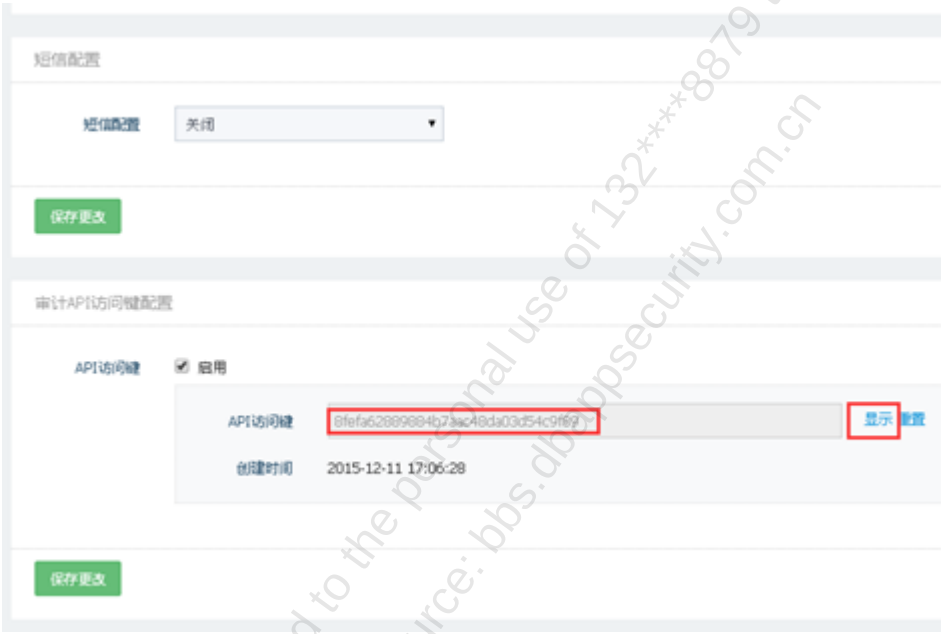
SSH，TELNET：审计操作命令

RDP：审计图形会话命令和键盘命令

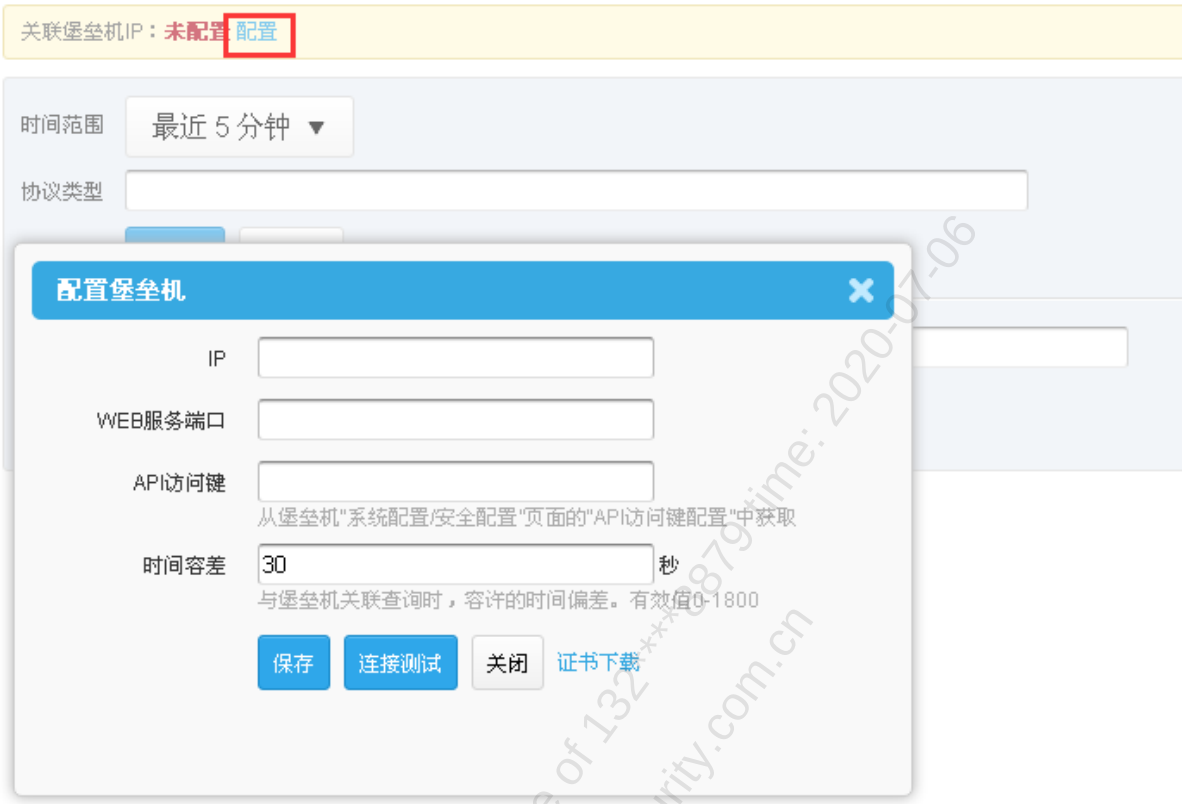
VNC、FTP、SFTP：基本会话信息，包括客户端和主机的信息。

堡垒联动功能需要同品牌的堡垒机才能实现，具体步骤如下：

(1) 登录堡垒系统，打开[系统/系统配置/安全配置]项，获取 API 访问键值，如下图所示：



(2) 登陆数据库审计系统，打开[审计/日常行为/会话查询]页面，点击“关联堡垒机 IP”的<配置>文字链接，进行配置堡垒机信息。



配置信息如下表：

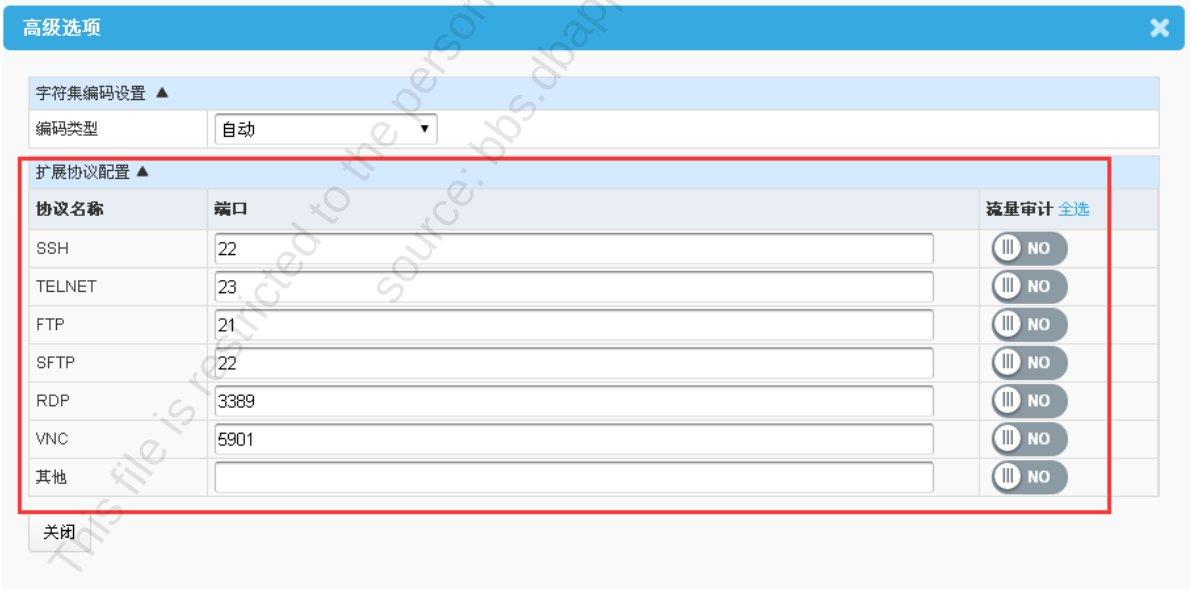
表4-11 堡垒配置信息表

字段	内容
IP	堡垒机对应的IP地址
WEB服务端口	默认为443端口
API访问键	上一步从堡垒机[系统配置/安全配置]页面的“API访问键配置”中获取到的值
时间容差	与堡垒机关联查询时，容许的时间偏差。有效值0-1800

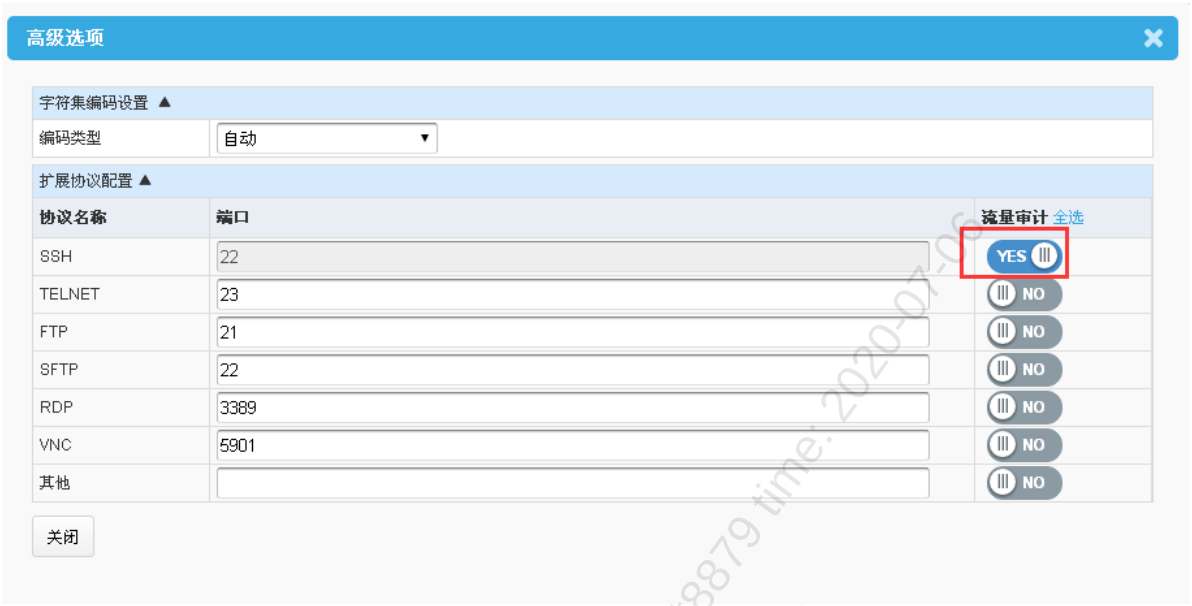
(3) 配置完成后，点击<连接测试>，如弹出“成功”，则配置正确，点击<保存>按钮。如弹出失败提示，则查看相应的配置信息的正确性。

(4) 再打开[探测器/探测器相关配置/物理端口]，添加审计对象

(5) 在新增物理端口界面，点击“高级选项”文字链接，配置扩展协议端口



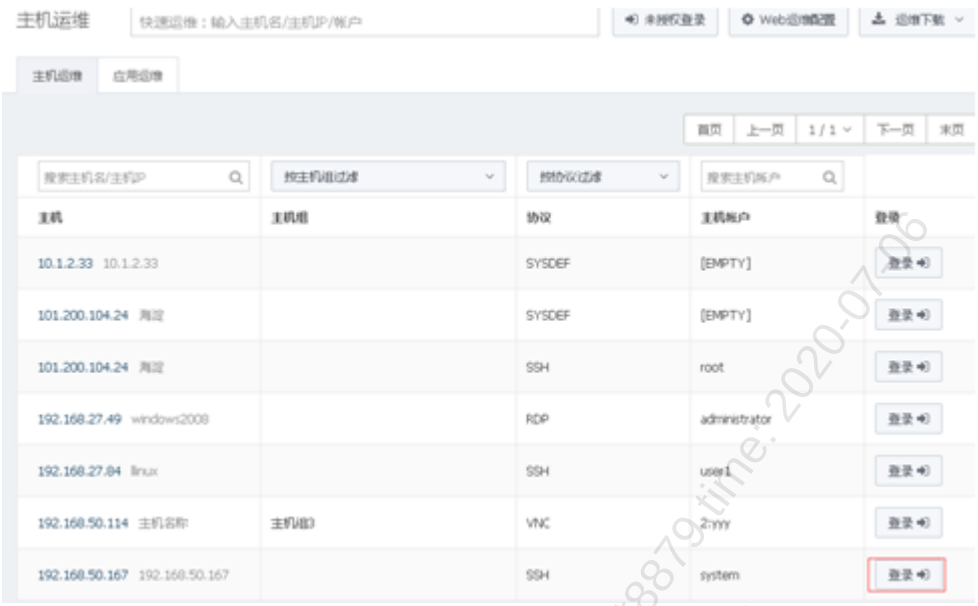
(6) 如需要审计主机“192.168.50.167”的 ssh 22 端口，则在扩展协议配置右边的“流量审计”打开审计状态为“yes”即可。



(7) 配置完成后，保存即可。

(8) 打开[探测器/探测器相关配置/探测器]，把该审计对象加载到业务主机群中。

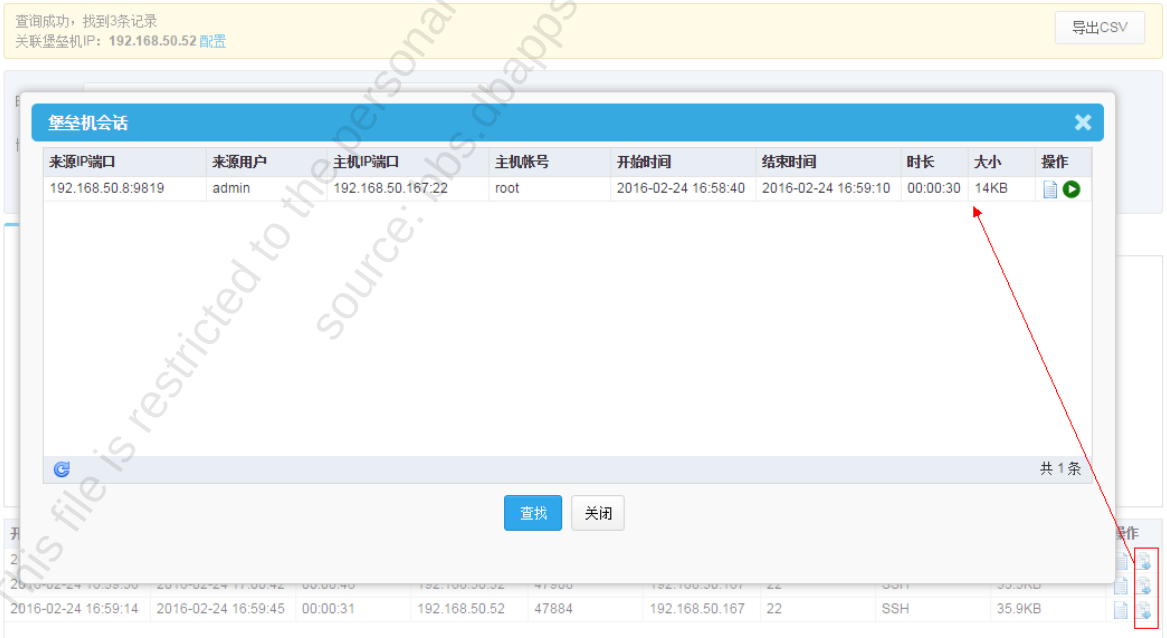
(9) 登陆堡垒系统， 打开[运维/主机运维]页面，选择对应的主机，点击<登录>打开主机并操作相关信息。



(10) 操作完成后，退出主机。

(11) 登陆审计系统，打开[审计/日常行为/会话查询]页面，默认“只查询堡垒机”选项会处理选中查询，点击<查询>，可以查询到对应的会话审计列表。

(12) 点击审计记录后面的“关联”图标，打开堡垒关联会话页面。



(13) 点击关联页面的“详细”图标，打开会话详细信息页面

会话详细 (ID:2380473e56cd70c00000000303000005)

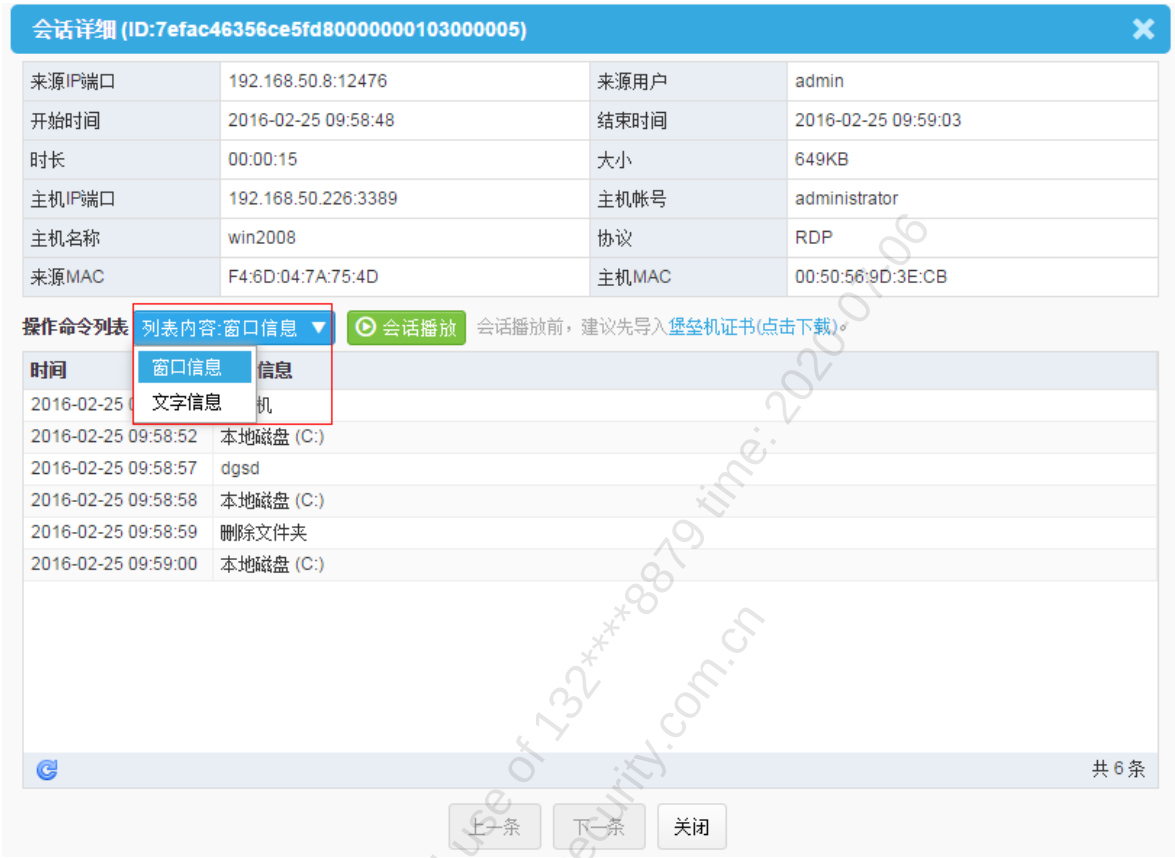
来源IP端口	192.168.50.8:9819	来源用户	admin
开始时间	2016-02-24 16:58:40	结束时间	2016-02-24 16:59:10
时长	00:00:30	大小	14KB
主机IP端口	192.168.50.167:22	主机帐号	root
主机名称	167	协议	SSH
来源MAC	F4:6D:04:7A:75:4D	主机MAC	00:50:56:8D:36:F5

操作命令列表 会话播放 会话播放前，建议先导入堡垒机证书(点击下载)。

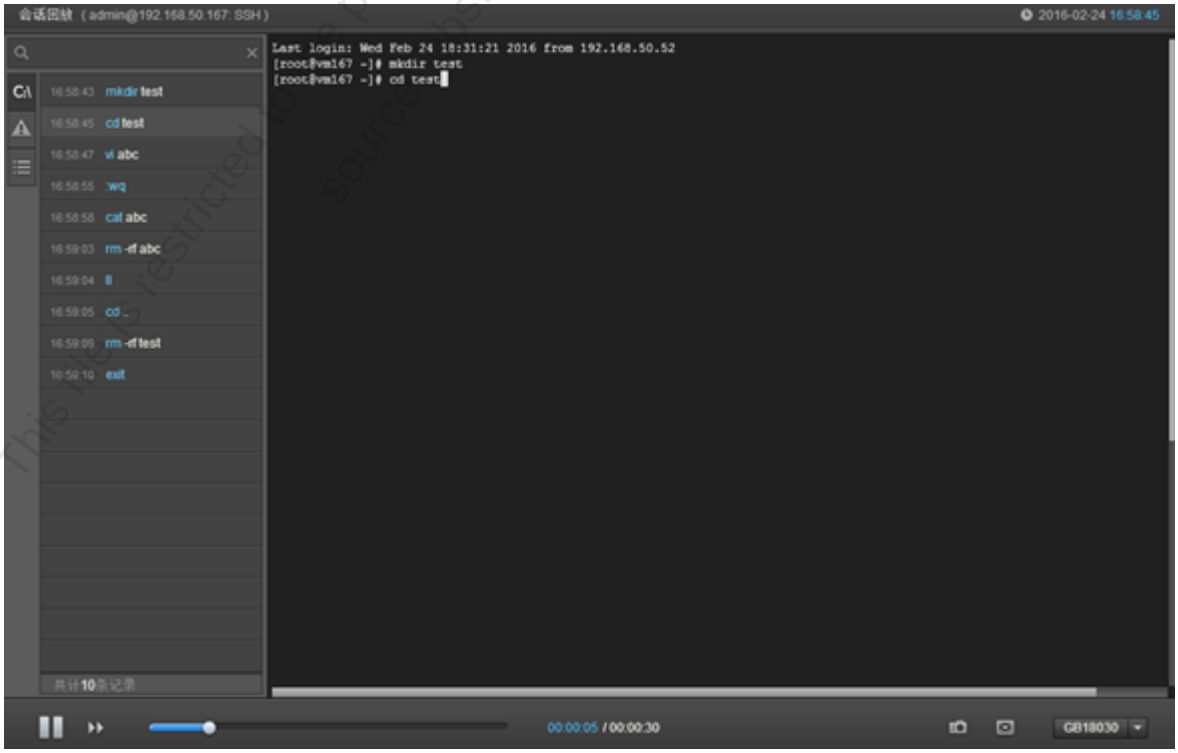
时间	命令
2016-02-24 16:58:43	[root@vm167 ~]# mkdir test
2016-02-24 16:58:45	[root@vm167 ~]# cd test
2016-02-24 16:58:47	[root@vm167 test]# vi abc
2016-02-24 16:58:55	:wq
2016-02-24 16:58:58	[root@vm167 test]# cat abc
2016-02-24 16:59:03	[root@vm167 test]# rm -rf abc
2016-02-24 16:59:04	[root@vm167 test]# ll
2016-02-24 16:59:05	[root@vm167 test]# cd ..
2016-02-24 16:59:09	[root@vm167 ~]# rm -rf test
2016-02-24 16:59:10	[root@vm167 ~]# exit

共 10 条

上一条 下一条 关闭



(14) 点击关联页面的“播放”图标，打开会话播放页面。



4.3.5 回放

1. 功能简介

模拟回放一遍审计记录。

2. 回放步骤

(1) 进入[审计/日常行为/回放]，打开回放页面。如图 4-28 所示。

图4-28 审计回放查询

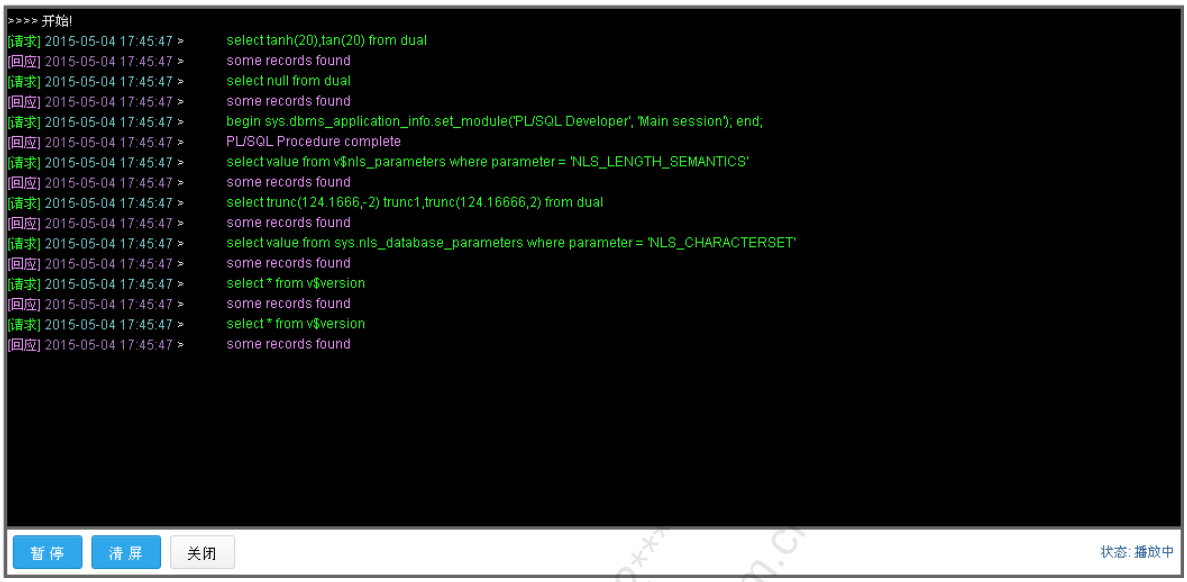
详细选项如表 4-12。

表4-12 审计回放信息

选项	用途说明
时间范围	查询在指定时间内对数据库进行的所有操作。默认搜索最近五分钟的数据
报文	查询审计内容。多个关键字用空格分隔，字符个数2~255，特殊字符用空格代替查询条件
业务主机群	选择查询相关的业务主机群
操作类型	选择查询的操作类型。如select,insert,update,delete等操作
关联账号	按指定的关联账号查询
客户端IP	按指定的客户端IP查询。如填入192.168.3.25，则查询客户端IP为192.168.3.25的所有操作
账号	按指定的用户名查询。如填入sa，则可以查询到sa用户登录的所有操作
客户端工具	默认为”全部”。其中的选项可通过[配置/常规/客户端工具]页面进行管理，也可以直接点击“客户端工具”下拉框后面的“管理”链接直接打开管理页面
服务端IP	按指定的服务端IP查询。如填入192.168.21.2，则查询服务端IP为192.168.21.2 的所有操作
SID	按指定的数据库SID查询
来访客户网络	默认为”全部”。其中的选项可通过[配置/常规/来访客户网络]页面进行管理

(2) 输入查询条件，单击<回放>，回放审计查询结果记录。如图 4-29 所示。

图4-29 审计回放图



4.4 审计过滤

4.4.1 审计选项

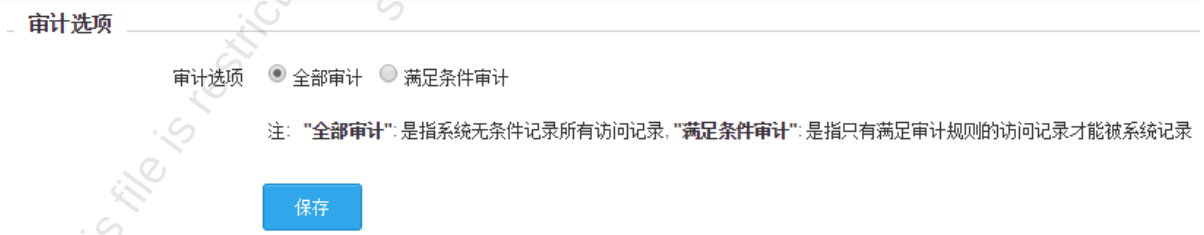
1. 功能简介

审计选项是针对规则配置而言的，默认是“全部审计”。

2. 审计选项配置

(1) 打开[规则/规则/审计选项]，打开审计选项页面配置。如图 4-30 所示。

图4-30 审计选项配置图



详细选项如表 4-13

表4-13 审计选项信息

选项	用途说明
全部审计	默认是全部审计，指系统无条件记录所有访问记录
满足条件审计	只有满足配置的审计规则的访问记录才能被系统审计到，没有满足规则条件的则不会被审计

(2) 选择审计选项，单击<保存>即可。

4.4.2 指定源 IP 审计

1. 功能简介

只针对指定的 IP 进行审计，其它源 IP 或业务系统的记录不再审计。

2. 配置指定源 IP 审计

(1) 进入[配置/常规/指定源 IP 审计]，打开指定源 IP 审计配置界面。如图 4-31 所示。

图4-31 指定源 IP 审计

注意

一旦配置并保持了 IP，系统就只审计此列表中的源 IP 产生的数据。

(2) 点击<新增>，打开新增页面。如图 4-32 所示。

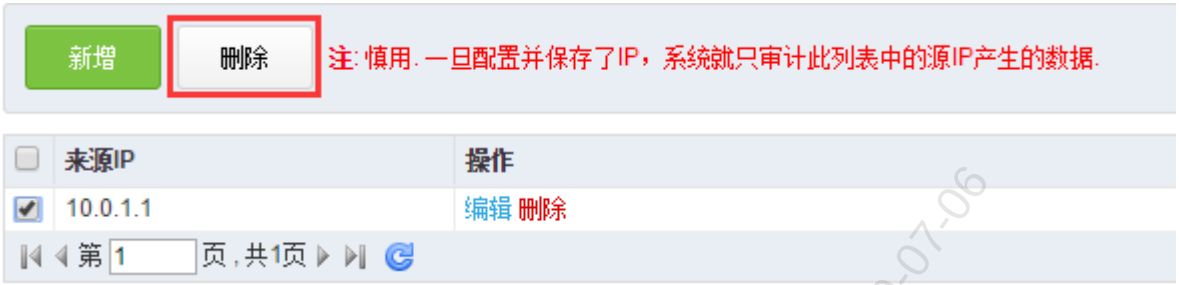
图4-32 新增源 IP

表4-14 指定源 IP 信息

选项	用途说明
来源IP	必选项。 • 支持单个 IP 地址，如 192.168.1.10 • 支持 IP 网段，如 192.168.1.*

(3) 点击<删除>，删除选中的源 IP。如图 4-33 所示。

图4-33 删除源 IP 审计



说明

删除也可以点击源 IP 对应的<删除>，逐个删除。

(4) 点击<编辑>，修改源 IP。如图 4-34 所示。

图4-34 编辑源 IP

4.4.3 IP 过滤

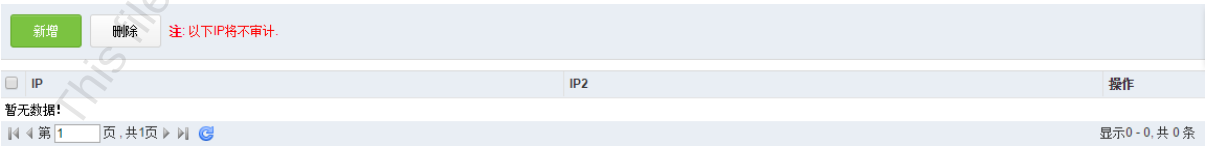
1. 功能简介

该功能是对 IP 或 IP 所对应的业务系统发出的数据不再进行审计和记录。

2. 配置 IP 过滤

(1) 进入[配置/常规/IP 过滤]，打开 IP 过滤配置页面。如图 4-35 所示。

图4-35 IP 过滤



注意

一旦配置并保持了 IP，此 IP 将不审计。

(2) 点击<新增>，打开新增页面。如图 4-36 所示。

图4-36 配置 IP 过滤

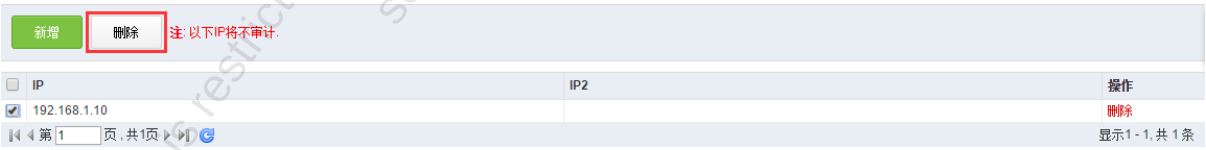
选项说明参见表 4-15。

表4-15 IP 过滤信息

选项	用途说明
不区分来源及目标	新增IP作为源IP或目标IP都会被过滤
同时满足来源及目标	分别新增源IP和目标IP 其中， 源IP可以为单个IP、IP网段、IP地址段或多个IP用”,”分割 目标IP只能填写单个IP，并且需要填写端口
IP	必填项。 • 支持单个 IP 地址，如 192.168.1.10 • 支持 IP 网段，如 192.168.1.* • IP 地址段，如 192.168.1.1-192.168.1.100

(3) 点击<删除>，删除选中的 IP。如图 4-37 所示。

图4-37 删除 IP



说明

删除也可以点击 IP 对应的<删除>，逐个删除。

4.4.4 报文过滤

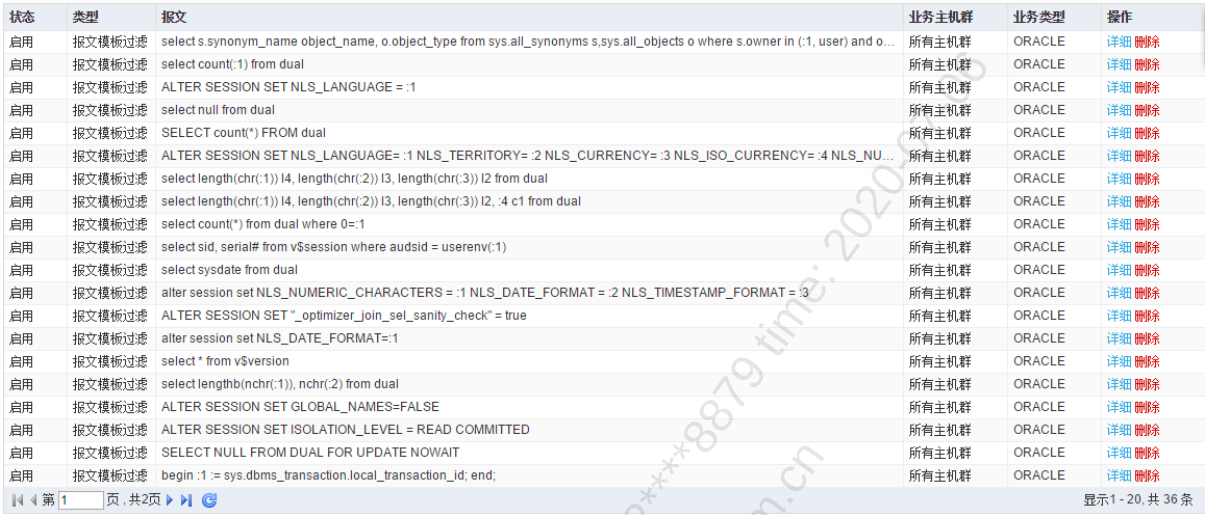
1. 功能简介

主要是对报文过滤的模板进行管理维护。

2. 配置报文过滤

进入[配置/常规/报文过滤]，打开报文过滤页面。如图 4-38 所示。

图4-38 报文过滤



状态	类型	报文	业务主机群	业务类型	操作
启用	报文模板过滤	select s.synonym_name object_name, o.object_type from sys.all_synonyms s,sys.all_objects o where s.owner in (:1, user) and o...	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select count(:1) from dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	ALTER SESSION SET NLS_LANGUAGE = :1	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select null from dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	SELECT count(*) FROM dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	ALTER SESSION SET NLS_LANGUAGE= :1 NLS_TERRITORY= :2 NLS_CURRENCY= :3 NLS_ISO_CURRENCY= :4 NLS_NU...	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select length(chr(:1)) l4, length(chr(:2)) l3, length(chr(:3)) l2 from dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select length(chr(:1)) l4, length(chr(:2)) l3, length(chr(:3)) l2, :4 c1 from dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select count(*) from dual where 0=:1	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select sid, serial# from v$session where audsid = userenv(:1)	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select sysdate from dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	alter session set NLS_NUMERIC_CHARACTERS = :1 NLS_DATE_FORMAT = :2 NLS_TIMESTAMP_FORMAT = :3	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	ALTER SESSION SET "_optimizer_join_sel_sanity_check" = true	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	alter session set NLS_DATE_FORMAT=:1	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select * from v$version	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	select lengthb(nchr(:1)), nchr(:2) from dual	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	ALTER SESSION SET GLOBAL_NAMES=FALSE	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	ALTER SESSION SET ISOLATION_LEVEL = READ COMMITTED	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	SELECT NULL FROM DUAL FOR UPDATE NOWAIT	所有主机群	ORACLE	详细 删除
启用	报文模板过滤	begin :1 := sys.dbms_transaction.local_transaction_id; end;	所有主机群	ORACLE	详细 删除

第 1 页，共2页　　显示1 - 20, 共 36 条

报文过滤选项说明见表 4-16。

表4-16 报文过滤信息

选项	用途说明
详细	查看报文过滤模板的详细信息。
删除	删除对应的报文过滤模板。

5 告警

5.1 告警通知

5.1.1 通知告警

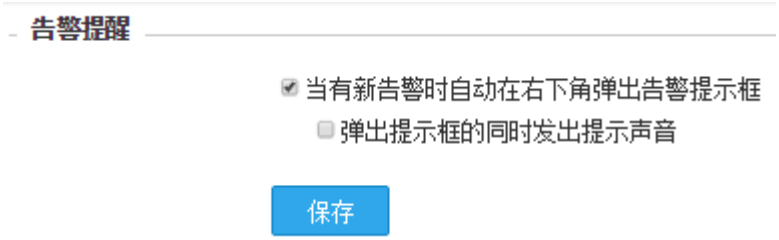
1. 功能简介

告警提醒是在发生告警的情况下，可以在浏览器的右下角以冒泡的形式自动弹出告警提示框。

2. 配置告警提醒

(1) 进入[配置/告警通知/告警提醒]，打开告警提醒配置界面。如图 5-1 所示。

图5-1 告警提醒



(2) 选择是否弹出提示框、发出提示声音。

(3) 点击<保存>，保存配置。

5.1.2 发送配置

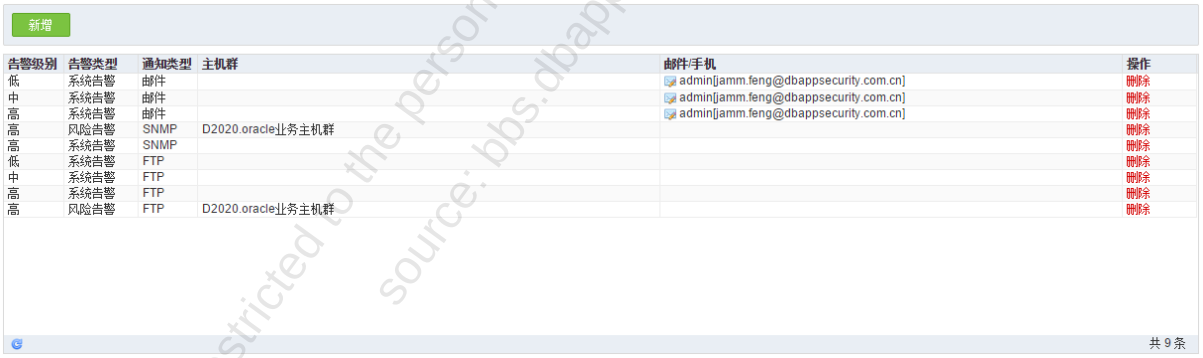
1. 功能简介

将告警通过邮件、短信、FTP、SYSLOG 和 SNMP 方式，将告警信息发送给相关人员，以便相关人员及时处理告警。

2. 发送配置

(1) 进入[配置/告警通知/发送配置]，打开发送配置界面。如图 5-2 所示。

图5-2 发送配置



(2) 点击<新增通知>，打开[新增通知]页面。如图 5-3 所示。

图5-3 新增通知

(3) 选择业务主机群、告警级别、通知类型及与通知类型相关的配置。见表 5-1。

表5-1 发送配置信息

选项		用途说明
告警类型		必选项。默认为“风险告警”。
业务主机群		必选项。
告警级别		必选项。默认为“高”
通知类型	邮件	以邮件方式发送告警通知 • 点击<修改收件人邮件地址>，修改收件人的邮件地址 • 点击<邮件服务器配置>，配置邮件服务器。参见 5.1.4 邮件
	短信	以短信方式发送告警通知 • 选择发送给谁 • 点击<修改收件人手机>，修改收件人的手机号码 • 点击<短信接口配置>，配置短信接口。参见 5.1.5 短信 注：短信方式目前不支持系统告警，配置后不会生效。
	SNMP	以SNMP方式发送告警通知 • 点击<SNMP 服务器配置>，配置 SNMP 服务器。参见 5.1.8 SNMP
	SYSLOG	以SYSLOG方式发送告警通知 • 选择 SYSLOG 类型，等级，使用默认值即可。参见表 5-2SYSLOG 日志类型、表 5-3SYSLOG 等级类型 • 点击<Syslog 服务器配置>，配置 SYSLOG 服务器。参见 5.1.7 SYSLOG
	FTP	以FTP方式发送告警通知 • 点击<FTP 服务器配置>，配置 FTP 服务器。参见 5.1.6 FTP
	阻断	以阻断方式配置告警通知 • 选择阻断设备和阻断时长

表5-2 SYSLOG 日志类型

选项	用途说明
kernel messages	内核日志消息
user-level messages	随机的用户日志消息
mail system	邮件系统日志消息
system daemon	系统守护进程日志消息
security/authorization messages	安全管理日志消息
messages generated internally by syslogd	syslogd本身的日志消息
line printer subsystem	行打印机日志消息
network news subsystem	新闻服务日志消息
UUCP subsystem	UUCP系统日志消息
clock daemon	clock 守护进程日志信息
FTP daemon	FTP守护进程日志信息
NTP subsystem	NTP日志信息
log audit	日志审计
log alert	高优先级日志信息
local0～local7	保留为本地使用

表5-3 SYSLOG 等级类型

选项	用途说明
Emergency	紧急情况，会导致系统不可用
Alert	高优先级故障，必须马上采取行动
Critical	严重错误
Error	错误事件
Warning	警告事件
Notice	普通但重要的事件
Informational	一般信息
Debug	调试信息

(4) 点击<保存>，保存配置。点击<关闭>，取消操作。

5.1.3 发送情况

1. 功能简介

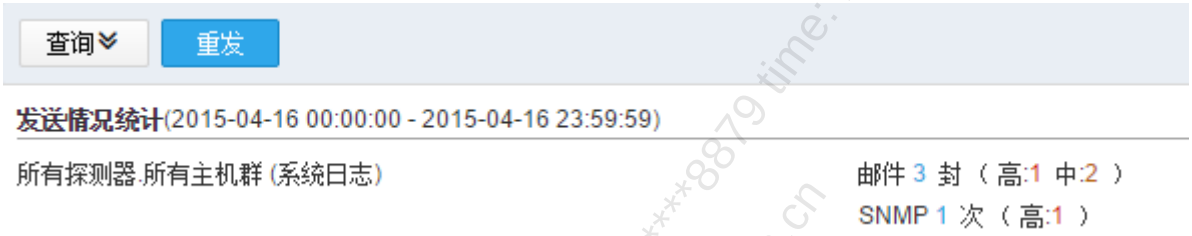
发送情况是告警信息发送情况统计。内容主要包括：

- 查询发送情况和重发告警信息。
- 显示发送情况统计信息和重发情况统计信息。

2. 查询

(1) 进入[配置/告警通知/发送情况]，打开发送情况页面。如图 5-4 所示。

图5-4 发送情况



(2) 点击<查询>，打开查询配置页面。如图 5-5 所示。

图5-5 发送情况查询

(3) 选择业务主机群、类型和发送时间。参见表 5-4。

表5-4 发送情况查询信息

选项	用途说明
业务主机群	必选项
类型	必选项。默认为“全部”。包括全部、邮件、短信、SNMP、SYSLOG和FTP
发送时间	选择发送的开始时间和结束时间

(4) 点击<查询>，查询发送情况；点击<重置>，重置查询条件；点击<关闭>，取消操作。

3. 重发

(1) 进入[配置/告警通知/发送情况]，打开发送情况页面(如图 5-4)。

(2) 点击<重发>，打开重发页面。如图 5-6 所示。

图5-6 重发

(3) 选择告警发生的开始时间和结束时间。

(4) 点击<发送>，重新发送告警通知；点击<关闭>，取消操作。

5.1.4 邮件

1. 功能简介

在告警时，通过邮件服务器，可以将告警信息以邮件形式发送给相关人，供相关人处理告警。

2. 配置邮件

(1) 进入[配置/告警通知/邮件]，打开邮件配置页面。如图 5-7 所示。

图5-7 邮件服务器

(2) 填写相关内容。参见表 5-5。

表5-5 邮件信息

选项	用途说明
发送邮件服务器	必选项。支持输入域名或IP地址

		• 点击<DNS 服务器配置>，配置 DNS 服务器
不需要SMTP验证	发送人邮箱	必填项。填写发送人的邮箱
	端口	必填项。发送邮件服务器的端口。默认为25
需要SMTP验证	发送人邮箱	必填项。填写发送人的邮箱
	密码	必填项。发送人邮箱对应的密码
	加密类型	选择加密类型。默认为“不加密”
	端口	必填项。发送邮件服务器的端口 • 选择“不加密”，默认为 25 • 选择“TLS”，默认为 465 • 选择“SSL”，默认为 587
单封邮件最多显示前		必填项。发送时，每一封邮件内容显示的告警信息条数，当告警信息条数超过所设置的数值时，只显示统计信息，不显示单条告警信息。默认值为100，可设置值范围：10～500
发送统计信息		必选项。选择“是”，将发送统计信息；选择“否”，则不发送

(3) 点击<保存>，保存配置；点击<发送测试邮件>，发送邮件测试配置是否正确。

5.1.5 短信

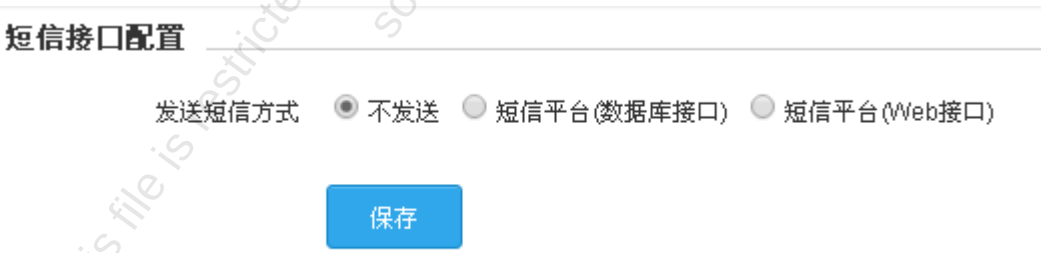
1. 功能简介

在告警时，通过短信接口，可以将告警信息以短信形式发送给相关人，供相关人处理告警。

2. 配置短信接口

(1) 进入[配置/告警通知/短信]，打开短信配置页面，默认为不发送。其中有两种发送方式，一种通过数据库接口，一种通过 WEB 接口。如图 5-8 所示。

图5-8 短信接口



(2) 选择“数据库接口”，配置相关参数，保存即可。参见表 5-6

图5-9 数据库接口配置

表5-6 短信数据库接口信息

选项	用途说明
数据库类型	支持Oracle、Sqlserver、Mysql
数据库IP地址	必填项。填写数据库IP地址
数据库连接端口	必填项。填写数据库端口
用户名	必填项。填写数据库用户名
密码	必填项。填写数据库密码
数据库名（SID）	必填项。填写数据库名或SID信息
调用方式	有两种方式： 插入语句：直接通过SQL语句把告警信息插入到数据库中 存储过程：通过调用存储过程把告警信息插入到数据库中
插入SQL模板	当调用方式为“插入语句”时，此项才会出来。 可使用两个参数（1.手机号码，2.短信内容），用?表示，顺序可在“参数顺序”中设置。 例：insert into MSG(count,phonenum,content,prionity) values(1,?,?,1)
存储过程名称	当调用方式为“存储过程”时，此项才会出来。 可使用两个参数（1.手机号码，2.短信内容），用?表示，顺序可在“参数顺序”中设置。 例：MsgSend(1,?,?,1)
参数顺序	有两个选项： 第一个参数为手机号码,第二个参数为短信内容 第一个参数为短信内容,第二个参数为手机号码
短信内容	配置时，是使用参数指代告警记录的内容。 具体可用参数可单击该项后面的“点击查看所有可用参数”链接文字打开参数说明对话框查看参数内容。
字符编码	有两种：UTF-8、GBK
间隔发送最短时间	每条告警发送的最短间隔时间
每日发送最多条数	每日最多发送条数，只能配置1-10000
测试短信内容	测试短信内容，可修改默认值。
测试号码	输入测试号码后，点击<发送测试短信>按钮，即可把测试内容发送到测试号码上。 此测试号码单纯是测试配置使用，并非告警信息接收者。

(3) 选择“WEB 接口”，配置相关参数，保存即可。

图5-10 短信 WEB 接口

表5-7 短信 WEB 接口信息

选项	用途说明
发送方式	支持POST、GET、JSON
URL	短信调用URL。当不同的发送方式不一样的配置： [POST]：直接输入调用的URL，例：http://www.sms.com/ [GET]：可以使用 [$PHONE] 和 [$SMSTEXT] 两个参数，分别表示手机号码和短信内容。例： http://www.sms.com/?Uid=username&key=password&Mobil=[$PHONE]&Text=[$SMSTEXT]

	[JSON]：直接输入调用的URL，例：http://www.sms.com/
POST参数	当发送方式为“POST”时，此项才会出来。 可以使用 [$PHONE] 和 [$SMSTEXT] 两个参数，分别表示手机号码和短信内容。 例：Uid=username&key=password&Mobil=[$PHONE]&Text=[$SMSTEXT]
请求内容	当发送方式为“JSON”时，此项才会出来。 可以使用 [$PHONE] 和 [$SMSTEXT] 两个参数，分别表示手机号码和短信内容。 例： {"moble":"[$PHONE]","content":"[$SMSTEXT]","account":"aaa","password":"123"}
请求头	请求头信息，点击<添加>可以输入对应的请求头名称和请求头值，可添加多个请求头信息
短信内容	配置时，是使用参数指代告警记录的内容。 具体可用参数可单击该项后面的“点击查看所有可用参数”链接文字打开参数说明对话框查看参数内容。
字符编码	有两种：UTF-8、GBK
间隔发送最短时间	每条告警发送的最短间隔时间
每日发送最多条数	每日最多发送条数，只能配置1-10000
测试短信内容	测试短信内容，可修改默认值。
测试号码	输入测试号码后，点击<发送测试短信>按钮，即可把测试内容发送到测试号码上。 此测试号码单纯是测试配置使用，并非告警信息接收者。

5.1.6 FTP

1. 功能简介

在告警时，通过 FTP，可以将告警信息以文件上传形式上传到 FTP，供相关人查看和处理告警。

2. 配置 FTP

(1) 进入[配置/告警通知/FTP]，打开 FTP 配置页面。如图 5-11 所示。

图5-11 配置 FTP 服务器

(2) 填写相关内容。参见表 5-8。

表5-8 FTP 信息

选项	用途说明
状态	必选项。默认为“启用”
IP	必填项。填写服务器IP
端口	必填项。填写端口。默认为21
用户名	必填项。访问FTP服务器的用户名
密码	必填项。用户名对应的密码
上传目录	必填项。告警信息文件上传到服务器的目录
单个文件最多显示前	发送时，每一次发送的文件内容显示的告警信息条数，当告警信息条数超过所设置的数值，只显示统计信息，不显示单条告警信息。默认值为100，可设置值范围：10～500
发送统计信息	必选项。选择是否发送统计信息

5.1.7 SYSLOG

1. 功能简介

在告警时，通过 SYSLOG 服务器，可以将告警信息以 SYSLOG 日志形式保存到 SYSLOG 服务器，供相关人查看和处理告警。

2. 配置 SYSLOG

(1) 进入[配置/告警通知/SYSLOG]，打开 SYSLOG 配置页面。如图 5-12 所示。

图5-12 配置 SYSLOG

Syslog 选项参见表 5-9。

表5-9 配置 Syslog

选项	用途说明
新增Syslog服务器	添加新的Syslog服务器
代理服务器配置	配置代理服务器
发送类型	必选项。发送统计信息或发送单条。 默认选择“发送统计信息”，在周期内发送的告警信息，接收端接收后，是以统计方式显示信息；若需要在接收端显示每条告警信

	息，可选择“发送单条”

(2) 点击<新增 Syslog 服务器>，打开新增 Syslog 服务器页面。如图 5-13 所示。

图5-13 新增 Syslog 服务器

a. 输入 Syslog 服务端配置项内容。

Syslog 服务端选项参见表 5-10。

表5-10 Syslog 服务端信息

选项	用途说明
状态	必选项。默认为“启用”
IP	必填项。填写服务器IP
端口	必填项。填写端口。默认为514
发送者	必填项。填写发送者。默认为“sender”

b. 单击<保存>，保存 Syslog 服务端配置。

(3) 点击<代理服务器配置>，打开代理服务器配置页面。如图 5-14 所示。

图5-14 配置代理服务器

a. 输入代理服务器选项内容。

Syslog 代理服务器选项参见表 5-11。

表5-11 代理服务器信息

选项	用途说明
状态	必选项。默认为“启用”
类型	默认为“SOCKS5”
IP	必填项。填写服务器IP
端口	必填项。填写端口
用户名	必填项。填写代理服务器的用户名
密码	必填项。填写用户名对应的密码

b. 单击<保存>，保存新增代理服务器配置。

5.1.8 SNMP

1. 功能简介

在告警时，通过 SNMP 服务器，可以将告警信息发送到 SNMP 接收端，供相关人查看和处理告警。

2. 配置 SNMP

(1) 进入[配置/告警通知/SNMP]，打开 SNMP 配置页面。如图 5-15 所示。

图5-15 SNMP 配置

(2) 填写相关内容。参见表 5-12。

表5-12 SNMP 信息

选项	用途说明
状态	必选项。默认为“启用”。
服务器IP	必填项。输入SNMP服务器IP。
端口	必填项。输入端口。默认为162。
OID	系统默认值。默认值为“public”。
MIB	使用系统默认值。
发送类型	必选项。 默认选择“发送单条”，在周期内发送的告警信息，接收端接收后，显示每条告警信息；若需要在接收端显示告警统计信息，可选择“发送统计信息”。

(3) 单击<保存>，保存 SNMP 服务器配置。

5.2 告警查询

5.2.1 高危(未处理)

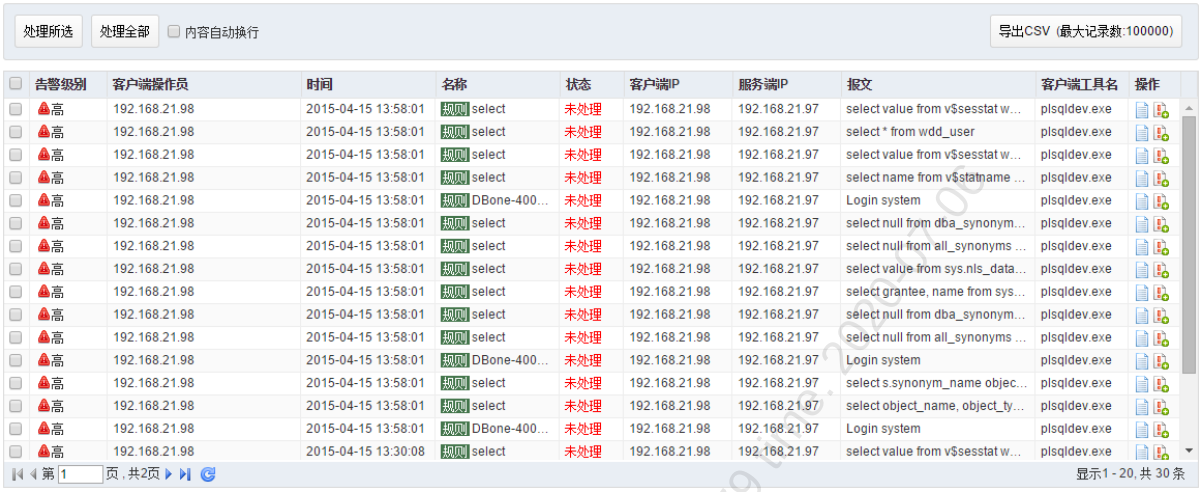
1. 功能简介

高危(未处理)指最近 12 小时内所有未处理的高危告警信息。

2. 处理告警

(1) 进入[风险/告警/高危(未处理)]界面，在未处理的列表中，勾选出需要处理的告警。如图 5-16 所示。

图5-16 未处理高风险列表



(2) 点击<处理所选>，打开处理页面，处理已选择的告警记录；

如需全部处理，点击<处理全部>，打开[处理]页面，处理列表中所有的告警记录。如图 5-17 所示。

图5-17 处理高风险

(3) 在处理页面，选择处理状态和添加描述信息。

(4) 点击<提交>，提交处理信息；点击<取消>，关闭页面，取消操作。

5.2.2 全部(未处理)

1. 功能简介

全部(未处理)包括最近 12 小时内所有未处理的告警信息。

2. 处理告警

(1) 进入[风险/告警/全部(未处理)]界面，在未处理的列表中，勾选出需要处理的告警。如图 5-18 所示。

图5-18 全部未处理风险列表

处理所选 处理全部 内容自动换行 导出CSV（最大记录数:100000）

告警级别	客户端操作员	时间	名称	状态	客户端IP	服务端IP	报文	客户端工具名	操作
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select value from v$sesstat w...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select * from wdd_user	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select value from v$sesstat w...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select name from v$statname ...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 DBone-400...	未处理	192.168.21.98	192.168.21.97	Login system	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select null from dba_synonym...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select null from all_synonyms ...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select value from sys.nls_data...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select grantee, name from sys...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select null from dba_synonym...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select null from all_synonyms ...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 DBone-400...	未处理	192.168.21.98	192.168.21.97	Login system	plsqldev.exe	
低	192.168.10.65	2015-04-15 13:58:01	特征 注入常用关...	未处理	192.168.10.65	192.168.11.148	GET http://192.168.11.148/pu...		
低	192.168.10.65	2015-04-15 13:58:01	特征 注入常用关...	未处理	192.168.10.65	192.168.11.148	GET http://192.168.11.148/stat...		
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select s.synonym_name objec...	plsqldev.exe	
高	192.168.21.98	2015-04-15 13:58:01	规则 select	未处理	192.168.21.98	192.168.21.97	select object_name, object_ty...	plsqldev.exe	

第 1 页，共2页 显示1 - 20, 共 35 条

(2) 点击<处理所选>，打开处理页面，处理已选择的告警记录；如需全部处理，点击<处理全部>，打开[处理]页面，处理列表中所有的告警记录。如图 5-19 所示。

图5-19 处理告警

(3) 在处理页面，选择处理状态和添加描述信息。

(4) 点击<提交>，提交处理信息；点击<取消>，关闭页面，取消操作。

5.2.3 告警分析

1. 功能简介

对某一时间段的告警信息进行分析，总结出 SQL 模板和发生的次数。

2. 分析查询

(1) 进入[风险/告警/告警分析]，打开告警分析界面。如图 5-20 所示。

图5-20 告警分析查询

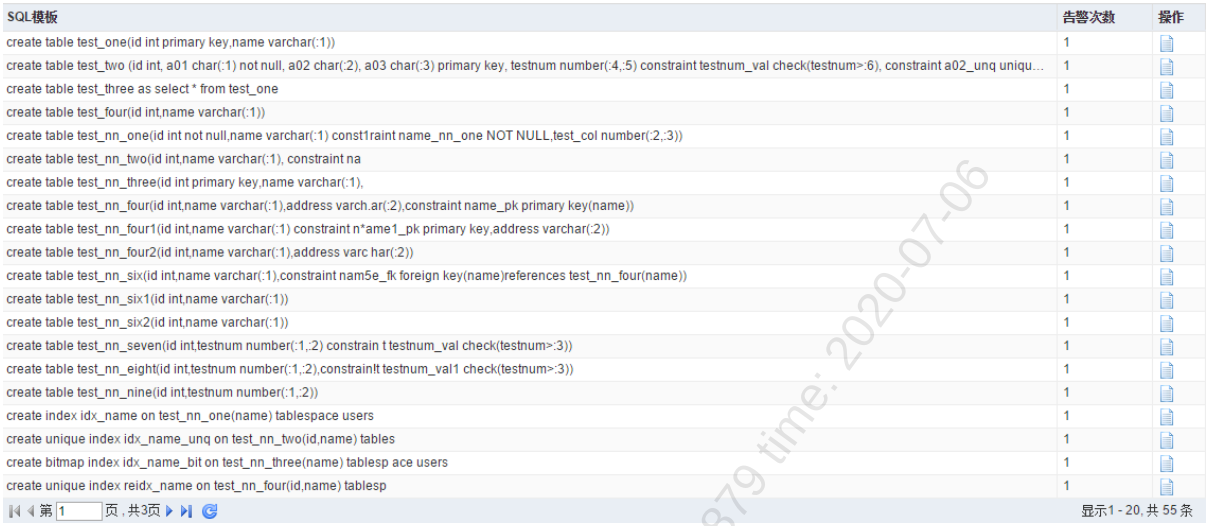
(2) 根据具体情况，填写相关的查询参数。参数说明见表 5-13。

表5-13 告警分析参数说明

选项	用途说明
风险级别	可选项。选择风险级别。默认为“全部”
业务主机群	可选项。选择业务主机群。默认为“全部”
客户端IP段	可填项。举例：192.168.3.*或192.168.*.*
客户端工具	可选项。默认为“全部”。具体参见13.1.2 客户端工具
时间范围	可选项。指告警发生的时间范围。默认为“最近12小时” 点击<自定义时间>，弹出自定义时间输入框
状态	可选项。告警处理的状态。默认为“未处理”。 点击<更多条件>，弹出处理相关的更多相关信息
规则	可选项。选择相关的规则库。默认为“全部”
来访客户网络	可选项。选择来访客户网络。默认为“全部”
客户端Mac段	可填项。输入客户端Mac段。举例：0a:0b:0c:*:*:*
账号	可选项。登录到数据库的账号

(3) 单击<查询>，查询告警分析结果。如图 5-21 所示。

图5-21 告警分析结果



SQL模板	告警次数	操作
create table test_one(id int primary key,name varchar(:1))	1	
create table test_two (id int, a01 char(:1) not null, a02 char(:2), a03 char(:3) primary key, testnum number(:4,:5) constraint testnum_val check(testnum>:6), constraint a02_unq uniqu...	1	
create table test_three as select * from test_one	1	
create table test_four(id int,name varchar(:1))	1	
create table test_nn_one(id int not null,name varchar(:1) const1raint name_nn_one NOT NULL,test_col number(:2,:3))	1	
create table test_nn_two(id int,name varchar(:1), constraint na	1	
create table test_nn_three(id int primary key,name varchar(:1),	1	
create table test_nn_four(id int,name varchar(:1),address varch.ar(:2),constraint name_pk primary key(name))	1	
create table test_nn_four1(id int,name varchar(:1) constraint n*ame1_pk primary key,address varchar(:2))	1	
create table test_nn_four2(id int,name varchar(:1),address varc har(:2))	1	
create table test_nn_six(id int,name varchar(:1),constraint nam5e_fk foreign key(name)references test_nn_four(name))	1	
create table test_nn_six1(id int,name varchar(:1))	1	
create table test_nn_six2(id int,name varchar(:1))	1	
create table test_nn_seven(id int,testnum number(:1,:2) constrain t testnum_val check(testnum>:3))	1	
create table test_nn_eight(id int,testnum number(:1,:2),constrainlt testnum_val1 check(testnum>:3))	1	
create table test_nn_nine(id int,testnum number(:1,:2))	1	
create index idx_name on test_nn_one(name) tablespace users	1	
create unique index idx_name_unq on test_nn_two(id,name) tables	1	
create bitmap index idx_name_bit on test_nn_three(name) tablesp ace users	1	
create unique index reidx_name on test_nn_four(id,name) tablesp	1	

告警分析结果说明见表 5-14。

表5-14 告警分析结果说明

选项	用途说明
SQL模板	对告警分析时间段内产生的告警记录进行分析，总结出SQL模板
告警次数	发生的告警次数
操作	单击，查看告警分析的详细信息，包括行为模板、触发规则、发生趋势、行为列表等信息

5.2.4 查询

1. 功能简介

查询告警信息。

有两种方式：

- 基础查询
- 高级查询

2. 基础查询

(1) 进入[风险/告警/查询]界面，单击“基本查询”标签打开基本查询界面。如图 5-22 所示。

图5-22 基础查询

(2) 根据基础查询条件，填写相关的查询参数。参见表 5-15。

表5-15 风险基础查询信息

选项	用途说明
时间范围	可选项。指告警发生的时间范围。默认为“最近12小时” 点击<自定义时间>，弹出自定义时间输入框
规则	可选项。选择相关的规则库。默认为“全部”
风险级别	可选项。选择风险级别。默认为“全部”
业务主机群	可选项。选择业务主机群。默认为“全部”
来访客户网络	可选项。选择来访客户网络。默认为“全部”
账号	可填项。登录到数据库的账号
客户端工具	可选项。默认为“全部”。具体参见13.1.2 客户端工具
操作系统用户	可填项。客户端操作系统用户
SID	可填项。SID信息
客户端IP段	可填项。查询方式可选择等于或不等于。举例：192.168.3.*或192.168.*.*
客户端Mac段	可填项。查询方式可选择等于或不等于。输入客户端Mac段。举例：0a:0b:0c:*:*:*
服务端端口	可填项。服务器端端口号
服务端IP段	可填项。查询方式可选择等于或不等于。举例：192.168.3.*或192.168.*.*
服务端Mac段	可填项。查询方式可选择等于或不等于。举例：0a:0b:0c:*:*:*
影响行数	可填项。查询方式可选择大于、小于、大于等于、小于等于、等于
SQL长度	可填项。查询方式可选择大于、小于、大于等于、小于等于、等于。单位可选择字节和KB
返回结果集大小	可填项。查询方式可选择大于、小于、大于等于、小于等于、等于。单位可选择字节、KB、MG、GB

执行时长	可填项。查询方式可选择大于、小于、大于等于、小于等于、等于。单位可选择毫秒和秒
状态	可选项，默认是“未处理”
返回结果集	可填项。返回结果集，支持模糊查询，但如果告警数据量大时不建议使用此查询条件
执行结果	可填项，执行结果，精确查询

(3) 相关查询参数填写后，点击<查询>，进行查询。

(4) 查看查询结果。查询结果查询结果显示在查询条件的下方。如图 5-23 所示。

图5-23 基本查询结果

基本查询结果信息说明参见表 5-16。

表5-16 基本查询信息说明

选项	用途说明
处理所选	处理选中的告警记录。修改告警记录的状态。 状态包括：“处理中”、“处理完成”、“延时处理”、“拒绝处理”和“其他”
处理全部	处理所有查询出的告警记录。修改告警记录的状态。 状态包括：“处理中”、“处理完成”、“延时处理”、“拒绝处理”和“其他”
内容自动换行	如选中，查询结果列的内容自动换行
归并列	将查询结果按一定的类型进行统计归并。 归并类型包括：“客户端工具名”、“客户端IP”、“账号”和“规则” 默认归并类型为：“客户端工具名”
导出CSV	将查询结果列导出为CSV格式文件，不支持客户端操作员和描述两列的导出。 导出文件名：eventlist.zip 最大记录数：100000

3. 高级查询

(1) 进入[风险/告警/查询]界面，单击“高级查询”标签打开高级查询界面。如图 5-24 所示。

图5-24 高级查询

(2) 根据基础查询条件，填写相关的查询参数。参见表 5-17。

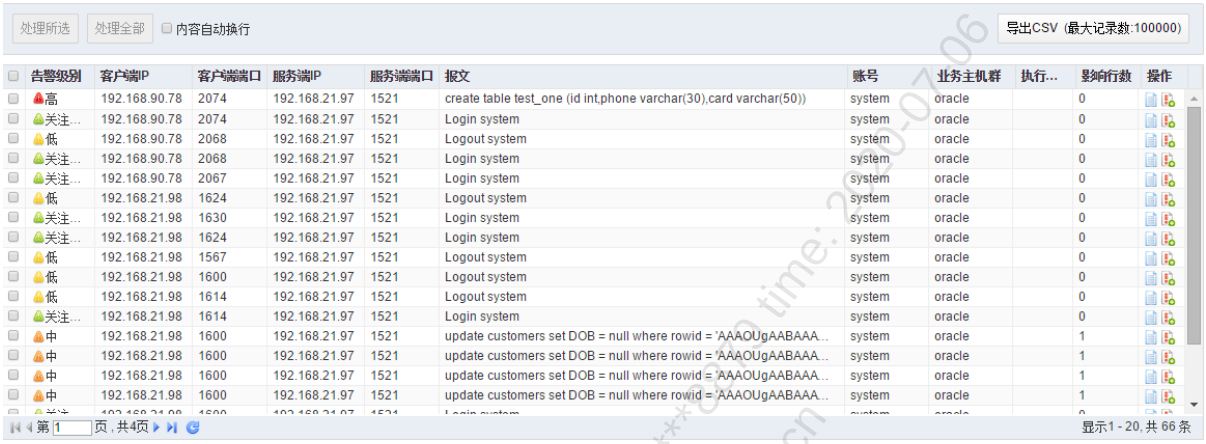
表5-17 风险高级查询信息

选项	用途说明
风险级别	必填项。默认为“全部”
操作类型	必填项。选择操作数据库的类型，默认为“全部”
业务主机群	可选项。选择业务主机群。默认为“全部”
规则	可选项。选择相关的规则库。默认为“全部”
客户端IP	可填项。客户端的IP地址
账号	可选项。登录数据库的账号
客户端工具	可选项。指告警发生的时间范围。默认为“最近12小时” 点击<自定义时间>，弹出自定义时间输入框
时间范围	可选项。指告警发生的时间范围。默认为“最近12小时” 点击<自定义时间>，弹出自定义时间输入框
报文	可填项。可填多个关键字，用空格隔开，表示同时满足。范围：2~255个字符
来访客户网络	可填项。 有两种方式： • 直接填写。可填写多个 IP，多个 IP 用以“,”分割； • 从“来访客户网络”中选择。“来访客户网络”的内容在[配置/常规/来访客户网络]中配置，也可以单击<例外 IP>，则如来源 IP 在“例外 IP”中，虽然也在“来访客户网络”中，但不触发告警 可填项，HTTP客户程序向服务器发送请求的时候必须指明请求类型。单击<添加>选择请求头类型，填写相关信息
服务端IP	可填项。服务端的IP地址
关联账号	可填项。与访问数据库相关联的账号。如登录某个信息系统的账号
SID	可选项。数据库的SID

(3) 相关查询参数填写后，点击<查询>，进行查询。

(4) 查看查询结果。查询结果查询结果显示在查询条件的下方。如图 5-25 所示。

图5-25 高级查询结果



查询结果信息说明参见表 5-16。

6 规则配置

6.1 规则配置（DB）

6.1.1 功能简介

规则配置（DB）的保护对象为数据库，包括规则配置、对象组管理、规则优先级和快速加载四个模块，满足规则配置的审计记录，会触发告警。

设备出厂时，默认对主流的数据库内置一些规则模板，此内置规则如需要使用，需要根据业务的实际情况进行修改配置使用。

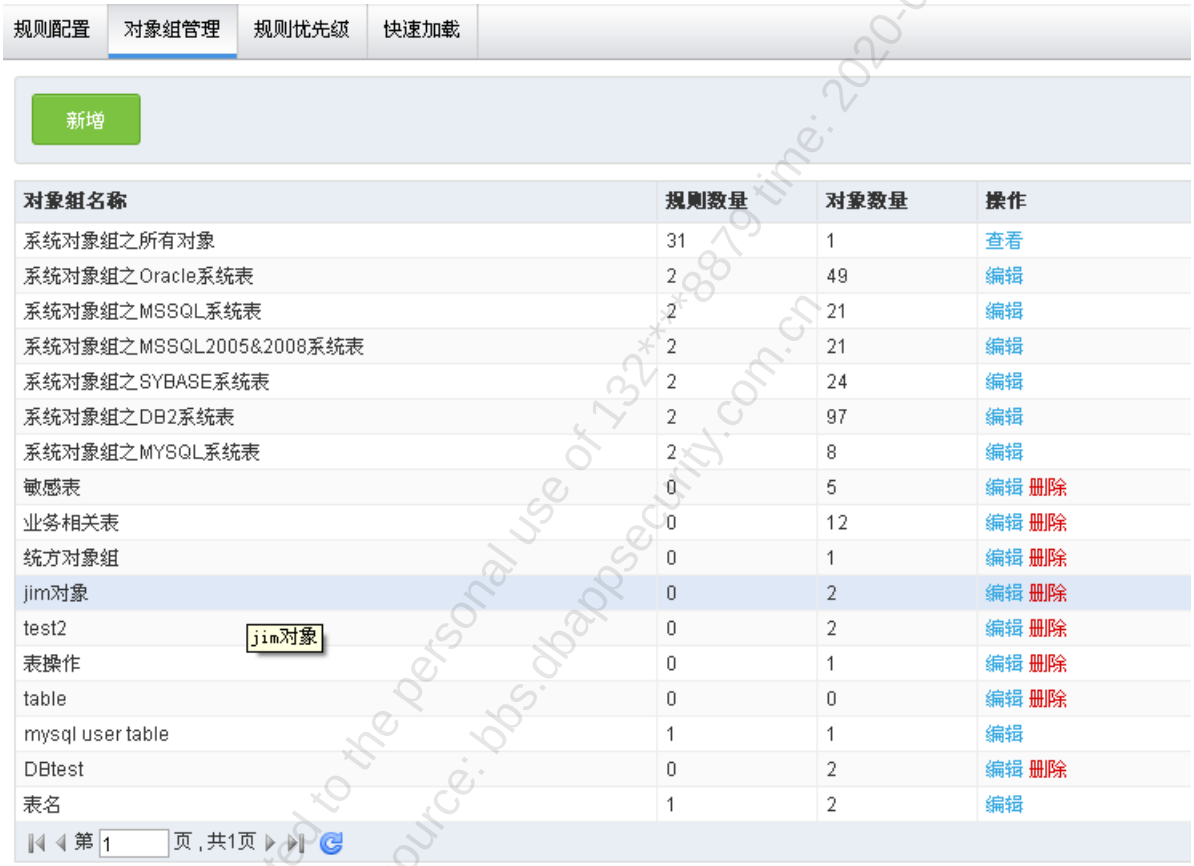
6.1.2 配置 DB 规则

1. 配置对象组

将相关的数据库对象(如表、用户、包、函数、存储过程、视图、字段等)划分到一个组内进行管理。

(1) 进入[规则/规则/规则配置(DB)]，单击“对象组管理”标签打开对象组管理界面。如图 6-1 所示。

图6-1 对象组管理



(2) 单击<新增>，打开新增页面。如图 6-2 所示。

图6-2 新增对象组

(3) 输入对象组名，单击<保存并添加对象>。如图 6-3 所示。

图6-3 保存对象组

(4) 选择添加对象类型，并输入对象名，单击<添加对象>。如图 6-4 所示。

图6-4 添加对象

(5) 单击<关闭>，返回对象组列表。如图 6-5 所示。

图6-5 对象列表

2. 配置规则

(1) 进入[规则/规则/规则配置(DB)]，单击“规则配置”标签打开规则配置界面。如图 6-6 所示。

图6-6 规则配置

(2) 单击<新增>，出现新增下拉列表框页面。如图 6-7 所示。

图6-7 新增规则组

(3) 在下拉列表中选择<新增规则组>进入规则组配置页面。如图 6-8 所示。

图6-8 配置规则组

(4) 输入规则组名称，单击<保存>即可添加规则组。

(5) 选择添加的规则组，单击<新增规则>打开规则配置界面。图 6-9 所示。

图6-9 新增规则 1

图6-10 新增规则 2

详细选项如表 6-1。

表6-1 DB 规则信息

选项	字段名称	用途说明
基本信息	规则名称	必填项，填入规则名称

	规则组	必选项，可选择自定义的规则组，也可以选择系统默认规则组
	规则等级	必选项，系统默认等级为高。等级包括高、中、低、关注行为、一般行为和不审计。 在[规则/规则/审计选项]页面，选择“满足条件审计”时，此处的“一般行为”等级按钮才可选 等级为“不审计”时，满足该规则的记录，不存放在系统中，在[审计/日常行为/综合查询]中查询不到记录信息
客户端	客户端IP	可填项，指访问业务类型的客户端IP地址。 有两种方式： • 直接填写。可填写多个 IP，多个 IP 用以“,”分割； • 从“来访客户网络”中选择。“来访客户网络”的内容在[配置/常规/来访客户网络]中配置，也可以单击<例外 IP>，则如来源 IP 在“例外 IP”中，虽然也在“来访客户网络”中，但不促发告警
	客户端工具	可选项，定义规则作用的客户端工具。也可点击“配置-客户端工具”链接管理客户端工具
	客户端端口	可选项，可配置多个值或区间，多个值间以逗号“,”分隔，例：10-15,20,25,30-40。
	客户端MAC地址	可填项，可填多值，多个值间以逗号“,”分隔 默认隐藏项，此项需要点击“显示更多”才能显示
	操作系统用户	可填项，可填多值，多个值间以逗号“,”分隔 默认隐藏项，此项需要点击“显示更多”才能显示
	主机名	可填项，可填多值，多个值间以逗号“,”分隔 默认隐藏项，此项需要点击“显示更多”才能显示
服务器	服务器IP	可填项，可填多值，多个值间以逗号“,”分隔
	服务端端口	可配置多个值或区间，多个值间以逗号“,”分隔，例：10-15,20,25,30-40。
	数据库账号	可填项，指数据库登录用户，可填多值，多个值之间以“,”分割。如：system,sys
	服务端MAC地址	可填项，可填多值，多个值间以逗号“,”分隔 默认隐藏项，此项需要点击“显示更多”才能显示
	SID(数据库名)	可填项，Oracle 数据库输入 SID，其他数据库输入数据库名，可填多值，多个值间以逗号“,”分隔。 默认隐藏项，此项需要点击“显示更多”才能显示
	业务类型	可选项，可选择单个或多个 默认隐藏项，此项需要点击“显示更多”才能显示
行为	对象组	可选项，指规则作用的对象组。在“对象组管理”标签页面管理对象组
	操作类型	可选项，指关注的操作类型。如select,update,delete等
	SQL模板	可填项，SQL模板的ID，可填多值，多个值间以逗号“,”分隔。
	SQL关键字	可填项， SQL关键字：可通过<增加>按钮添加多个关键字。支持以正则表达式方式匹配报文。单击<正则验证>输入报文内容，单击<提交>，验证输入内容与执行结果关键字中的正则表达式是否匹配 条件运算逻辑表达式：如SQL关键字填写后，此项为必填项。 条件间的关系，支持“与、或、非、括号”运算(&：与，|：或，~：非)，条件使用序号表示，

		即“1”表示条件1，例： 1&2，则代表有2个SQL关键字条件，且两个关键字都要满足才能告警。
	SQL长度	可填项，允许范围0字节到64K，输入0则不匹配该项 默认隐藏项，此项需要点击“显示更多”才能显示
	关联表数	可填项， SQL操作涉及表的个数大于等于此值,触发本规则.允许输入最大值为255。 默认隐藏项，此项需要点击“显示更多”才能显示
	操作对象	可选项，可选择单个或多个 默认隐藏项，此项需要点击“显示更多”才能显示
	WHERE子句	可选项，是否包含WHERE，三个选项：不判断、有WHERE子句、没有WHERE子句 默认隐藏项，此项需要点击“显示更多”才能显示
结果	执行时长	可填项，SQL执行所用的时间，允许配置从0到2000000000之间的任意范围。SQL执行时长属于此范围，则触发规则。
	影响行数	可填项，允许配置从0到2147483647之间的任意范围。SQL操作返回的记录数或受影响的行数属于此范围，则触发规则。
	返回结果集	可填项， SQL关键字：可通过<增加>按钮添加多个关键字。支持以正则表达式方式匹配结果集。单击<正则验证>输入结果集内容，单击<提交>，验证输入内容与返回结果关键字的正则表达式是否匹配 条件运算逻辑表达式：如SQL关键字填写后，此项为必填项。 条件间的关系，支持“与、或、非、括号”运算(&：与，|：或，~：非)，条件使用序号表示，即“1”表示条件1，例： 1&2，则代表有2个结果集条件，且结果集中需要同时满足这两个条件才能告警。
	返回结果集大小	可填项，允许范围0字节到3GB，输入0则不匹配该项。 默认隐藏项，此项需要点击“显示更多”才能显示
	执行结果	可填项，支持以正则表达式方式匹配 默认隐藏项，此项需要点击“显示更多”才能显示
其它	时间	可选项，选择任意时间，每天，每星期，每月
	每天告警最大个数	默认1000，最大只能输99999，如不想限制每天告警数，可输入0
	业务主机群	添加时可先不选，但如果想要此规则生效，必须要选择规则对应生效的业务主机群
	白名单	可选项，如果审计的记录内容符合白名单则不告警

(6) 输入相关的信息，单击<保存>即可添加规则。

3. 配置规则优先级

调整每个业务主机群下规则优先级，使审计记录按照规则优先级来触发告警。

(1) 进入[规则/规则/规则配置(DB)]，单击“规则优先级”标签打开规则优先级界面。如图 6-11 所示。

图6-11 规则优先级

(2) 选择某一业务主机群，右侧出现该业务主机群对应的规则。如图 6-12 所示。

图6-12 配置规则优先级

(3) 操作“上移”“下移”“置顶”“置底”图标，调整规则优先级。

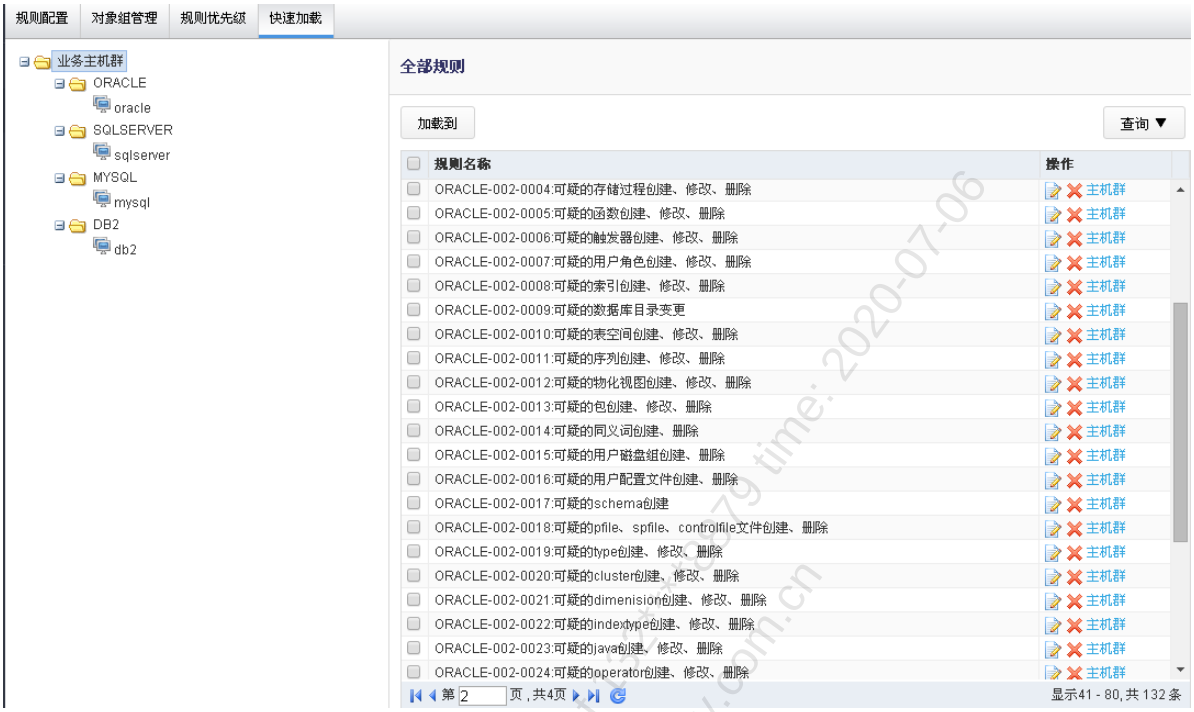
(4) 单击<保存调整>，即可配置业务主机群对应规则优先级。

4. 配置快速加载

对每个业务主机群快速加载或卸载规则。

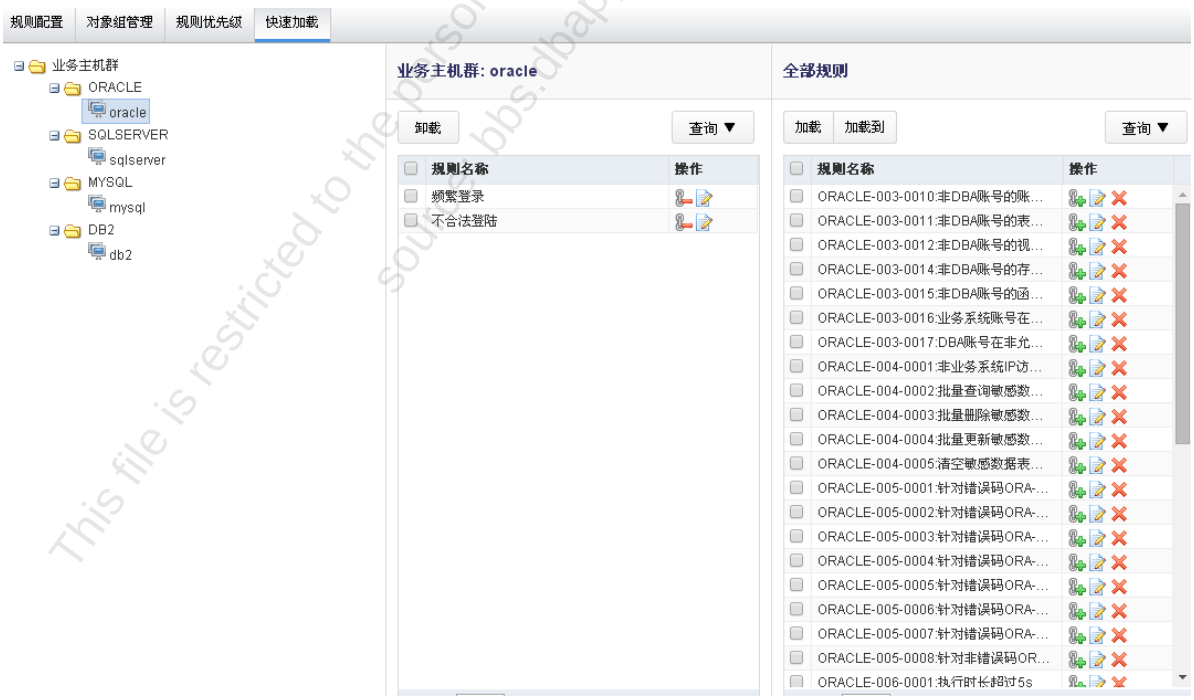
(1) 进入[规则/规则/规则配置(DB)]，单击“快速加载”标签打开快速加载界面。如图 6-13 所示。

图6-13 快速加载



(2) 选择某一个业务主机群，出现该业务主机群已加载和未加载的所有规则。如图 6-14 所示。

图6-14 配置快速加载



(3) 对已加载规则，单击“卸载”图标即可卸载规则。

(4) 对未加载规则，单击“加载”图标即可加载规则，也可以通过复选框选择多个规则进行加载

6.1.3 配置举例

1. 配置要求

为业务主机群 mysql 配置一条规则，名称为“login 规则”，登陆时长超过 10S 的触发告警，此规则挂载在“自定义规则组”中，且每天告警数不限。

2. 配置步骤

(1) 进入[规则/规则/规则配置(DB)]，单击“规则配置”标签打开规则配置界面。如图 6-15 所示。

图6-15 DB 规则配置

(2) 单击[新增/新增规则组]。如图 6-16 所示。

图6-16 新增 DB 规则组

(3) 在打开的新增规则组页面中，规则组名称为“自定义规则”。如图 6-17 所示。

图6-17 配置 DB 规则组

(4) 单击[保存]按钮，自定义规则组完成，选择“自定义规则”。如图 6-18 所示。

图6-18 选择 DB 规则组

(5) 单击[新增规则]，打开新增规则页面。如图 6-9 图 6-10 所示。

(6) 在“规则名称”中输入“login 规则”，在“结果”标签中的“执行时长”中输入“10000”，“每天告警最大个数”输入“0”，选择业务主机群“mssql 业务主机群[D2020]”。如图 6-19 所示。

图6-19 配置 DB 规则

(7) 单击[保存]，此规则配置完成，自动生效。

(8) 当满足“执行时长大于 10 秒”，且对应业务主机群是“mssql 业务主机群”，就会触发告警。

6.2 规则配置（WEB）

6.2.1 功能简介

规则配置（WEB）的保护对象为 WEB，包括规则配置、规则优先级和快速加载三个模块，满足规则配置的审计记录，会触发 WEB 告警。

6.2.2 配置 WEB 规则

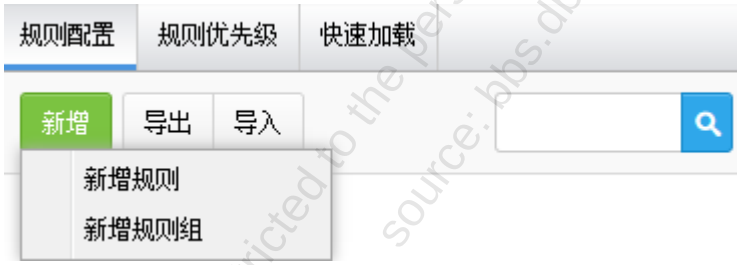
1. 配置规则

(1) 进入[规则/规则/规则配置(WEB)]，单击“规则配置”标签打开规则配置界面。如图 6-20 所示。

图6-20 WEB 规则配置

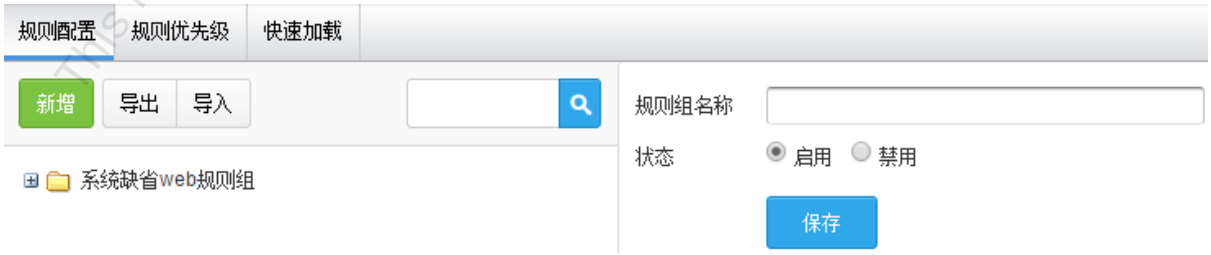
(2) 单击<新增>，出现新增下拉列表框面。如图 6-21 所示。

图6-21 新增 WEB 规则组



(3) 在下拉列表中选择<新增规则组>进入规则组配置页。如图 6-22 所示。

图6-22 配置 WEB 规则组



(4) 输入规则组名称，单击<保存>即可添加规则组。如图 6-23 所示。

图6-23 选择 WEB 规则组

(5) 选择添加的规则组，单击<新增规则>打开规则配置界面。如图 6-24 所示。

图6-24 新增 WEB 规则

详细选项如表 6-2。

表6-2 WEB 规则信息

选项	用途说明
规则名称	必填项，填入规则名称
状态	必填项，默认为“启用”，如选择禁用，则不可用
规则组	必选项，可选择自定义的规则组，也可以选择系统默认规则组
来源IP	可填项，指访问业务类型的客户端IP地址。 有两种方式： • 直接填写。可填写多个 IP，多个 IP 用以“,”分割； • 从“来访客户网络”中选择。“来访客户网络”的内容在[配置/常规/来访客户网络]中配置，也可以单击<例外 IP>，则如来源 IP 在“例外 IP”中，虽然也在“来访客户网络”中，但不触发告警
来源MAC地址	可填项，客户端的MAC地址
请求方法	可选项，规则中需要关注的HTTP的请求方法，如GET、POST、HEAD
URL	可填项，请求URL地址，支持正则验证
请求文件类型	可填项，可填写多值，多值间用‘,’隔开。如gif,jpg,js,html
HTTP版本	可选项，可选多项，HTTP目前有4个版本：0.9，1.0，1.1，2.0
请求头	可填项，HTTP客户程序向服务器发送请求的时候必须指明请求类型。单击<添加>选择请求头类型，填写相关信息
请求参数	可填项，请求中的参数信息，存在于cookie、post内容或者url中
响应码	可填项，由3位十进制数字组成，出现在由HTTP服务器发送的响应的第一行
白名单	可选项，如果审计的记录内容符合白名单则不告警
时间	可选项，选择任意时间，每天，每星期，每月
规则等级	必选项，系统默认等级为高。等级包括高、中、低、关注行为、一般行为和不审计。 在[规则/规则/审计选项]页面，选择“满足条件审计”时，此处的“一般行为”等级按钮才可选。 等级为“不审计”时，满足该规则的记录，不存放在系统中，在[审计/日常行为/综合查询]中查询不到记录信息
每天告警最大个数	默认1000，最大只能输99999，如不想限制每天告警数，可输入0
业务主机群	添加时可先不选，但如果想要此规则生效，必须要选择规则对应生效的业务主机群

(6) 输入相关的信息，单击<保存>即可添加规则。

2. 配置规则优先级

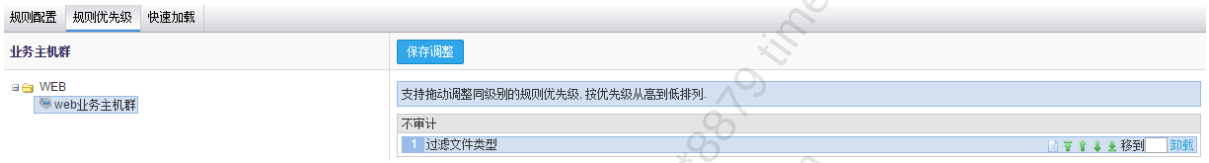
调整每个业务主机群下规则优先级，使审计记录按照规则优先级来触发告警。

(1) 进入[规则/规则/规则配置(WEB)]，单击“规则优先级”标签打开规则优先级界面。如图 6-25 所示。

图6-25 WEB 规则优先级

(2) 选择某一业务主机群，右侧出现该业务主机群对应的规则。如图 6-26 所示。

图6-26 配置 WEB 规则优先级



(3) 操作“上移”“下移”“置顶”“置底”图标，调整规则优先级。

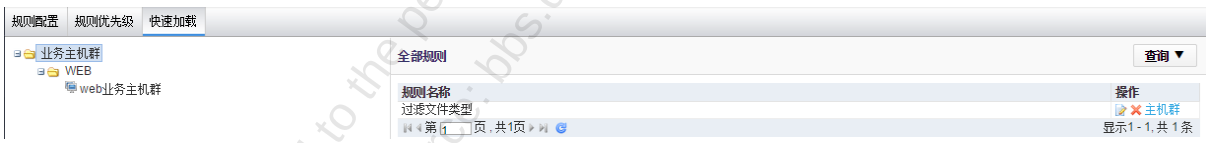
(4) 单击<保存调整>，即可配置业务主机群对应规则优先级。

3. 配置快速加载

对每个业务主机群快速加载或卸载规则。

(1) 进入[规则/规则/规则配置(WEB)]，单击“快速加载”标签打开快速加载界面。如图 6-27 所示。

图6-27 WEB 规则快速加载



(2) 选择某一个业务主机群，出现该业务主机群已加载和未加载的所有规则。如图 6-28 所示。

图6-28 配置 WEB 规则快速加载

(3) 对已加载规则，单击“卸载”图标即可卸载规则。

(4) 对未加载规则，单击“加载”图标即可加载规则。

6.3 规则白名单

满足规则白名单中条件的审计记录，不会触发告警。

6.3.1 配置准备

确定白名单的相关内容。

6.3.2 配置规则白名单

(1) 进入[规则/规则/白名单]界面，打开配置规则白名单页面，默认显示所有规则。如图 6-29 所示。

图6-29 规则白名单

(2) 选择需要加载白名单的规则，出现已选择的白名单和未选择的白名单。如图 6-30 所示。

图6-30 规则白名单查看

(3) 在白名单和未选择的白名单中，选择白名单，卸载或加载，即可添加、删除白名单。如图 6-31 所示。

图6-31 配置规则白名单

6.3.3 配置举例

1. 配置要求

配置一条白名单，即数据库账号为“sa”时，挂载到规则名为“login 规则”下，使触发规则名为“login 规则”告警时，不告警。

2. 配置步骤

(1) 配置一条规则，规则名为“login 规则”，配置规则见 4.2.2 配置 DB 规则。

(2) 进入[规则/规则/白名单]界面，打开配置规则白名单页面，默认显示所有规则。如图 6-32 所示。

图6-32 规则白名单列表

(3) 选择“login 规则”，右侧出现“未选择的白名单”。如图 6-33 所示。

图6-33 查看规则白名单

(4) 单击<新增>，打开规则白名单新增界面，输入“名称”为“sa 用户不告警”，“数据库账号”为“sa”。如图 6-34 所示。

图6-34 新增规则白名单

(5) 单击[保存]按钮，新增白名单成功。如图 6-35 所示。

图6-35 保存白名单

(6) 在“未选择白名单”中选择“sa 用户不告警”，单击[加载]，即可加载规则白名单到 login 规则中。如图 6-36 所示。

图6-36 加载规则白名单

(7) 白名单加载完成后，如果审计记录触发规则名为“login 规则”，但是账号为“sa”，则不告警。

7 统计告警

在某一固定时间范围内，根据统计条件（同一客户端 IP，同一数据库账号，同一会话，同一客户端工具）触发设置的规则，并达到设置的次数时，就会触发统计告警，目前统计告警不支持统计告警外送功能。

7.1 统计告警配置

统计告警配置如下：

(1) 打开[规则/规则配置（DB）]页面，点击<新增>按钮，打开规则配置页面，选择“统计规则”，如下图：

图7-1 统计告警

相关统计配置信息如下表：

表7-1 统计配置信息

选项	用途说明
统计时长	某一时间范围内统计告警，允许范围1秒到30分钟。
累计次数	只有告警触发次数达到累计次数时才会触发统计告警，允许范围2到30次。
累计条件	统计“告警触发”的条件，目前主要有四种条件，分别为同一会话、同一客户端IP、同一数据库账号、同一客户端工具

注：统计告警中“高、中、低”等级目前仅仅只是统计告警等级标识，没有优先匹配的概念，会全匹配所有统计告警条件。

(2) 配置统计规则信息和配置触发规则告警条件，如下图配置了5秒内同一客户端IP，触发“login”登录规则3次时，会生成统计告警。

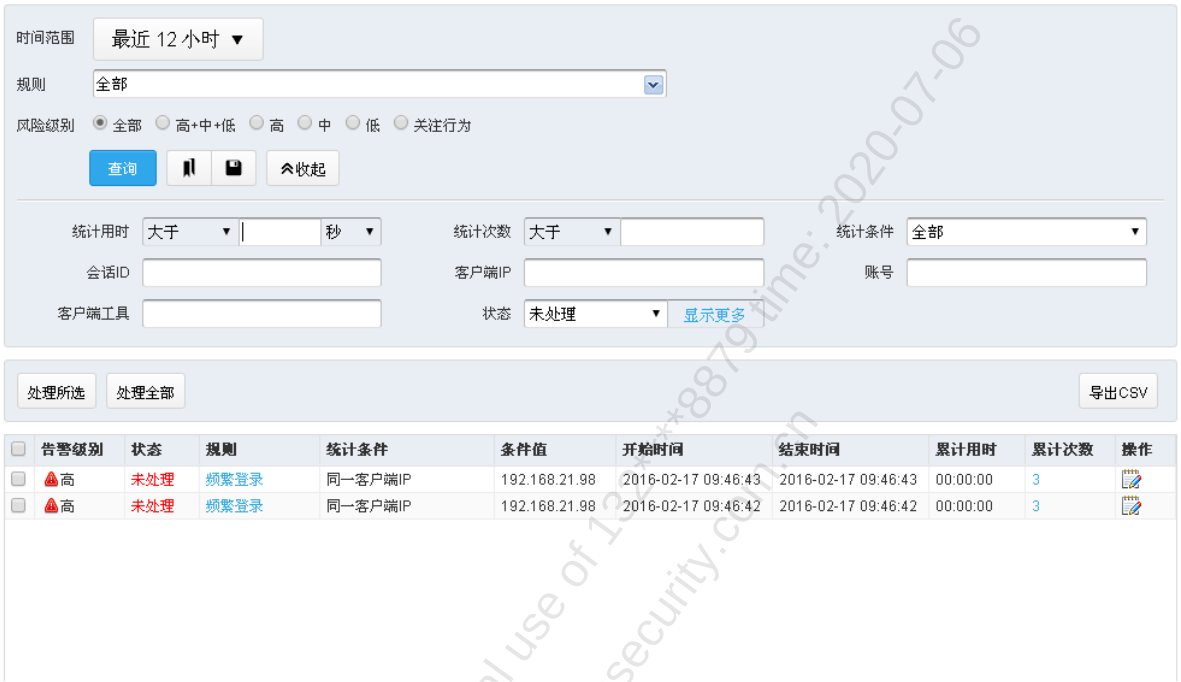
图7-2 统计规则配置

(3) 配置完成后，当同一个客户端IP，5秒内触发“login”登录规则3次时，就会产生统计告警。

7.2 统计告警查询

(1) 打开[风险/告警/统计告警]页面，可以根据条件查询统计告警。

图7-3 统计告警查询



列表中相关信息说明如下：

表7-2 统计列表信息说明

选项	用途说明
告警级别	分为高，中，低，关注行为
状态	只有告警触发次数达到累计次数时才会触发统计告警，允许范围2到30次。
规则	统计规则名，点击规则名链接可以查看具体的统计规则信息
统计条件	有同一客户端IP，同一会话，同一数据库账号，同一客户端工具
条件值	统计条件为同一客户端IP，则显示为IP地址 统计条件为同一会话，则显示会话ID 统计条件为同一数据库账号，则显示数据库账号 统计条件为同一客户端工具，则显示客户端工具
开始时间	统计开始时间
结束时间	统计结束时间
累计用时	统计时长
累计次数	统计周期内触发规则的记录数
操作	点击“操作”按钮，可以对此统计规则进行操作。

(2) 点击列表中“累计次数”，可以查看该统计告警详细信息，即触发规则的相关审计信息。

图7-4 告警详细

(3) 点击“导出 CSV”图标，可以导出统计信息。

8 反向代理

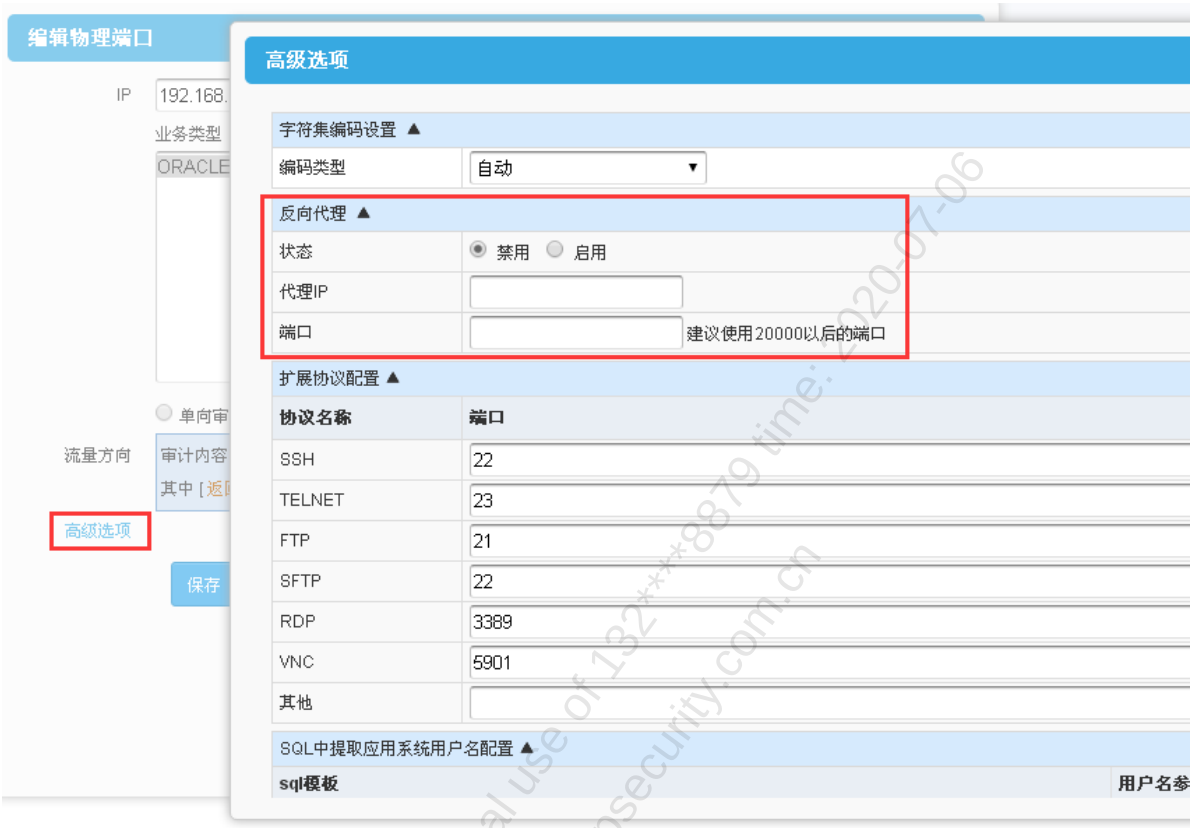
反向代理适用于流量不能到审计设备，又不允许安装 agent 代理软件的情况。

它的原理是直接把我们的审计设备当作一个代理，客户端数据库连接直接连接到我们的审计设备，通过审计设备再到达数据库，从而达到审计数据库的目的

配置过程如下：

(1) 打开[探测器/探测器相关配置/物理端口]页面，选择需要审计的数据库(如 192.168.21.97)，在物理端口编辑界面，点击“高级选项”打开设置代理服务器页面。

图8-1 代理服务器配置



(2) 配置反向代理服务器。

a) 状态：选择启用，如禁用则不再生效，代理不再生效。

b) 代理 IP：填写本台审计设备的 IP

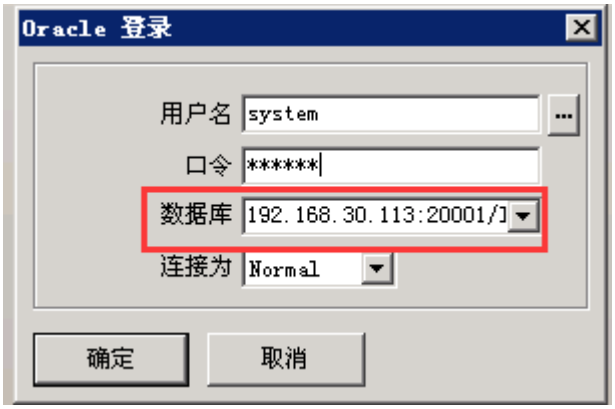
c) 端口：填写代理端口，以防端口已被占用，建议填写 20000 以后端口

(3) 配置完成后，返回并保存物理端口信息即可。

(4) 打开[探测器/探测器相关配置/探测器]页面，把上一步已配置好的物理端口挂载到对应的主机群下。

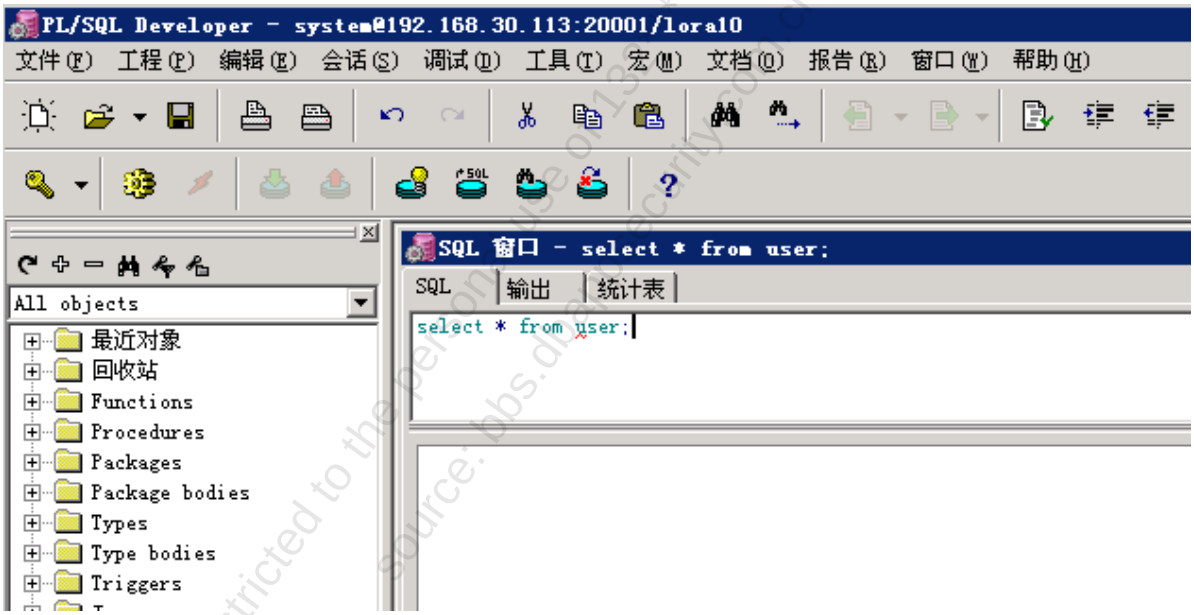
(5) 数据库客户端工具或其它系统的连接信息配置为反向代理服务器 IP 和端口，如上一步代理 IP 配置为审计设备 IP：192.168.30.113，端口：20001，如下 pl/sql 数据库客户端配置连接信息如下：

图8-2 客户端工具



(6) 登陆后，操作数据库，其实相当于登陆访问数据库 192.168.21.97

图8-3 操作数据库



(7) 打开[审计/日常行为/综合查询]页面，查看审计记录，能审计到相应的数据库。

图8-4 审计查询

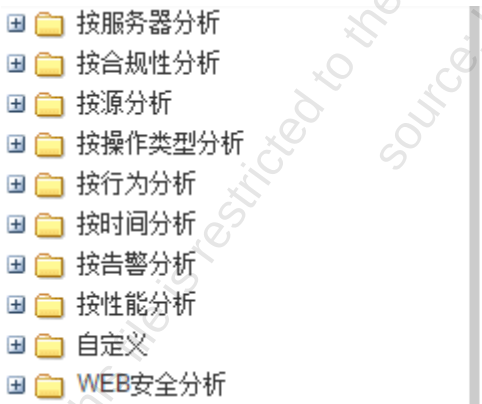
9 报表

9.1 报表预览

9.1.1 功能简介

预览某一时间段(默认统计当天的数据)的报表信息。如图 9-1 所示。

图9-1 报表预览



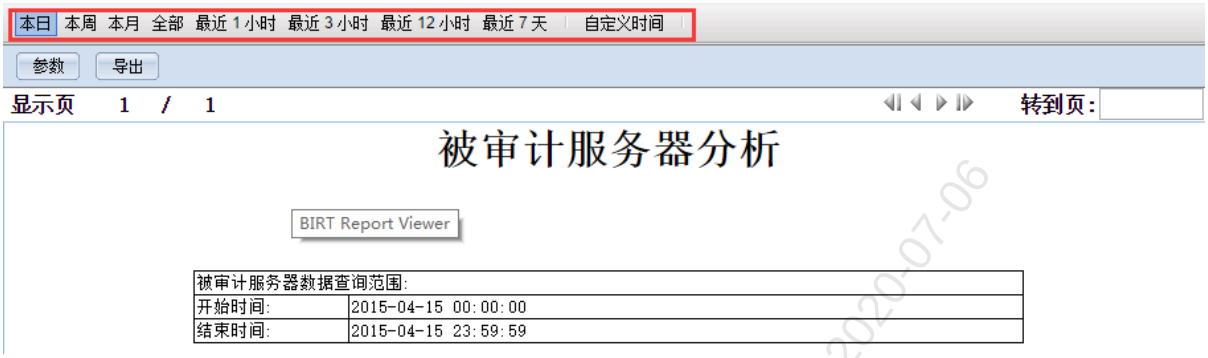
9.1.2 配置预览报表

(1) 通过[报表/报表/报表预览]，打开报表预览页面。

(2) 选择预览报表的周期。有两种方式：

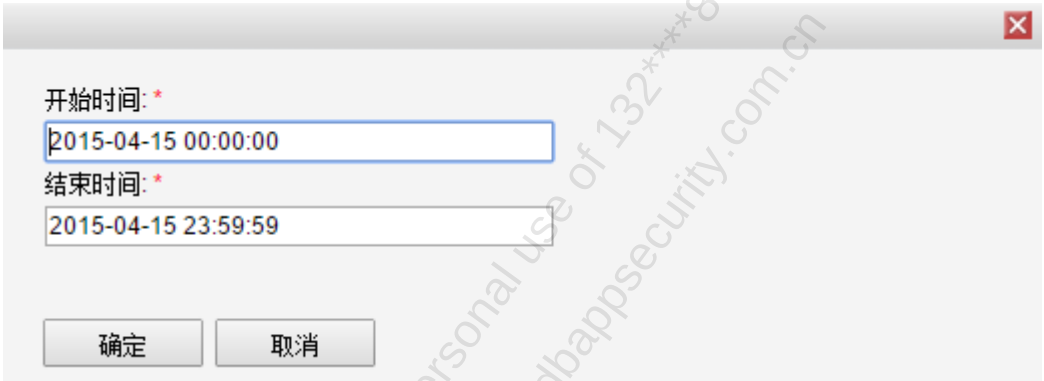
- 快速设置时间段。如图 9-2 所示。

图9-2 快速设置时间段



- 设置参数。点击<参数>，设置参数。如图 9-3 所示。

图9-3 设置参数



各报表说明，参见表 9-1。

表9-1 报表信息

报表类型	报表	用途说明
按服务器分析	被审计服务器分析	统计了被审计服务器的详细信息 包括服务器IP、源IP数、账号数、客户端工具数、告警数、审计记录数等情况
	总体审计情况分析	包括被审计服务器的详细信息报表，每台被审计服务器的审计记录数情况报表，各种数据库类型的比例图报表
按合规性分析	SOX	从计划与组织、确保和控制、评估风险三个方面，全面分析数据库安全状况
按源分析	账号使用情况分析	包括指定审计对象的各项详细信息、审计记录最多和最少的10个主机名、所有主机名对应的审计记录数、账号数最多的主机名、告警数最多的主机名、客户端工具数最多的主机名和指定审计对象主机名统计（访问量最大和最小TOP10）
	源IP访问分析	统计指定审计对象的各项详细信息、审计记录数最多和最少的10个源IP地址、审计记录所对应的所有的源IP地址、账号数最多的源IP地址、告警数最多的源IP地址、客户端工具数

		最多的源IP地址和指定审计对象源IP地址统计（访问量最大TOP10和最小TOP10）
	客户端工具分析	包含访问最多的客户端工具TOP10和访问最少的客户端工具TOP10，客户端工具对应审计记录数的情况
	指定审计对象主机名统计	统计了账号的活跃度、登陆次数账号最多的TOP10，登陆源IP数账号最多的TOP10，审计记录数账号最多的TOP10和最少的TOP10、所有账号的审计记录数和指定审计对象的各项详细信息
按操作类型分析	DDL操作分析	统计DDL操作数量最多的TOP10，以及从账号角度和源IP地址角度分析DDL操作的数量
	DML操作分析	统计DML操作类型的百分比情况，帮助管理人员了解整个数据库的DML操作情况，以辅助其优化数据库
	高危操作分析	统计高危数据删除行为的统计信息和高危数据删除行为的各项详细信息
按行为分析	账号新增及删除	统计了账号的新增和删除情况
	密码修改分析	统计了密码的修改情况、密码修改比较频繁的账号和密码修改最少的账号
	授权行为分析	统计了授权行为的账号和源IP、授权最多的10个账号和源IP
	权限回收分析	统计了权限回收的账号源IP、权限回收最多的10个账号和源IP
	用户权限分析(非查询)	每个帐号的操作类型、操作对象使用情况，了解每个账号的权限使用情况
	用户权限分析(查询)	每个帐号的操作类型、操作对象使用情况，了解每个账号的权限使用情况
	敏感或系统表访问统计	统计了敏感表被访问次数最多的TOP10
	认证管理分析	统计了登陆失败账号最多的TOP10、不同账号登陆最多的10个源IP地址、登陆失败源IP最多的TOP10
按时间分析	审计记录数分析	统计了所有被审计服务器记录数在不同时间段的变化情况，不同服务器IP的审计记录数不同时间段的变化情况
	并发会话数分析	按照时间展示并发会员曲线图，帮助审计人员了解数据库的实时会员状态
	在线用户数分析	按照时间展示在线用户数曲线图，帮助审计人员了解数据库的在线用户数情况
	在线源IP数分析	按照时间展示在线源IP地址书曲线图，帮助审计人员了解数据库的在线源IP地址情况
	在线客户端工具数分析	按照时间展示在线客户端工具数曲线图，帮助审计人员了解数据库的在线客户端工具情况
	DDL数量分析	按照时间展示DDL操作总数量和操作类型数量曲线图，帮助审计人员了解数据库的DDL操作情况
	DML数量分析	按照时间展示DML操作总数量和操作类型数量曲线图，帮助审计人员了解数据库的DML操作情况

	系统资源	展示数据库审计设备的CPU、内存、磁盘空间等利用情况，帮助审计管理人员了解审计设备的自身运行情况，即使发现审计异常情况
	流量分析(网口)	展示本台数据库审计的总体速率曲线和各采集端口速率情况
	流量分析(源IP)	展示本台数据库审计流量最大的10个访问IP
	流量分析(服务器IP)	展示本台数据库审计流量最大的10个被访问IP
按告警分析	规则告警分析	按规则告警级别（高/中/低）显示告警数量，从源IP角度了解各级别、各种攻击类型的特征告警情况，以源IP为视角，了解违规行为最多的帐号
	特征告警分析	从特征告警级别进行分析，从源IP角度了解各级别、各种攻击类型的特征告警情况，从URL角度了解告警情况，识别受攻击最严重的URL
按性能分析	SQL平均执行时长	展示平均执行时长最大的50个SQL语句，帮助客户提供数据库性能优化的参考数据，发现一些可能不太合理的SQL语句
	SQL单次执行时长TOP50	展示单次执行时长最大的50个SQL语句，帮助客户发现一些不合理的SQL语句，并找出执行者和时间，以方便客户分析具体原因，采取有效措施规避
	执行次数最多的SQL语句(TOP50)	展示执行次数最多的50个SQL语句，方便客户有针对性的优化SQL语句
WEB安全分析	WEB访问IP统计	统计访问URL数量最多的访问者IP以及具体URL的信息
	WEB访问URL统计	统计访问次数最多URL以及访问IP信息
	WEB访问返回时长统计	统计访问时长最大的URL

说明

如果是纯数据中心，有部份不支持显示的报表会隐藏，需要去探测器查看。

9.2 自动发送

9.2.1 功能简介

自动将报表发送到指定的邮箱中。

9.2.2 配置自动发送

(1) 打开[报表/报表/自动发送]，打开自动发送页面进行配置。如图 9-4 所示。

图9-4 自动发送

选项说明如表 9-2。

表9-2 报表自动发送信息

选项	用途说明
状态	必选项。默认为“启用”
生成周期	必选项。默认为“每天”
报表选择	选择报表中需要包含的内容。“已选项”列表显示包含的内容
文件格式	选择文件格式。支持“PDF”和“WORD”两种格式。默认为“PDF”
收件人	报表发送的接收人。需要先配置邮件服务器

注意

添加收件人前，需要先在[配置/告警通知/邮件]中配置邮件服务器。具体参见 5.1.4 邮件。

说明

自动发送报表的信息在[报表/报表/自动发送]页面的下方显示。

点击报表文件列表，下载生成的报表文件。

10 数据库扫描

10.1 端口扫描

1. 功能简介

根据指定 IP 段的端口，自动发现 Oracle 或 SQL Server 数据库。

2. 操作步骤

(1) 进入[风险/风险/端口扫描]，打开端口扫描页面。如图 10-1 所示。

图10-1 端口扫描

(2) 单击<端口扫描设置>，打开端口扫描设置页面。如图 10-2 所示。

图10-2 端口扫描设置

扫描设置选项说明见表 10-1。

表10-1 扫描设置选项说明

选项	用途说明
状态	必选项。默认为“启用”
扫描IP地址范围	必选项。 • 单个 IP 地址：192.168.1.10 • IP 网段：192.168.1.* • IP 地址段：192.168.1.1-192.168.1.100 最多添加10条IP地址范围
扫描类型及端口范围	必选项。 支持Oracle和SQLServer两种数据库类型。 Oracle默认端口：1521 SQLServer默认端口：1433
扫描周期	必选项。 • 单次扫描 • 定期扫描，设置定期时间点

(3) 单击<保存>，保存端口扫描设置；或单击<保存并立即扫描>，进行端口扫描，如图 10-3 所示。

图10-3 端口扫描

(4) 扫描结束后，已扫描到的数据库会端口扫描的下方显示。如图 10-4 所示。

图10-4 扫描结果

扫描结果说明见表 10-2。

表10-2 扫描结果说明

选项	用途说明
删除	删除选中的扫描端口项。下一次扫描到被删除的对象时，依然会添加到扫描结果中
忽略	忽略选中的扫描端口项，下一次扫描到被忽略的对象时，则不被添加到扫描结果中
操作系统修改为	可修改ORACLE类型的操作系统
添加到探测器	将选中的扫描端口添加到对应的探测器中
已添加端口修改	修改物理端口。具体参见4.2.2 物理端口
类型	支持ORACLE、SQLSERVER。默认为“类型(全部)”
IP	数据库对应的IP地址
端口	数据库对应的端口号
版本	数据库系统对应的版本号
SID	数据库对应的SID
操作系统	数据库运行的操作系统
扫描发现时间	端口扫描发生的时间

状态	扫描端口是否添加到探测器的状态，包括“已添加”和“未添加”
操作	对扫描端口的操作 • 删除：下一次扫描到被删除的对象时，依然会添加到扫描结果中 • 忽略：下一次扫描到被忽略的对象时，则不被添加到扫描结果中

10.2 风险评估

1. 功能简介

建立评估任务，扫描数据库，发现存在的风险或漏洞。

2. 操作步骤

(1) 进入[风险/风险/风险评估]，打开风险评估页面。如图 10-5 所示。

图10-5 风险评估

(2) 单击<新建评估任务>，打开新建评估任务页面。如图 10-6 所示。

图10-6 新增评估任务

(3) 输入新增评估任务选项信息。具体参见表 10-3。

表10-3 新增评估任务选项

选项	用途说明
状态	必选项。默认为“启用”
任务名称	必选项。 输入任务名称
扫描周期	必选项。 • 单次扫描 • 定期扫描，设置定期时间点

(4) 单击<保存>，保存评估任务，并弹出添加数据库页面。如图 10-7 所示。

图10-7 添加数据库

(5) 单击<添加数据库>，打开添加数据库信息页面。如图 10-8 所示。

图10-8 数据库信息

数据库选项说明参见表 10-4。

表10-4 数据库选项说明

选项	用途说明
评估类型	必选项。支持授权扫描和非授权扫描 • 授权扫描：需要填入数据库登陆信息 • 非授权扫描：不需要填入数据库登陆信息
数据库类型	必选项。数据库类型。如ORACLE、SQLSERVER等
IP	必填项。数据库 IP 地址
端口	必填项。数据库端口号
登录用户名	必填项。登录数据库的用户名
登录密码	必填项。登录数据库用户名对应的登录密码
SID	必填项。只有在数据库类型为ORACLE时，才需要SID
数据库名	必填项。只有在数据库类型为DB时，才需要数据库名

(6) 单击<添加>，添加参与评估任务的数据库信息。

(7) 添加任务成功后，在风险评估页面显示任务信息。如图 10-9 所示。

图10-9 添加任务成功

10.3 评估结果

1. 功能简介

查看数据库的风险评估结果。

2. 操作步骤

进入[风险/风险/评估结果]，进入评估结果页面。如图 10-10 所示。

图10-10 评估结果

11 权限管理

11.1 全部用户

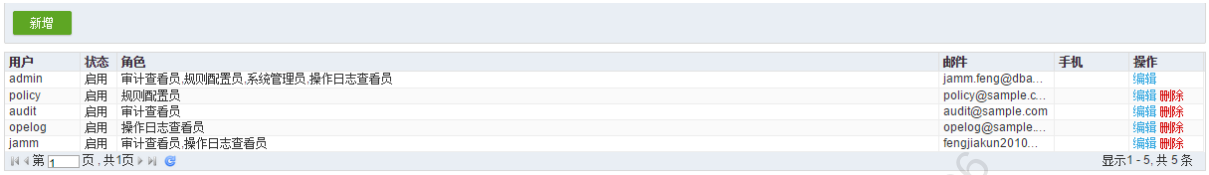
1. 功能简介

对登陆和操作系统的用户进行管理。包括新增、编辑和删除用户。

2. 用户配置

(1) 进入[系统/权限管理/全部用户]，打开全部用户配置页面。如图 11-1 所示。

图11-1 全部用户



系统自带四个用户信息。参见表 11-1。

表11-1 自带用户信息

用户	角色	用户名/密码	说明
admin	系统管理员	admin/Dbapp@2013	管理员
policy	规则配置员	policy/ Dbapp@2013	负责配置规则
audit	审计查看员	audit/ Dbapp@2013	负责查看审计记录
opelog	操作日志查看员	opelog/ Dbapp@2013	对系统自身的操作日志进行查看

注意

其中 admin 只支持编辑操作，不支持删除操作，其他三个用户支持编辑和删除操作。

系统自带四个角色信息。参见表 11-2。

表11-2 系统自带的角色信息

角色	权限说明
系统管理员	系统管理、探测器管理
规则配置员	配置规则、查看各类审计记录及风险、功能配置
审计查看员	查看风险、查看报表、查看审计记录
操作日志查看员	查看系统自身操作日志

注意

系统自带的角色不能编辑、删除。

(2) 点击<新增>，增加用户。如图 11-2 所示。

图11-2 新增用户

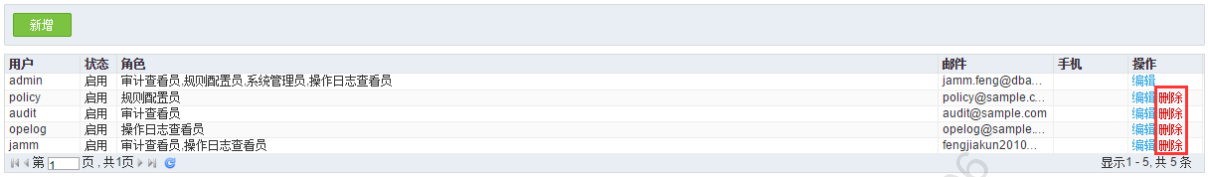
用户选项说明参见表 11-3。

表11-3 用户信息

选项		说明
基本信息	状态	必选项。默认值为“启用”
	用户	必填项。有字母和数字及下划线组成，长度3~32个字符
	描述	对用户进行描述。长度0~128个字符
	密码	必填项。输入密码，为数字和字母的组合。密码长度8~30个字符
	确认密码	必填项。再次输入密码，两次密码输入要一致
联系方式	Email	必填项。输入用户的Email。可以填写多个值并用','隔开
	手机	可选项。输入用户的手机号。可以填写多个值并用','隔开
角色		可选项。支持多选。系统自带的四种角色

(3) 点击<删除>，删除用户。如图 11-3 所示。

图11-3 删除用户



(4) 点击<编辑>，编辑用户。如图 11-4 所示。

图11-4 编辑用户

注意

密码修改后，系统暂不做强制性退出，请单独退出重新登录。

11.2 用户安全设置

1. 功能简介

主要包括登陆安全设置、密码长度设置和密码过期设置。

2. 安全设置

(1) 进入[系统/权限管理/用户安全设置]，打开用户安全设置页面。如图 11-5 所示。

图11-5 用户安全设置

(2) 配置相关内容，点击<保存>。选项说明参见表 11-4。

表11-4 安全设置信息

选项	说明
登录安全设置	• 设置多少秒内，登录次数达到一定限制，锁定该用户多少秒 • 设置登录时是否需要验证码
密码长度设置	• 设定密码的最短长度和最长长度 • 在新增用户设置密码时和修改用户密码时，会使用到该设置
密码过期设置	• 设置密码过期状态 • 设置密码过期时间

11.3 IP访问控制

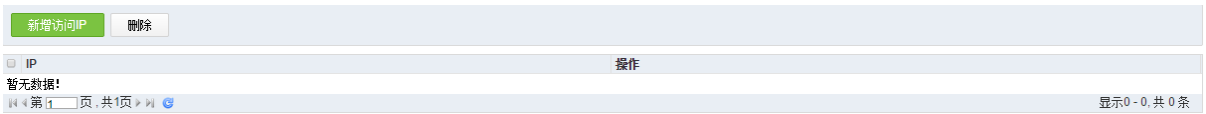
1. 功能简介

新增访问 IP 后，审计系统只允许列表中的 IP 访问，其他 IP 不允许登录系统。

2. 访问 IP 配置

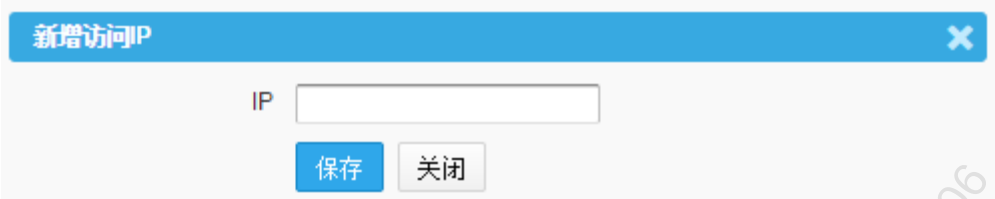
(1) 进入[系统/权限管理/IP 访问控制]，打开 IP 访问控制页面。如图 11-6 所示。

图11-6 IP 访问控制



(2) 点击<新增访问 IP>，新增访问 IP。如图 11-7 所示。

图11-7 新增访问 IP



新增访问 IP 选项说明参见表 11-5。

表11-5 访问 IP 信息

选项	用途说明
IP	必填项。 • 支持单个 IP 地址，如 192.168.1.10 • 支持 IP 网段，如 192.168.1.* • IP 地址段，如 192.168.1.1-192.168.1.100

(3) 点击<删除>，删除访问 IP。如图 11-8 所示。

图11-8 删除访问 IP

说明

删除也可以点击 IP 对应的<删除>，逐个删除。

(4) 点击<编辑>，编辑访问 IP。如图 11-9 所示。

图11-9 编辑访问 IP

12 数据维护

12.1 自动备份及恢复

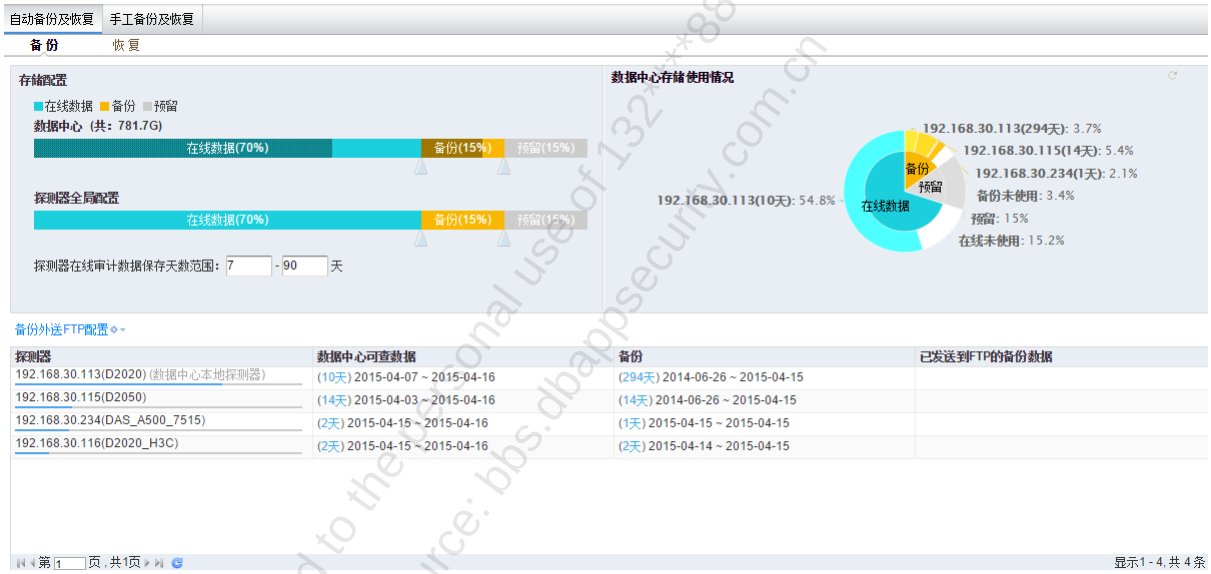
1. 功能简介

系统自动将数据备份到本地或外送到 FTP 服务器，同时也可以将本地或 FTP 服务器数据恢复到系统中，数据包括审计数据、配置数据和报表数据。

2. 自动备份

(1) 进入[系统/数据维护/备份和恢复]，点击<自动备份及恢复>下的<备份>，打开自动备份页面。如图 12-1 所示。

图12-1 自动备份



自动备份选项说明参见表 12-1。

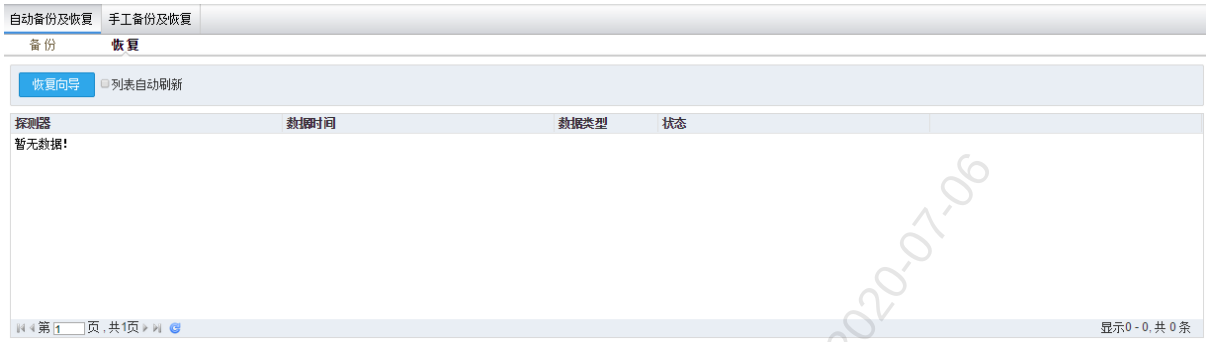
表12-1 自动备份信息

选项	用途说明
存储配置	数据中心和探测器全局配置的在线数据、备份数据、预留存储空间分配比情况
探测器在线审计数据保存天数范围	在线数据在探测器上保留的天数，如超过此日期，会自动清理相应的数据。默认值为3~365
数据中心存储使用情况	数据中心在线数据、备份和预留数据存储使用情况
备份外送FTP配置	配置FTP服务器。参见7.2.6 FTP

3. 自动恢复

(1) 进入[系统/数据维护/备份和恢复]，点击<自动备份及恢复>下的<恢复>，打开自动恢复页面。如图 12-2 所示。

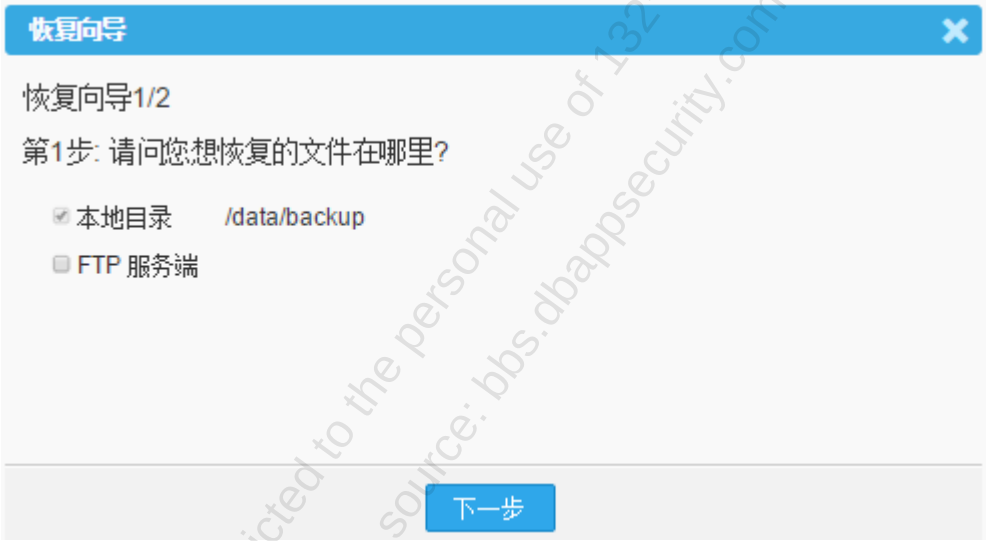
图12-2 自动恢复



(2) 自动恢复步骤。

a. 点击<恢复向导>，根据需要选择本地目录或者 FTP 服务器，点击<下一步>。如图 12-3 所示。

图12-3 恢复向导_步骤 1

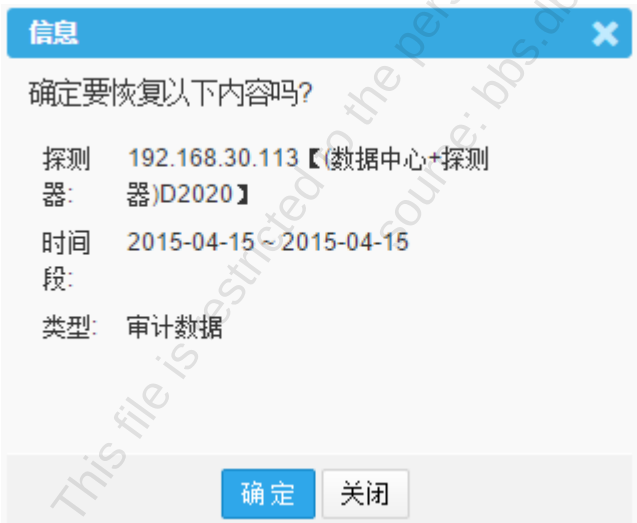


b. 进入恢复向导第二步，选择需要恢复的内容，点击【下一步】。如图 12-4 所示。

图12-4 恢复向导_步骤 2

c. 确认恢复。如图 12-5 所示。

图12-5 恢复向导_步骤 3



12.2 手工备份及恢复

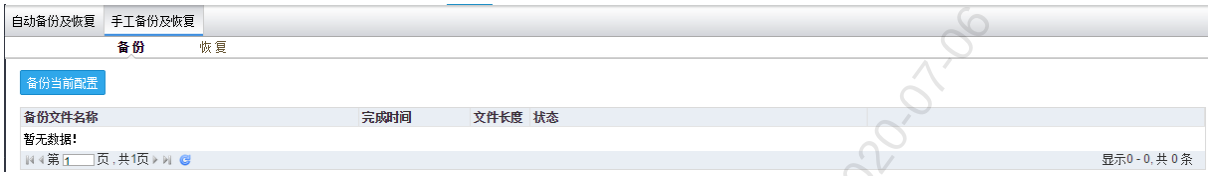
1. 功能简介

手动备份和恢复配置数据，不备份审计和报表数据。

2. 手工备份

(1) 进入[系统/数据维护/备份和恢复]，点击<手工备份及恢复>下的<备份>，打开手工备份页面。如图 12-6 所示。

图12-6 手工备份



(2) 手工备份步骤。

a. 点击<备份当前配置>，提交备份任务。

b. 备份完成后，会生成 RAR 格式的备份文件。可以点击备份文件，下载到本地计算机。如图 12-7 所示。

图12-7 手工备份配置文件

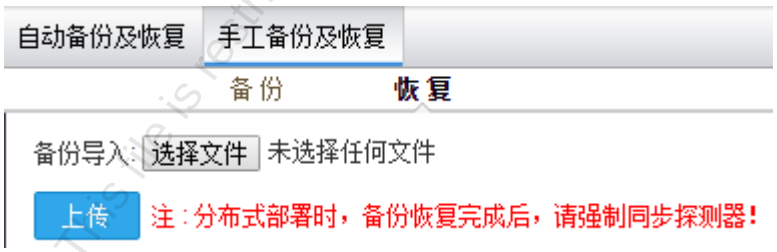
说明

点击备份文件后面的<删除>，删除备份文件。

3. 手工恢复

(1) 进入[系统/数据维护/备份和恢复]，单击<手工备份及恢复>下的<恢复>，打开手工恢复页面。如图 12-8 所示。

图12-8 手工恢复



(2) 手工恢复步骤。

a. 单击<选择文件>，选择备份恢复的 RAR 格式文件。

b. 单击<上传>，上传备份文件，恢复配置数据。

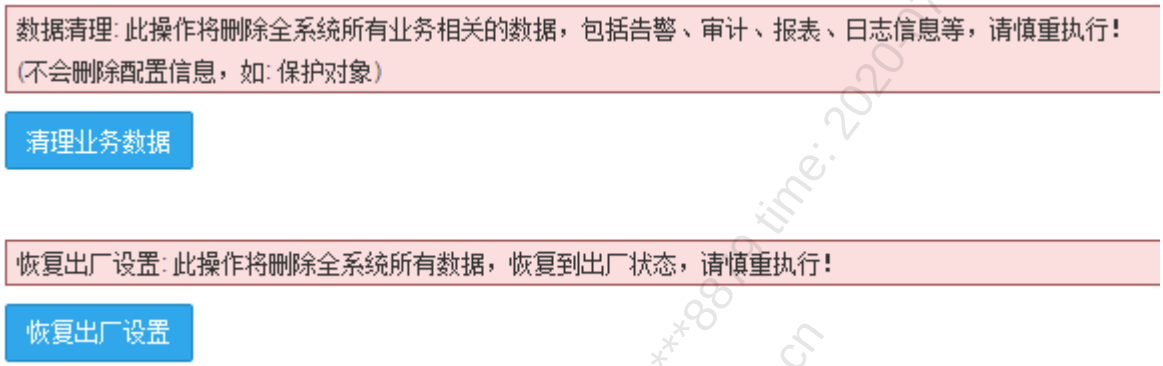
12.3 出厂设置

1. 功能简介

对系统做恢复和清理工作。此功能设置为谨慎操作区域。

(1) 进入进入[系统/数据维护/出厂设置]，打开出厂设置页面。如图 12-9 所示。

图12-9 出厂设置



13 系统

13.1 常规

13.1.1 引擎管理

1. 功能简介

管理审计引擎，启用或停止。

2. 配置引擎

(1) 进入[配置/常规/引擎管理]，打开引擎管理页面进行配置。如图 13-1 所示。

图13-1 引擎管理

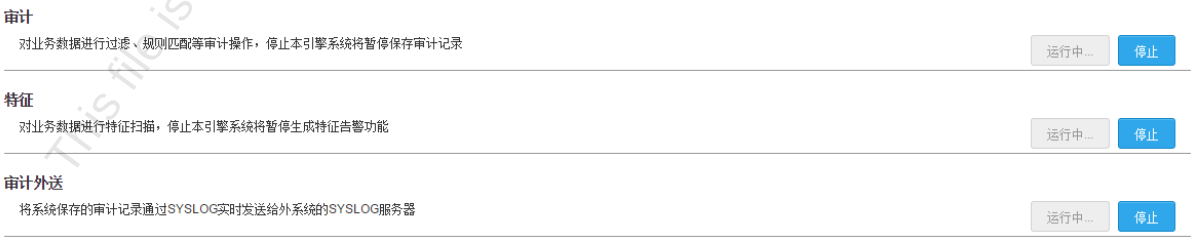


表13-1 引擎管理信息

选项	用途说明
审计	如果停止运行，则无法审计到数据，一般不建议用户停止运行审计引擎

特征	如果停止运行，则无法审计到特征数据，也不建议用户停止运行特征引擎
审计外送	如果停止运行，则无法将系统保存的审计记录通过SYSLOG实时发送给SYSLOG服务器，也不建议用户停止运行日志引擎

13.1.2 客户端工具

1. 功能简介

管理客户端工具。

2. 配置客户端工具

(1) 进入[配置/常规/客户端工具]，打开来访客户端工具界面。如表 13-2 所示。

图13-2 客户端工具

(2) 点击<新增>，打开新增页面，输入客户端工具保存即可。如图 13-3 所示。

图13-3 新增客户端工具

说明

客户端工具可自动采集。

13.1.3 来访客户网络

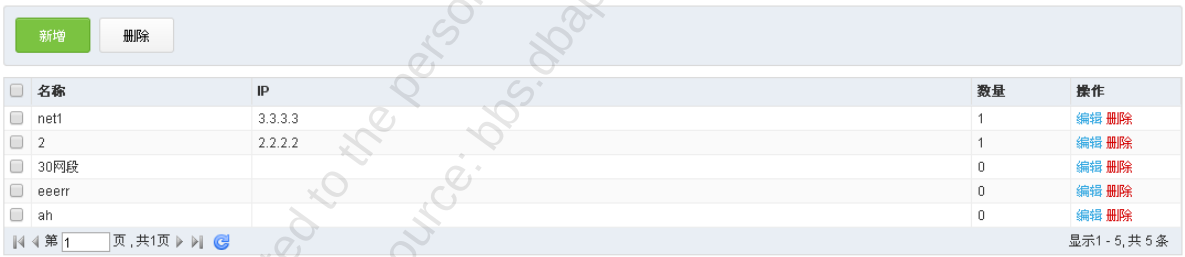
1. 功能简介

管理来访客户网络。

2. 配置来访客户网络

(1) 进入[配置/常规/来访客户网络]，打开来访客户网络配置界面。如图 13-4 所示。

图13-4 来访客户网络



(2) 点击<新增>，打开新增页面。如图 13-5 所示。

图13-5 新增来访客户网络

注意

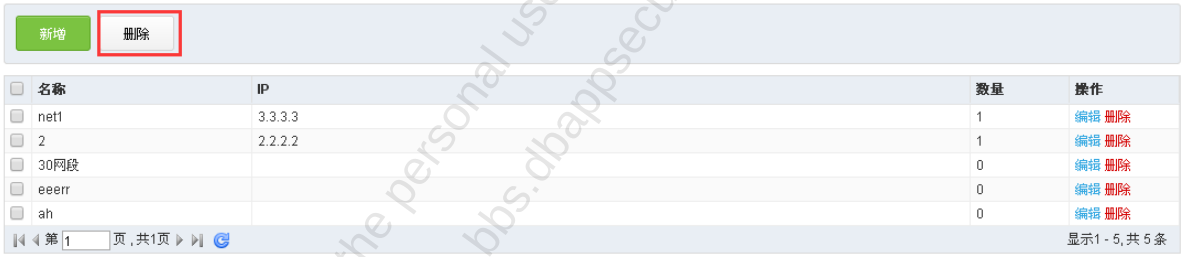
在点击<新增>，进入[新增来访客户网络]页面，此时只有“名称”输入框，输入名称后，点击<保存并添加 IP>后，才能看到添加 IP 的部分。

表13-2 来访客户网络信息

选项	用途说明
名称	必选项。输入后，点击<保存并添加IP>后，才能看到添加IP部分
IP	必选项。来访网络IP。 • 支持单个 IP 地址，如 192.168.1.10 • 支持 IP 网段，如 192.168.1.* • IP 地址段，如 192.168.1.1-192.168.1.100
已添加IP	已添加成功的IP

(3) 点击<删除>，删除选中的来访客户网络。如图 13-6 所示。

图13-6 删除来访客户网络



说明

删除也可以点击 IP 后面的<删除>，逐个进行删除。

(4) 点击<编辑>，修改来访客户网络。如图 13-7 所示。

图13-7 编辑来访客户网络

13.2 运行状态

13.2.1 系统资源

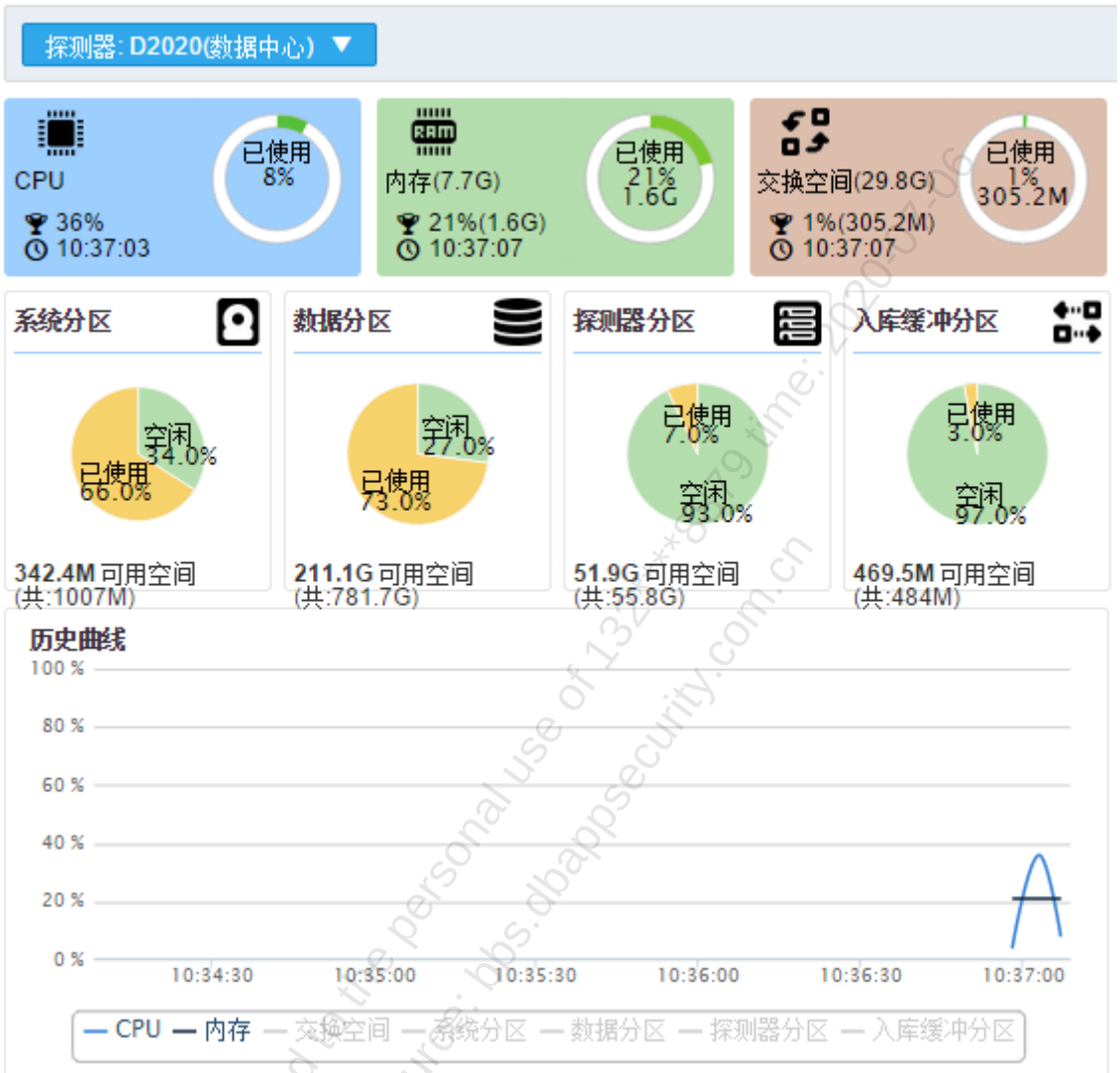
1. 功能简介

查看系统自身和各个探测器运行状态，包括 CPU 使用率、内存使用率、交换空间使用率和各个分区的使用情况。

2. 系统资源描述

进入[系统/运行状态/系统资源]，打开系统资源页面。如图 13-8 所示。

图13-8 系统资源



13.2.2 采集设备

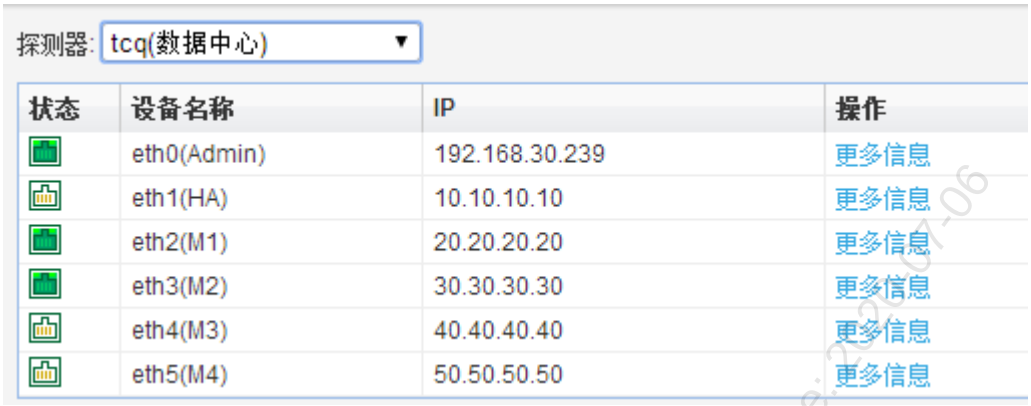
1. 功能简介

查看不同探测器各个采集网口的运行状态。

2. 采集设备描述

进入[系统/运行状态/采集设备]，打开采集设备页面。如图 13-9 所示。

图13-9 采集设备



13.2.3 同步验证

1. 功能简介

主要是将数据中心数据同步到各个探测器中，实现分布式部署。

2. 同步验证配置

(1) 进入[系统/运行状态/同步验证]，打开同步验证页面。如图 13-10 所示。

图13-10 同步验证

(2) 点击<强制同步>，会使用数据中心的数据覆盖指定探测器的数据。

13.3 系统管理

13.3.1 网络配置

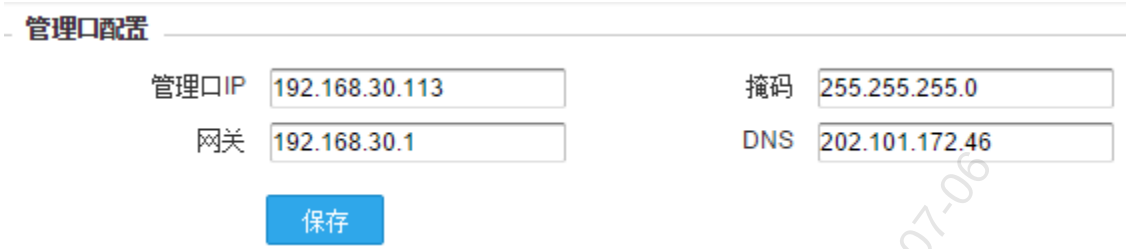
1. 功能简介

对网络管理口进行配置。

2. 网络配置

(1) 进入[系统/系统管理/网络配置]，打开网络配置页面。如图 13-11 所示。

图13-11 网络配置



(2) 配置相关的网络信息，点击<保存>即可。

说明

管理口 IP 修改完成后，系统会自动退出并跳转到新的 IP 重新登录。

13.3.2 时钟同步

1. 功能简介

把本机时间与服务器时间同步。

2. 时钟同步配置

(1) 进入[系统/系统管理/时钟同步]，打开时钟同步页面。如图 13-12 所示。

图13-12 时钟同步

(2) 配置时钟同步服务器 IP，点击<保存>，保存配置。

13.3.3 SNMP 配置

1. 功能简介

配置简单网络管理协议，方便对设备的管理。

2. SNMP 配置

(1) 进入[系统/系统管理/SNMP 配置]，打开 SNMP 配置页面。如图 13-13 所示。

图13-13 SNMP 配置

(2) 选择状态、SNMP 版本和填写 Community string。参见表 13-3。

表13-3 SNMP 配置项

选项	用途说明
状态	关闭或开启
SNMP版本	必选项
Community string	设置Community string

13.3.4 许可证

1. 功能简介

查看功能许可和上传许可证。

2. 许可证

(1) 进入[系统/系统管理/许可证]，打开许可证页面。如图 13-14 所示。

图13-14 许可证

(2) 单击<上传许可证>，选择许可证，单击<上传>，上传相应的许可证。如图 13-15 所示。

图13-15 上传许可证

(3) 单击<查看功能许可>，查看功能许可。如图 13-16 所示。

图13-16 查看功能许可

13.3.5 手动升级

1. 功能简介

用户从软件销售商处获得升级包后，通过页面升级系统。

2. 手动升级配置

(1) 进入[系统/系统管理/手动升级]，打开手动升级页面。如图 13-17 所示。

图13-17 手动升级

(2) 单击<选择文件>，选择相应的升级包。

(3) 单击<上传>，上传文件成功后，后台自动升级。参见表 13-4。

表13-4 文件上传配置

选项	用途说明
选择文件	选择升级包。 • 升级包不能大于 400M • 一次升级过程大概需要 5~10 分钟。如有多个升级包，切勿一次全部上传，需要一个升级完成后，再进行下一个 • 升级过程中可能会重启 WEB 服务，升级是否完成可通过刷新界面或使用排错[日志分析]查看升级日志
上传	上传升级包，升级系统 • 升级包上传后，请勿在对系统进行操作，防止发生意外导致升级包无法上传，从而导致升级失败
刷新	查看最近一次升级情况

13.3.6 系统调试

1. 功能简介

系统调试相关设置，包括端口管理、日志打包和 tcpdump 抓包。

2. 系统调试

(1) 进入[系统/系统管理/系统调试]，打开系统调试页面。如图 13-18 所示。

图13-18 系统调试

(2) 单击<关闭端口>(如图 13-18)，关闭 ssh、排错平台或 mysql 服务端口。

(3) 配置日志打包。选项说明参见表 13-5。

表13-5 日志打包信息

选项	用途说明
日志时间	生成日志的时间
截取行数	截取日志的行数。范围：1~200 万行

(4) 配置 tcpdump 抓包(如图 13-18)。

a. 单击<新建抓包任务>，新建任务。如图 13-19 所示。

图13-19 新建抓包任务图

新建抓包任务选项说明参见表 13-6。

表13-6 新建抓包任务说明

选项	用途说明
端口	抓包的端口
最大抓包时长	抓包持续时长。范围：1~86400 秒
最大文件大小	文件的最大值。范围：1~10480M
过滤串	包的过滤串

说明	最大抓包时长、最大文件大小有一个条件满足时，就会自动压缩抓包文件，显示在文件列表中。

b. 单击<确定>，添加新建任务；点击<关闭>，取消操作。

c. 操作抓包文件。在文件列表中，单击<下载>，下载对应的抓包文件；单击<删除>，删除对应的抓包文件；单击<查看 md5>，查看抓包文件的 md5。如图 13-20 所示。

图13-20 下载抓包文件图

说明	抓包文件下载完成后请及时删除压缩包，以免占用太多的磁盘空间。

13.3.7 关机

1. 功能简介

关闭或重启设备。

2. 关机

(1) 进入[系统/系统管理/关机]，打开关机页面。如图 13-21 所示。

图13-21 关机

(2) 单击<重启>，重启设备。

(3) 单击<关机>，关闭设备。

14 日志

14.1 操作日志

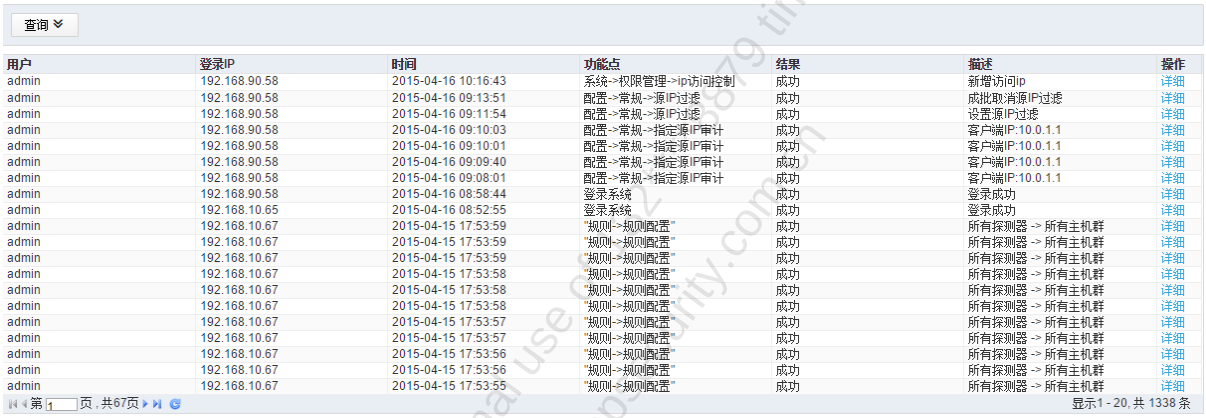
1. 功能简介

记录用户对系统的操作日志。

2. 操作日志

（1） 进入[日志/日志/操作日志]界面。如图 14-1 所示。

图14-1 操作日志列表



（2） 单击某一条日志<详细>，进入详细页面。如图 14-2 所示。

图14-2 操作日志详细

14.2 系统日志

1. 功能简介

记录系统相关的日志信息。

2. 操作日志

(1) 进入[日志/日志/系统日志]界面。如图 14-3 所示。

图14-3 系统日志列表

查询 处理

	发生时间	探测器	类型	状态	事件级别	内容	操作
	2015-05-04 14:49:26	tcq	异常日志	未处理	一般告警	主机当前交换空间使用率[41%]已超过[40%]的限定门限!	详细
	2015-05-04 13:59:13	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[97.0%]，超过了设定的[80.0%]	详细
	2015-05-04 09:48:05	tcq	异常日志	未处理	一般告警	主机当前交换空间使用率[40%]已超过[40%]的限定门限!	详细
	2015-05-04 09:28:00	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[96.0%]，超过了设定的[80.0%]	详细
	2015-05-04 05:06:50	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[95.0%]，超过了设定的[80.0%]	详细
	2015-05-04 00:35:40	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[94.0%]，超过了设定的[80.0%]	详细
	2015-05-04 00:05:32	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[93.0%]，超过了设定的[80.0%]	详细
	2015-05-03 19:44:23	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[93.0%]，超过了设定的[80.0%]	详细
	2015-05-03 14:53:07	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[92.0%]，超过了设定的[80.0%]	详细
	2015-05-03 10:01:50	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[91.0%]，超过了设定的[80.0%]	详细
	2015-05-03 05:10:34	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[90.0%]，超过了设定的[80.0%]	详细
	2015-05-03 00:09:14	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[89.0%]，超过了设定的[80.0%]	详细
	2015-05-02 18:47:50	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[88.0%]，超过了设定的[80.0%]	详细
	2015-05-02 13:26:26	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[87.0%]，超过了设定的[80.0%]	详细
	2015-05-02 08:15:04	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[86.0%]，超过了设定的[80.0%]	详细
	2015-05-02 02:53:40	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[85.0%]，超过了设定的[80.0%]	详细
	2015-05-02 00:02:55	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[84.0%]，超过了设定的[80.0%]	详细
	2015-05-01 21:02:08	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[84.0%]，超过了设定的[80.0%]	详细
	2015-05-01 15:00:33	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[83.0%]，超过了设定的[80.0%]	详细
	2015-05-01 09:09:00	tcq	异常日志	未处理	一般告警	受监控分区[/home]已使用[82.0%]，超过了设定的[80.0%]	详细

第 1 页，共2页　　显示1 - 20, 共 22 条

(2) 单击某一条日志<详细>，进入详细页面。如图 14-4 所示。

图14-4 操作日志详细

详细	
发生时间	2015-4-16 7:20:09
探测器	D2020
类型	异常日志
事件级别	一般告警
内容	受监控分区[/data]已使用[82.0%]，超过了设定的[80.0%]
处理	
状态	处理中
描述	已提交相关人员处理
	提交

(3) 在详细页面，对日志进行处理，点击<提交>，可处理该日志。