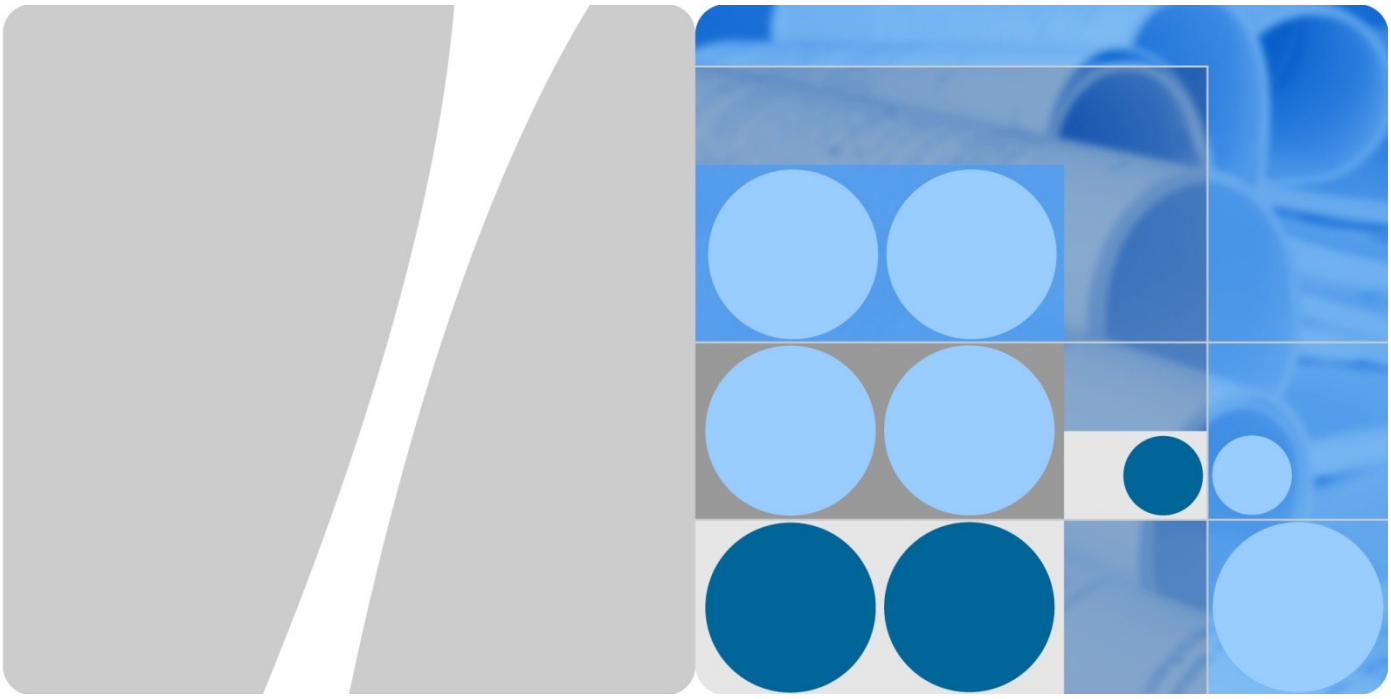


华为 UMA-DB 数据库审计特性描述

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目　录

1 策略管理特性

1.1 资产

【资产】用于数据库服务器的添加、修改、控制策略的应用等信息。

资产设置项有：来源限制、信任程序、信任账号、记录控制和应用策略。

【来源限制】用于控制客户端的访问操作 IP，其中分忽略 IP 地址和限定监测 IP 地址：忽略 IP 地址是将访问操作数据库的 IP 地址添加到里面即可不审计了；限定监测 IP 地址是将特定“嫌疑”的访问 IP 地址添加到里面进行审计。

【信任程序】用于将信任的数据库客户端程序名添加到里面，在此列表里的客户端程序所发起的数据库行为不会产生异常告警。

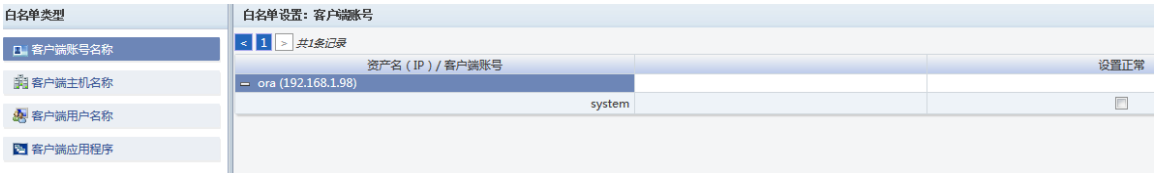
【信任账号】用于将信任的数据库账号添加到受信任账号列表里面，在此列表中的数据库账号所发起的数据库行为不会产生异常告警。

【记录控制】用于是否要启用审计客户端访问操作数据库所产生的原始数据包。注意：此处使用应与【来源限制】项一起结合使用，否则可能会产生大量的数据包，致使系统存储空间容易满。

【应用策略】是查看应用在该数据库资产上的策略列表，可删除其已应用的策略。

1.2 白名单

在【白名单】中，用户可以设置客户端的数据库账号、客户端主机名、客户端用户名和客户端应用程序是否异常。如果勾选上了说明其是正常的日志记录，就不产生异常告警；如果未勾选说明是异常的日志记录，就产生异常告警。



1.3 对象

【对象】的设置涉及到策略的应用，在编辑策略时需要编辑可选项，用于对数据库资产的策略告警。其中包括：标准 SQL 命令、客户端网络地址、客户端应用程序、数据库用户名称、客户端主机名称、客户端系统用户、表组。设置相应的策略要素与【策略】中的【匹配条件】一一对应。

【标准 SQL 命令】是设置 SQL 语句、SQL 命令等要素进行策略告警。

【客户端网络地址】是设置源操作主机的网络地址，用于策略设置中的 IP 告警。

【客户端应用程序】是设置源操作主机上的数据库客户端程序，用于策略设置中的程序告警。

【数据库用户名称】是设置数据库的账号，用于策略设置中的数据库账号告警。

【客户端主机名称】是设置源操作主机上的计算机名，用于策略设置中的计算机名告警。

【客户端系统用户】是设置源操作主机上的系统账户，用于策略设置中的系统账户告警。

【表组】是设置数据库的表名、字段名等数据库表信息，用于策略设置中的数据库表告警。

1.4 策略

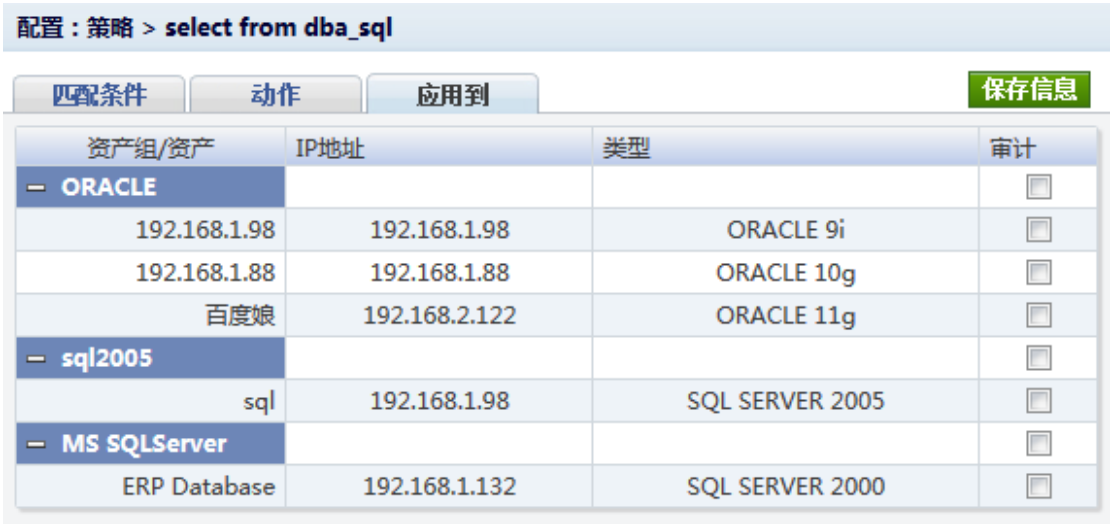
详细的配置步骤在该文档的“3.2.3 策略设置”章节中。

【策略】用于制定对数据库资产应用策略和产生策略告警记录，并可以产生相关审计记录。其中包括策略分类、策略添加、策略修改、策略告警邮件接收、策略应用等参数。

在【匹配条件】中，有字段项可编辑，该处既可以自定义添加修改，也可以在【对象】菜单下添加、修改、删除等进行操作。

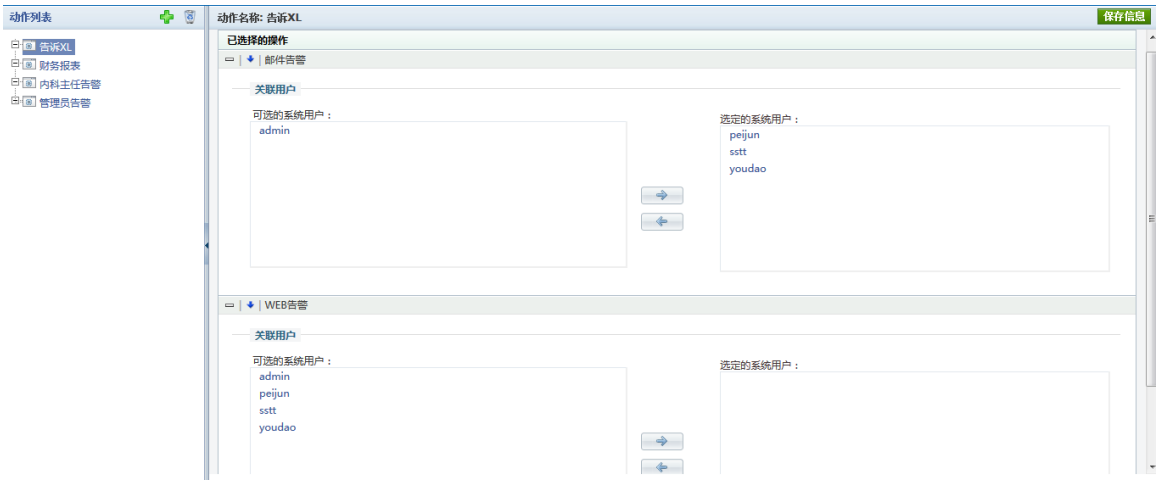
在【动作】中，可以选择要接收策略告警邮件的管理组：

在【应用到】中，可以将策略应用到数据库资产中，便于对资产进行更好的控制。



1.5 动作

【动作】用于对需要接收策略告警的系统用户进行统一管理与配置的，告警接收方式：邮件和 WEB 接收。



1.6 管理

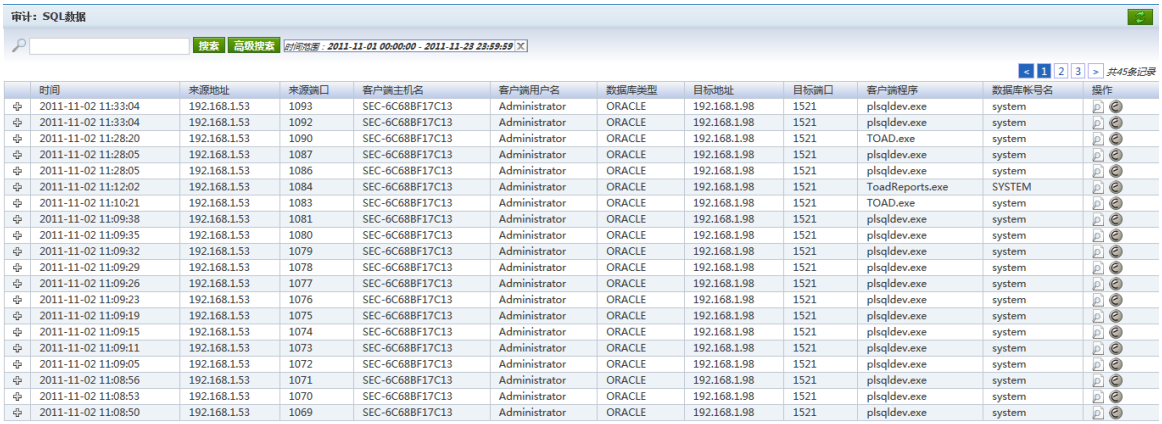
【管理】用于用户编辑好策略后需要在【应用策略】中点击“应用”按钮，告警策略才可生效。

2 日志审计特性

【日志审计】是以数据库服务器资产为审计对象，从而记录访问者对数据库服务器的操作与访问的行为；便对数据库运行情况的实时查看、故障分析以及告警级别的确定。其中包括：会话审计、策略告警、异常告警与系统事件。

2.1 会话审计

【会话审计】用于显示系统审计用户访问操作数据库的行为记录的显示。

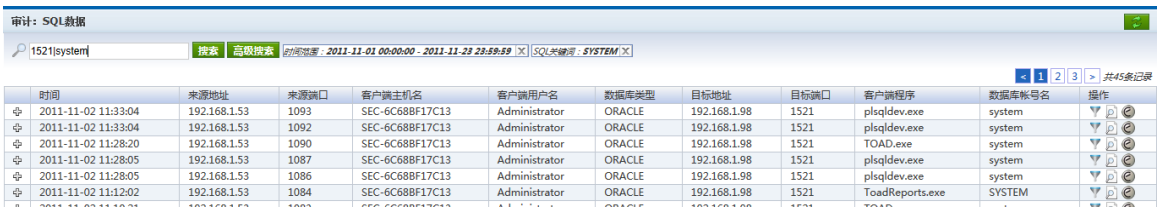


时间	来源地址	来源端口	客户端主机名	客户端用户名	数据库类型	目标地址	目标端口	客户端程序	数据库帐号名	操作
2011-11-02 11:33:04	192.168.1.53	1093	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:33:04	192.168.1.53	1092	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:28:20	192.168.1.53	1090	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	TOAD.exe	system	
2011-11-02 11:28:05	192.168.1.53	1087	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:28:05	192.168.1.53	1086	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:12:02	192.168.1.53	1084	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	ToadReports.exe	SYSTEM	
2011-11-02 11:10:21	192.168.1.53	1083	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	TOAD.exe	system	
2011-11-02 11:09:38	192.168.1.53	1081	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:35	192.168.1.53	1080	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:32	192.168.1.53	1079	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:29	192.168.1.53	1078	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:26	192.168.1.53	1077	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:23	192.168.1.53	1076	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:19	192.168.1.53	1075	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:15	192.168.1.53	1074	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:11	192.168.1.53	1073	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:09:05	192.168.1.53	1072	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:08:56	192.168.1.53	1071	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:08:53	192.168.1.53	1070	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	
2011-11-02 11:08:50	192.168.1.53	1069	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	

【高级搜索】提供全文检索功能，可以做到对海量的数据记录进行更加快速、方便的查询与定位。

“精确搜索”中可对时间、IP、端口、客户端程序、数据库账号、数据库类型、消息长度（SQL 语句长度）、SQL 语句关键词等详细检索条件。

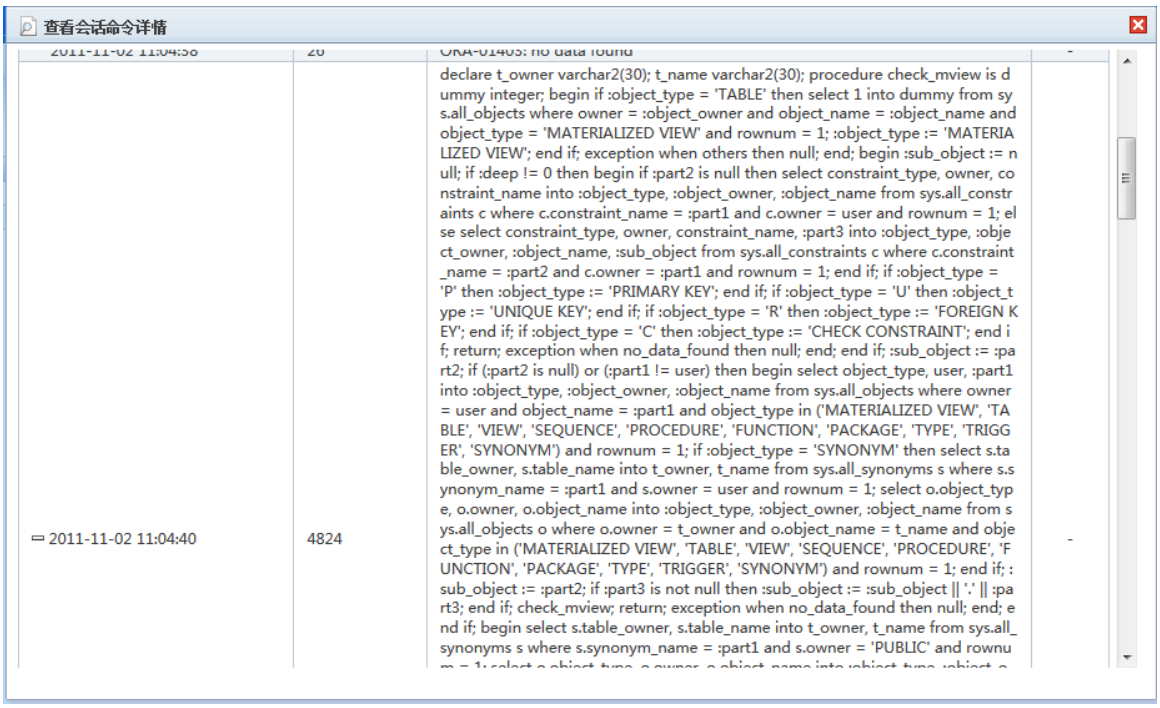
【搜索】提供快捷的搜索定位功能，可在输入框中输入单个关键词或组合关键词进行搜索，例如：输入“1521|system”组合搜索。



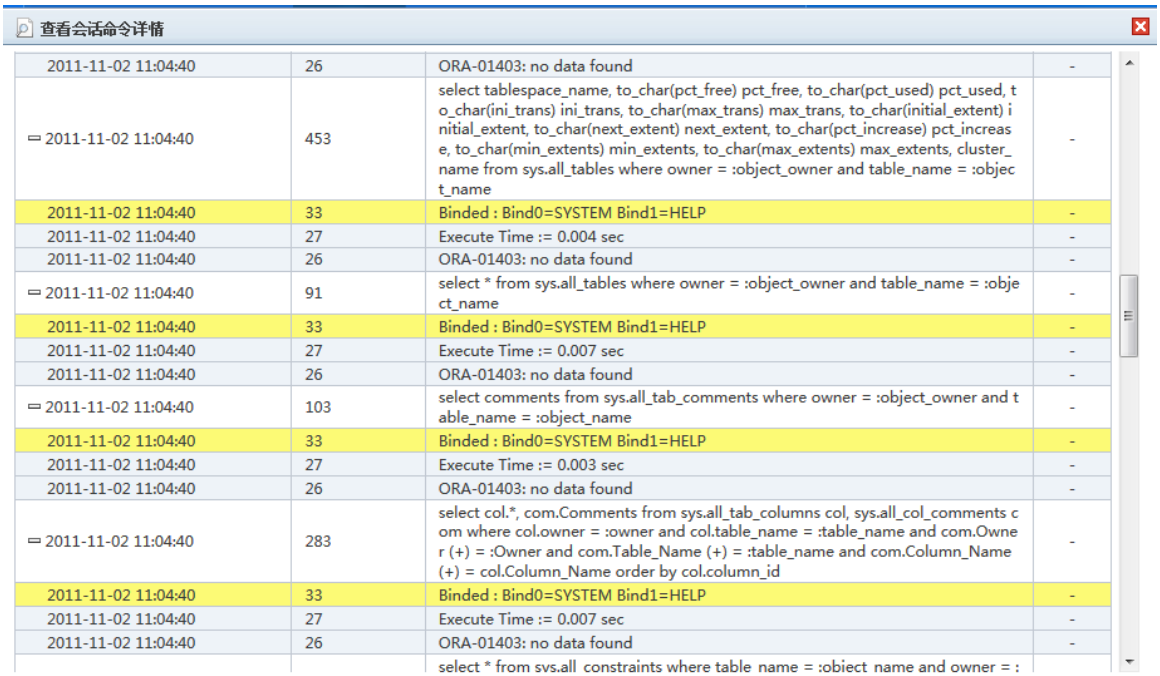
【操作】中提供“检索结果”、“SESSION 详情”和“原始 RAW PACKET 数据包”（PCAP 包）的下载。

【操作】中点击“ ”按钮，会出现“查看会话命令详情”页面框，此处深度解码数据库流，完整、细粒度分析并再现用户数据库操作活动会话过程。完整记录用户数据库会话细节，包括用户数据库登录行为、登出行为、SQL 操作用户名称、SQL 操作源程序名称、SQL 操作源终端名称、SQL 操作源终端登录用户名称、SQL 会话参数设置、SQL 操作语句、SQL 操作返回状态、SQL 操作涉及表组、字段、视图、索引、过程 、函数、SQL DML 操作影响行数、SQL SELECT 操作返回行数、SQL 语句执行时间、SQL 语句返回值解析、超长 SQL 语句、绑定变量值解析等。此功能国内唯一。

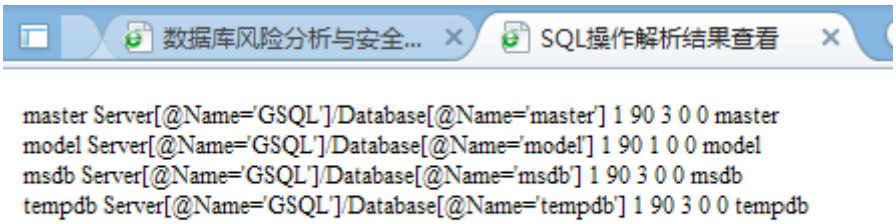
超长 SQL 语句解析：



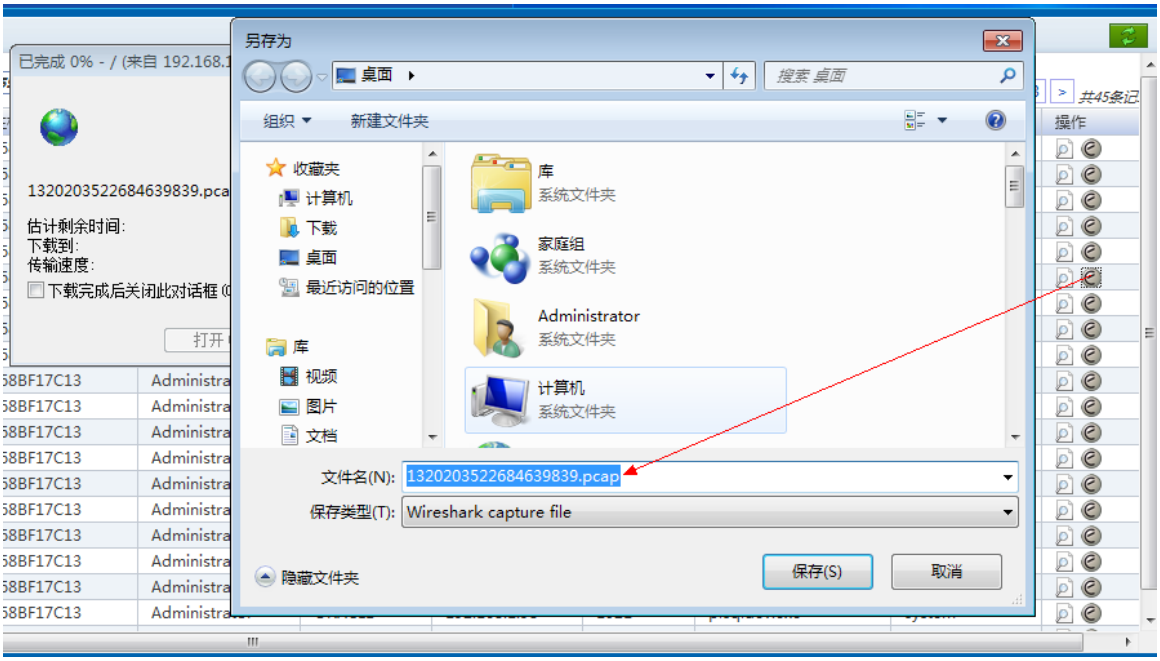
绑定变量值解析：



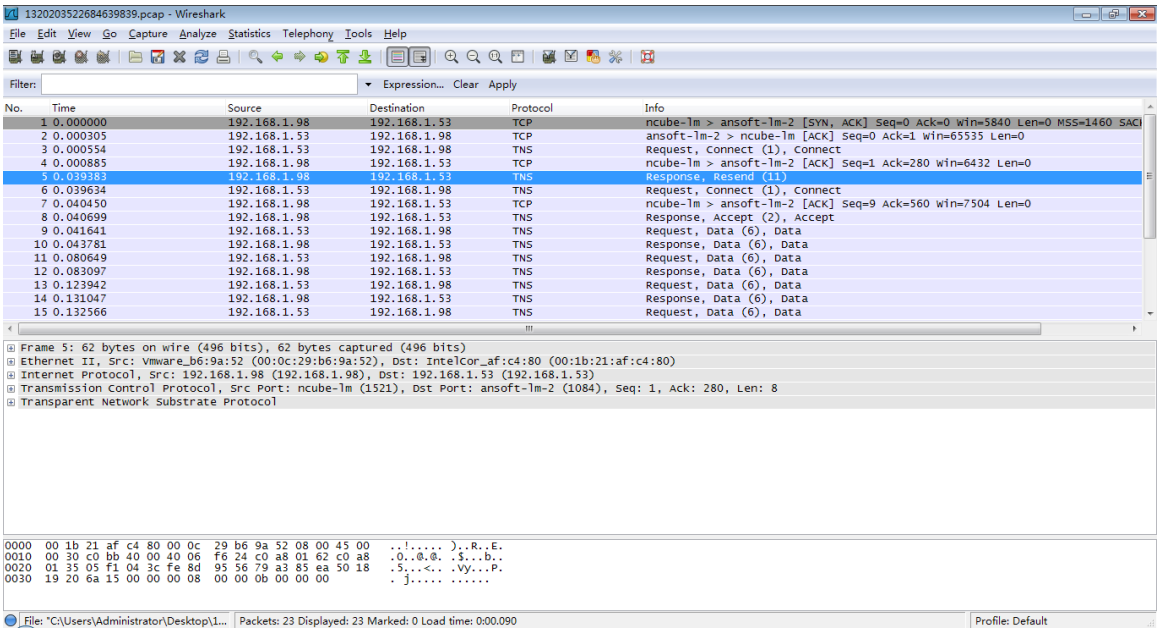
点击“查看会话命令详情”页面中的“ ”按钮，展现 SQL 操作返回值解析：



【操作】中点击“  ”按钮即可下载“原始 RAW PACKET 数据包（PCAP 包)”。“原始 RAW PACKET 数据包”记录整个数据库操作会话过程所有网络数据包。便于用户对原始数据包的分析，对数据的运行状态进行调试查看。



要查看“1320203522684639839.pcap”原始数据，需要在电脑上安装支持 pcap 格式的软件，例如：Wireshark。



2.2 策略告警

【策略告警】是由【策略】定义好的策略要素后，所产生的告警记录。

【策略告警】中包括告警级别、告警时间、数据库类型、IP、数据库账号、策略名称、SQL 语句、语句长度等详细信息。

2.3 异常告警

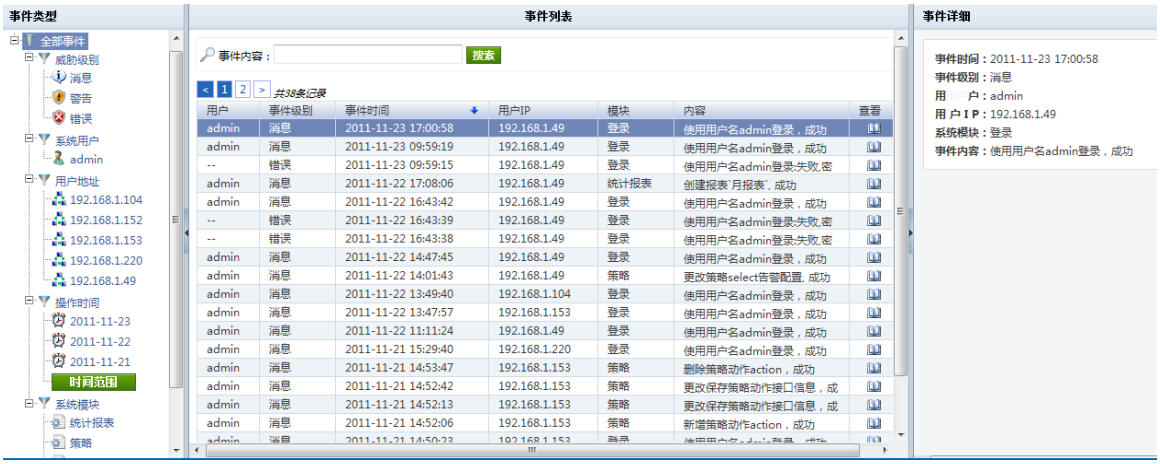
【异常告警】是由【白名单】、【信任账号】和【信任程序】中的设置是否要审计异常告警共同产生的审计记录。不对【白名单】、【信任账号】和【信任程序】进行任何设置，默认是将所有记录作为异常告警。

【异常告警】中包括：告警级别、告警时间、数据库类型、IP、数据库账号、异常描述、SQL 语句、语句长度等详细信息。

2.4 系统事件

【系统事件】记录的是管理员对系统本身的操作行为记录。

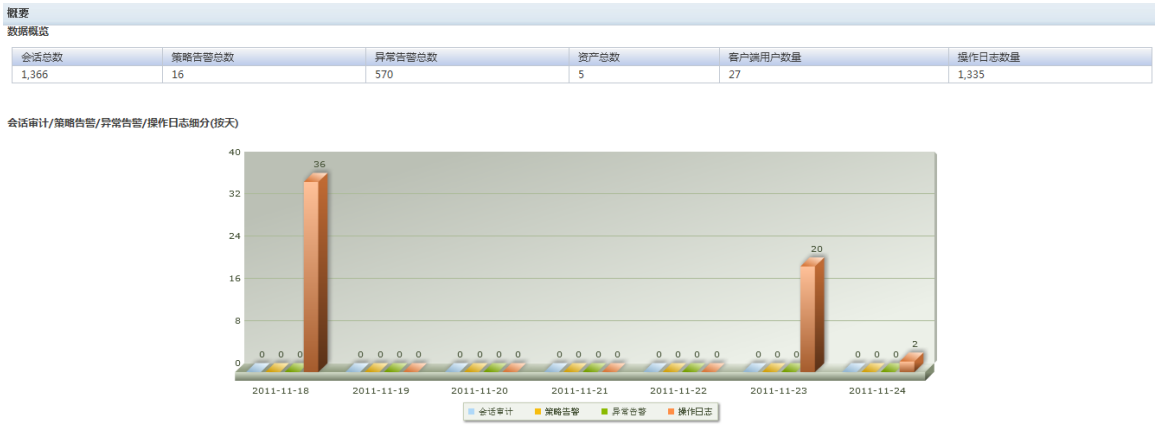
【系统事件】中包括：系统用户、威胁级别、用户 IP、操作时间、系统模块、事件内容等详细信息。



3 统计特性

3.1 概要

【概要】直观的展现会话审计、策略告警、异常告警、操作日志使用量。默认只显示 7 天的数据量。


概要

数据概览

会话总数	策略告警总数	异常告警总数	资产总数	客户端用户数量	操作日志数量
1,366	16	570	5	27	1,335

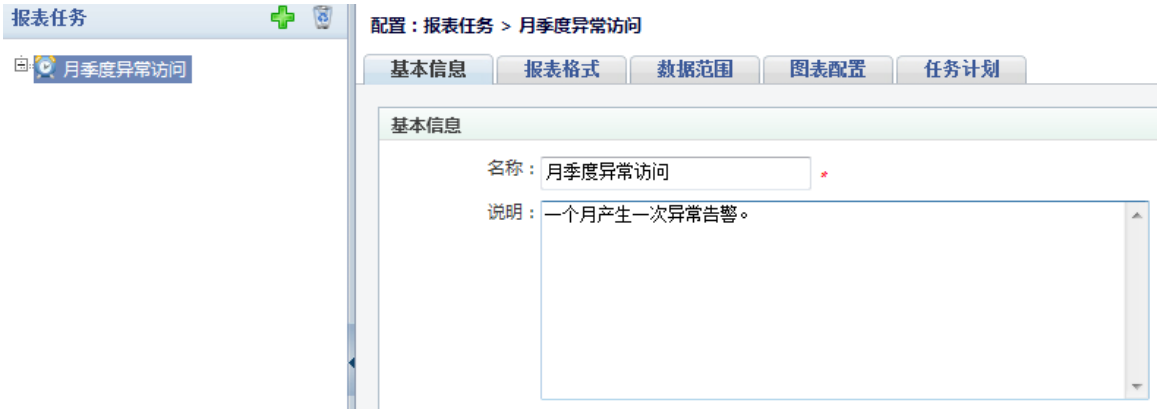
会话审计/策略告警/异常告警/操作日志细分(按天)

天	会话总数	策略告警总数	异常告警总数	客户端用户数量	操作日志数量
2011-11-18	0	0	0	0	36
2011-11-19	0	0	0	0	0
2011-11-20	0	0	0	0	0
2011-11-21	0	0	0	0	0
2011-11-22	0	0	0	0	0
2011-11-23	0	0	0	0	20

3.2 报表任务

【报表任务】用于定制统计报表的功能，可定制参数包括：基本信息、报表格式、数据范围、图表配置、任务计划。

【基本信息】设置报表名称以及名称说明。



【报表格式】设置报表输出格式（支持 PDF 和 CSV）以及标题格式名。

【数据范围】设置报表数据源信息、报表数据展现模式、报表过滤条件。这样可以产生用户所需的报表信息。

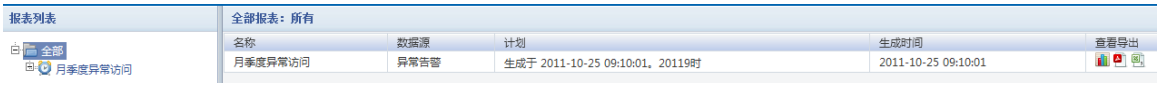
【图表配置】设置报表展现模块：3D 柱状图和 3D 饼状图，满足用户是视觉效果要求。

【任务计划】设置报表任务计划信息：任务周期、任务生成时间、任务报表数据时间。

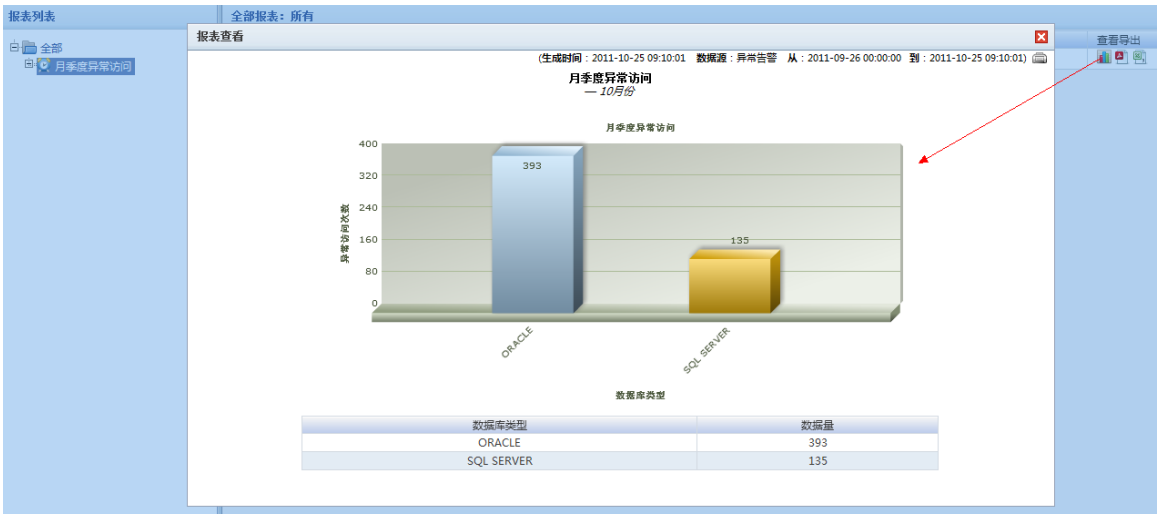
对以上设置参数配置完后，点击“ 全部保存 ”才可生效。

3.3 报表统计

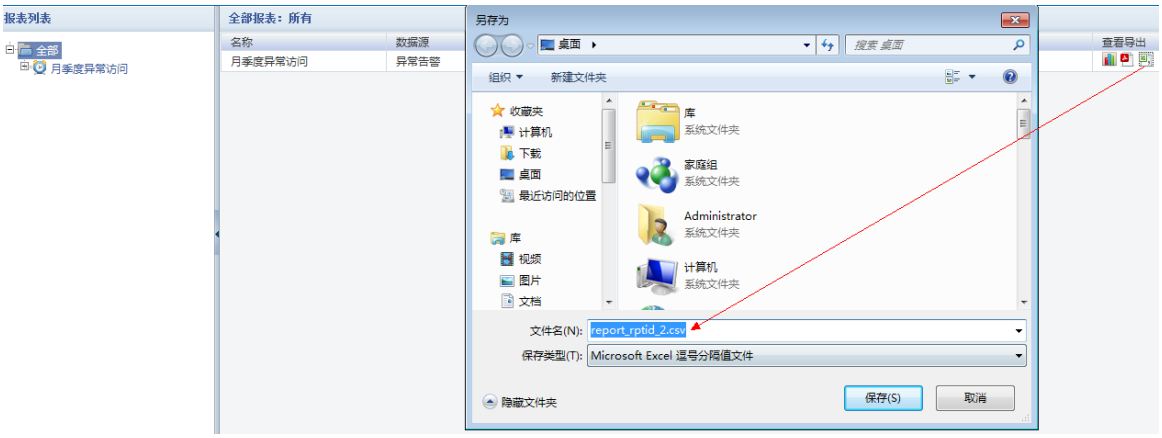
【报表统计】显示的是报表任务定制完后的效果，我们在该页面中可看到报表是否生效以及生效后的展现。



点击“ ”后，可以看到 3D 图状的效果以及报表数据展现：



点击“ ”后，可以看到 CSV 格式文件的下载：


报表列表
全部
月季度异常访问
全部报表：所有
名称
数据源
月季度异常访问
异常告警
另存为
桌面
搜索 桌面
组织
新建文件夹
收藏夹
计算机
下载
桌面
最近访问的位置
库
视频
图片
文档
库
系统文件夹
家庭组
系统文件夹
Administrator
系统文件夹
计算机
系统文件夹
文件名(N):
report_rptid_2.csv
保存类型(T):
Microsoft Excel 逗号分隔值文件
隐藏文件夹
保存(S)
取消
查看导出

4 监控特性

4.1 实时监控

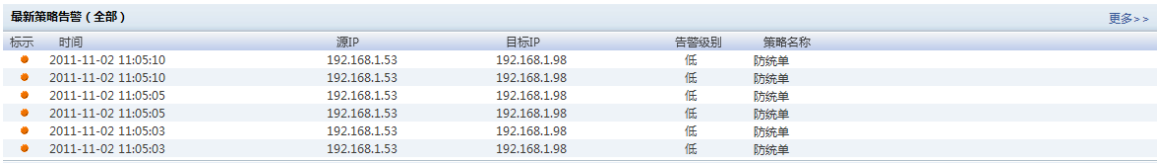
【实时监控】用于展现数据库服务器的运行状况：网络流量、数据包、突发连接、并发连接、SQL 语句、数据库类型、数据库组、单个数据库服务器、实时监控图、柱状图展现。

通过【实时监控】便于数据库管理人员，更加直观、快速的分析数据库服务器的运行状态，以便于对数据库维护做出正确分析与排错。

4.2 系统监测

4.3 最新策略告警

【最新策略告警】提供了实时的策略告警信息。可以通过“更多”进行页面跳转到【日志审计】下的【策略告警】页面。

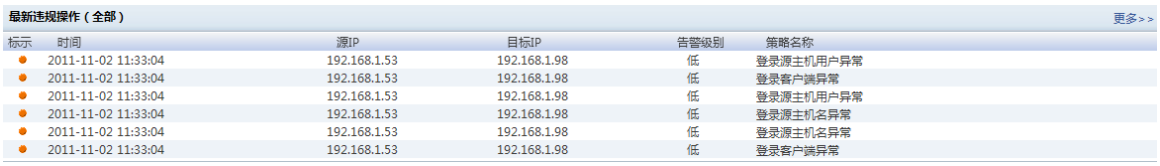


最新策略告警（全部） 更多>>

标示	时间	源IP	目标IP	告警级别	策略名称
	2011-11-02 11:05:10	192.168.1.53	192.168.1.98	低	防统单
	2011-11-02 11:05:10	192.168.1.53	192.168.1.98	低	防统单
	2011-11-02 11:05:05	192.168.1.53	192.168.1.98	低	防统单
	2011-11-02 11:05:05	192.168.1.53	192.168.1.98	低	防统单
	2011-11-02 11:05:03	192.168.1.53	192.168.1.98	低	防统单
	2011-11-02 11:05:03	192.168.1.53	192.168.1.98	低	防统单

4.4 最新违规操作

【最新违规操作】提供了实时的异常告警信息，可以通过“更多”进行页面跳转到【日志审计】下的【异常告警】页面。

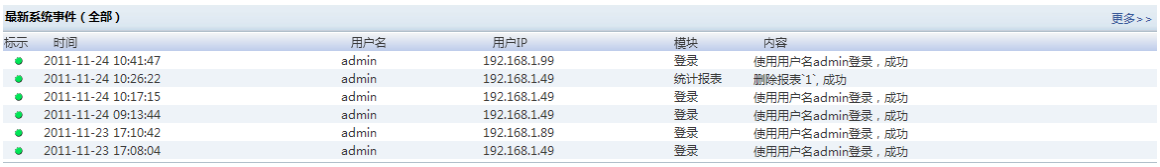


最新违规操作（全部） 更多>>

标示	时间	源IP	目标IP	告警级别	策略名称
	2011-11-02 11:33:04	192.168.1.53	192.168.1.98	低	登录源主机用户异常
	2011-11-02 11:33:04	192.168.1.53	192.168.1.98	低	登录客户端异常
	2011-11-02 11:33:04	192.168.1.53	192.168.1.98	低	登录源主机用户异常
	2011-11-02 11:33:04	192.168.1.53	192.168.1.98	低	登录源主机名异常
	2011-11-02 11:33:04	192.168.1.53	192.168.1.98	低	登录源主机名异常
	2011-11-02 11:33:04	192.168.1.53	192.168.1.98	低	登录客户端异常

4.5 最新系统事件

【最新系统事件】提供了实时的系统本身的异常告警信息，可以通过“更多”进行页面跳转到【日志审计】下的【系统事件】页面。



最新系统事件（全部） 更多>>

标示	时间	用户名	用户IP	模块	内容
	2011-11-24 10:41:47	admin	192.168.1.99	登录	使用用户名admin登录，成功
	2011-11-24 10:26:22	admin	192.168.1.49	统计报表	删除报表`1`，成功
	2011-11-24 10:17:15	admin	192.168.1.49	登录	使用用户名admin登录，成功
	2011-11-24 09:13:44	admin	192.168.1.49	登录	使用用户名admin登录，成功
	2011-11-23 17:10:42	admin	192.168.1.89	登录	使用用户名admin登录，成功
	2011-11-23 17:08:04	admin	192.168.1.49	登录	使用用户名admin登录，成功

4.6 系统硬件运行状态

此处可以查看到系统的 CPU 使用率、内存使用率、接口速率。便于用户查看系统实时运行性能。


CPU使用率
25.44%
内存使用率
7.32%
接口速率
eth0
6.51K, 4.28K
上行
下行