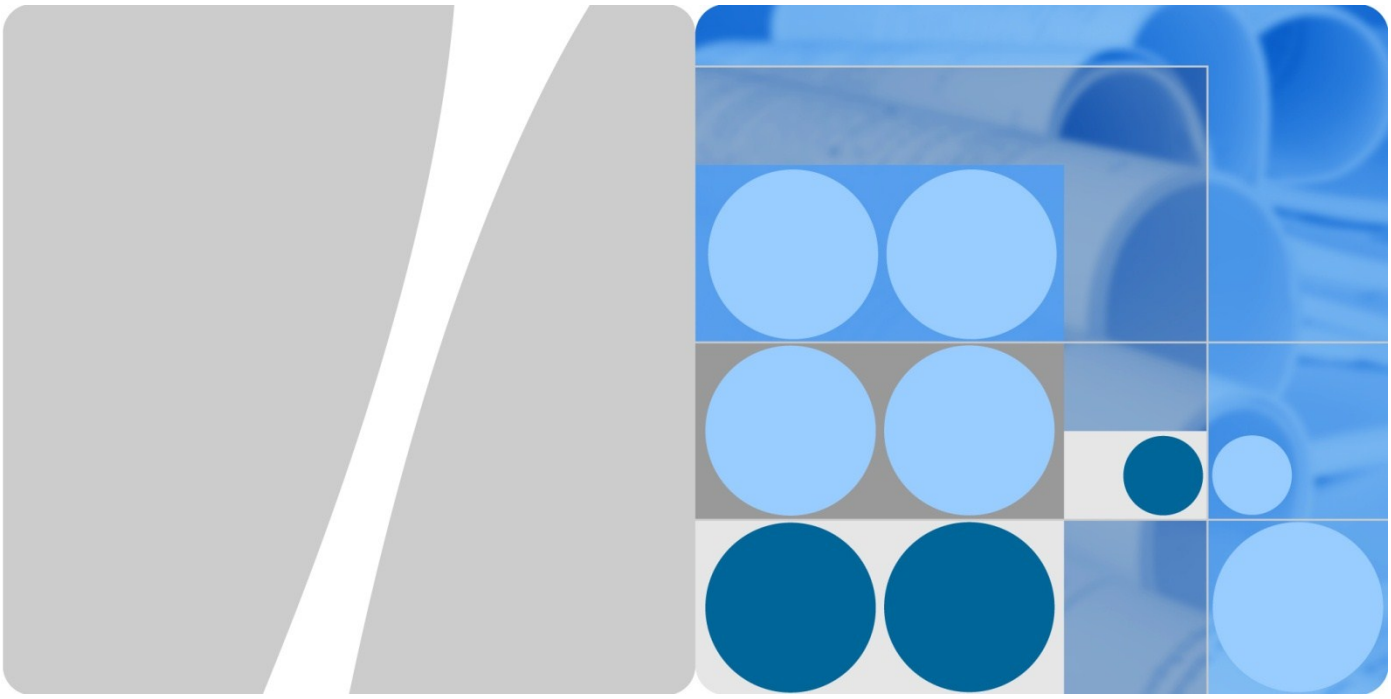


华为 UMA-DB 数据库审计系统技术白皮书

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： 4008302118

目 录

1 概述

1.1 用户现状

随着计算机技术的飞速发展，数据库的应用十分广泛，深入到各个领域，但随之而来产生了数据的安全问题以及数据库访问的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰、成败。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为业界人士探索研究的重要课题之一。

由于计算机和网络的普及和广泛应用，越来越多的关键业务系统运行在数据库平台上。数据库中的数据作为企业的财富发挥着越来越重要的作用，同时也成为不安定因素的主要目标。如何确保数据库自身的安全，已成为现代数据库系统的主要评测指标之一。数据库是信息技术的核心和基础，广泛应用在电信、金融、政府、商业、企业等诸多领域，当我们说现代经济依赖于计算机时，我们真正的意思是说现代经济依赖于数据库系统。数据库中储存着诸如银行账户、医疗保险、电话记录、生产或交易明细、产品资料等极其重要和敏感的信息。尽管这些系统的数据完整性和安全性是相当重要的，但对数据库采取的安全检查措施的级别还比不上操作系统和网络的安全检查措施的级别。许多因素都可能破坏数据的完整性并导致非法访问，这些因素包括复杂程度、密码安全性较差、误配置、未被察觉的系统后门以及数据库安全策略的缺失等。

不完善的数据库安全保障设施不仅会危及数据库的安全，还会影响到数据库的操作系统和其它信用系统。还有一个不很明显的原因说明了保证数据库安全的重要性－数据库系统自身可能会提供危及整个网络体系的机制。例如，某个公司可能会用数据库数据库保存所有的技术手册、文档和白皮书的库存清单。数据库里的这些信息并不是特别重要的，所以它的安全优先级别不高。即使运行在安全状况良好的操作系统中，入侵者也可通过“扩展入驻程序”等强有力的内置数据库特征，利用对数据库的访问，获取对本地操作系统的访问权限。这些程序可以发出管理员级的命令，访问基本的操作系统及其全部的资源。如果这个特定的数据库系统与其它数据库有信用关系，那么入侵者就会危及整个网络域的安全。

由此可见，数据库安全实际上是信息系统信息安全的核心，在这种情况下，有必要采用专业的新型数据库安全产品，专门对信息系统的数据库进行保护。

1.2 产品概述

面对以上种种的安全隐患和市场需求，华为公司推出了新型的审计系统，用以解决数据库安全问题。

华为统一数据库审计系统是华为公司自行研制开发的新一代数据库安全审计系统。数据库审计系统通过旁路侦听的方式对访问数据库的数据流进行采集、分析和识别。实时监视数据库的运行状态，记录多种访问数据库行为，发现对数据库的异常访问，并对访问数据库的相关行为、发送和接收的相关内容进行存储、分析、排名和查询。

随着数据库的使用越来越普及，给我们带来许多方便的同时，也给数据库也带来了许多风险和挑战，例如：非法访问数据库、利用合法访问数据库身份对数据库进行非法操作、正常访问数据库对数据库进行误操作、上传下载数据、泄露公司敏感和机密信息。这些威胁和挑战事件多数是来自于内部合法访问者的“合法”操作，仅靠某些安全产品如防火墙等的日志和控制功能并不能很好的满足对这些网络安全事件（特别是基于应用程序）的行为审计要求，数据库审计系统正是在这样的需求下产生的。华为凭借在安全审计领域多年的技术积累和研发经验，推出的适用于多种网络环境的新一代数据库安全审计系统。它通过专门细致的网络数据获取协议分析技术、数据存储技术、数据查询技术并配合完善的管理规则，帮助访问者应对来自网络中的风险和挑战。

1.3 功能简介

作为数据库审计系统主要用于网络中对数据库的访问行为、内容进行审计、报警、过滤和分析，多种数据库的访问，如：oracle、informix、DB2、SQL server、sybase等。数据库审计系统部署于网络到数据库的核心交换机连接处。

2 系统架构

2.1 系统功能组成

数据库审计系统主要由以下3个部分组成：

① 数据库审计侦听收集引擎；

② 数据库审计数据存储中心；

③ 数据库审计控制管理中心；

数据库审计系统侦听收集引擎、数据库审计系统数据存储中心、数据库审计系统控制管理中心在物理

上部署在同一台专用服务器上。

数据库审计系统侦听收集引擎全面监听网络连接到数据库的数据流，根据配置的策略，实时监视所有数据包进行分析记录，并将审计结果保存在数据库审计系统数据存储中心的相应数据库里；同时数据库审计系统侦听收集引擎接收并执行数据库审计系统控制管理中心的各种策略。

数据库审计系统数据存储中心主要用于各种数据保存，并提供各种数据查询。

数据库审计系统控制管理中心主要用于提供审计、管理等策略设置接口，如配置数据库服务器管理；程序升级等接口；数据库审计系统控制管理中心采用B/S架构，通过提供浏览器服务端，使管理人员很方便的通过网页浏览器对数据库审计系统控制管理中心进行操作管理。

2.2 系统部署

面对某用户的网络结构图（如图1），我们采用的是将数据库审计系统部署在内网的核心交换机上。

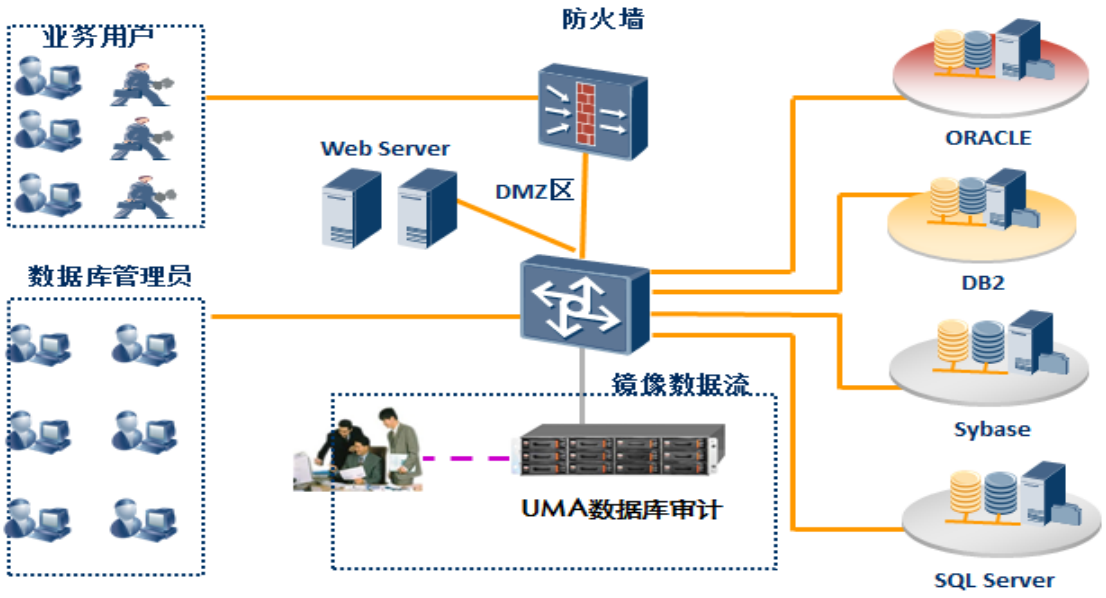


图1：某用户的网络拓扑图

项目中在内网中核心交换机采用了负载均衡的方式对接，这样的话，数据流就会随意走2台核心交换机，我们只需在2台核心交换机上各配置一个镜像端口，连接到数据库审计系统即可。

3 产品功能

3.1 功能介绍

审计对象：数据库审计系统所指的审计对象是指数据库审计系统逻辑上能够审计的数据库服务器；数据库审计系统可以采用多级部署方式管理审计对象；并且在数据库审计系统内部可以按照多种方式来表示审计对象：如客户端的登录IP、登录用户名、登录主机名、登录程序、来源端口等；服务端的数据库类型、数据库端口、数据库账号；会话详情的SQL语句、消息长度、数据库服务器返回信息、绑定变量解析等。数据库审计系统的主要功能包括：系统管理、策略管理、日志审计、统计报表、实时监控和系统监测。

- 系统管理是对数据库审计系统本身的配置，以便对系统的访问、授权与管理等功能。其中包括：接口配置、用户管理、输出配置与授权许可。
- 策略管理是对目标数据库服务器资产的添加、授权、策略制定、告警设置等配置功能。其中包括：资产、白名单、对象、策略、动作与管理。
- 日志审计是以数据库服务器资产为审计对象，从而记录运维人员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。
- 实时监控提供数据库实时监控功能，可以对总体或数据库类型或数据库组别进行实时监控，监控其网络流量、数据包、突发链接、并发连接数、SQL语句数。并提供波形图展示，用户能够直观地了解当前数据库运行状态。
- 系统监测是用户通过数据库审计系统的审计数据信息的显示；以便用户全面的、统一的、及时的对数据库服务器的运行情况进行分析与排错。其中包括：最新策略告警、最新违规操作、最新系统事件。

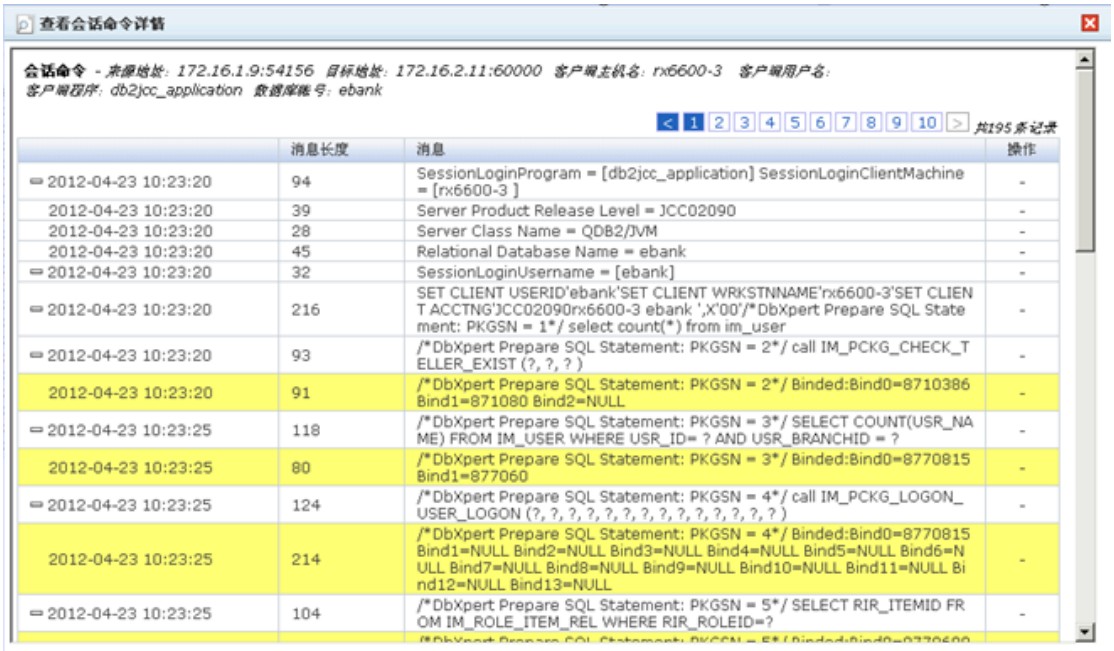
3.2 功能特点

3.2.1 流技术与完整会话审计

数据库审计系统采用现今最先进的网络数据审计技术——流技术，保存“流生命期”内“上下文”相关环境，进行分析解码。数据库审计系统根据流ID进行相关记录，每个会话数据流具备一个64位长的唯一ID。流与流之间，保证高度唯一性。

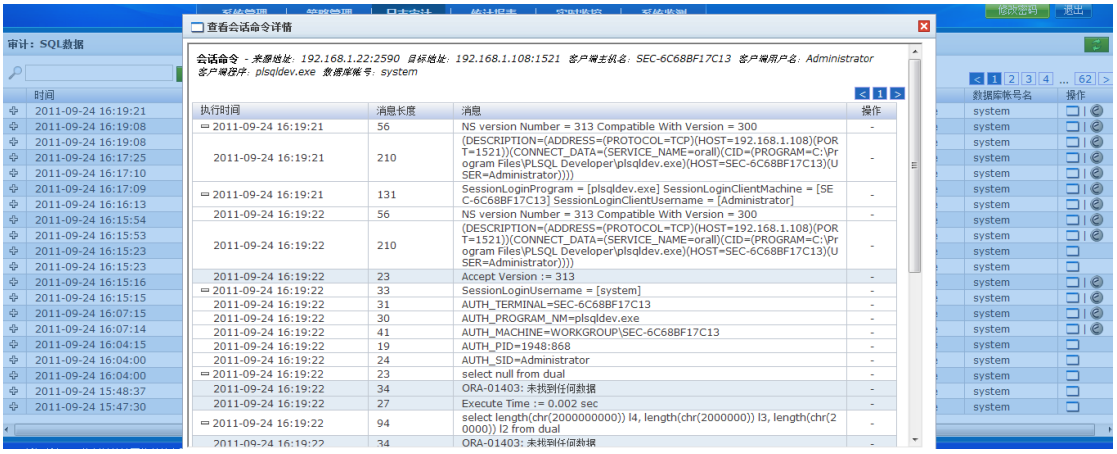
时间	来源地址	来源端口	客户端主机名	客户端用户名	数据库类型	目标地址	目标端口	客户端程序	数据库帐号名	操作
2011-09-24 16:19:21	192.168.1.22	2590	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:19:08	192.168.1.22	2588	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:19:08	192.168.1.22	2587	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:17:25	192.168.1.22	2585	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:17:10	192.168.1.22	2583	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:17:09	192.168.1.22	2582	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:16:13	192.168.1.22	2580	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:54	192.168.1.22	2578	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:53	192.168.1.22	2577	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:23	192.168.1.22	2574	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	
2011-09-24 16:15:23	192.168.1.22	2573	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	
2011-09-24 16:15:16	192.168.1.22	2570	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:15	192.168.1.22	2569	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:07:15	192.168.1.22	2566	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:07:14	192.168.1.22	2565	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:04:15	192.168.1.22	2563	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	
2011-09-24 16:04:00	192.168.1.22	2561	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	
2011-09-24 16:04:00	192.168.1.22	2560	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	
2011-09-24 15:48:37	192.168.1.22	2558	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 15:47:30	192.168.1.22	2556	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	

深度解码数据库网络数据流传输协议，完整、细粒度分析并再现用户数据库操作活动会话过程。会话审计内容从访问的发起、连接、到结束进行完整记录。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语句执行时间、原始数据库记录包等。



	消息长度	消息	操作
2012-04-23 10:23:20	94	SessionLoginProgram = [db2jcc_application] SessionLoginClientMachine = [rx6600-3]	-
2012-04-23 10:23:20	39	Server Product Release Level = JCC02090	-
2012-04-23 10:23:20	28	Server Class Name = QDB2/JVM	-
2012-04-23 10:23:20	45	Relational Database Name = ebank	-
2012-04-23 10:23:20	32	SessionLoginUsername = [ebank]	-
2012-04-23 10:23:20	216	SET CLIENT USERID'ebank'SET CLIENT WRKSTNNAME'rx6600-3'SET CLIENT ACCTNG'JCC02090rx6600-3 ebank ',X'00'/*DbXpert Prepare SQL Statement: PKGSN = 1*/ select count(*) from im_user	-
2012-04-23 10:23:20	93	/*DbXpert Prepare SQL Statement: PKGSN = 2*/ call IM_PCKG_CHECK_TELLER_EXIST (?, ?, ?)	-
2012-04-23 10:23:20	91	/*DbXpert Prepare SQL Statement: PKGSN = 2*/ Binded:Bind0=8710386 Bind1=871080 Bind2=NULL	-
2012-04-23 10:23:25	118	/*DbXpert Prepare SQL Statement: PKGSN = 3*/ SELECT COUNT(USR_NAME) FROM IM_USER WHERE USR_ID= ? AND USR_BRANCHID = ?	-
2012-04-23 10:23:25	80	/*DbXpert Prepare SQL Statement: PKGSN = 3*/ Binded:Bind0=8770815 Bind1=877060	-
2012-04-23 10:23:25	124	/*DbXpert Prepare SQL Statement: PKGSN = 4*/ call IM_PCKG_LOGON_USER_LOGON (?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?)	-
2012-04-23 10:23:25	214	/*DbXpert Prepare SQL Statement: PKGSN = 4*/ Binded:Bind0=8770815 Bind1=NULL Bind2=NULL Bind3=NULL Bind4=NULL Bind5=NULL Bind6=NULL Bind7=NULL Bind8=NULL Bind9=NULL Bind10=NULL Bind11=NULL Bind12=NULL Bind13=NULL	-
2012-04-23 10:23:25	104	/*DbXpert Prepare SQL Statement: PKGSN = 5*/ SELECT RIR_ITEMID FROM IM_ROLE_ITEM_REL WHERE RIR_ROLEID=?	-

完整解析、记录、关联SQL操作语句参数，可自动回溯重构完整SQL操作语句。



3.2.2 “细粒度”数据库审计

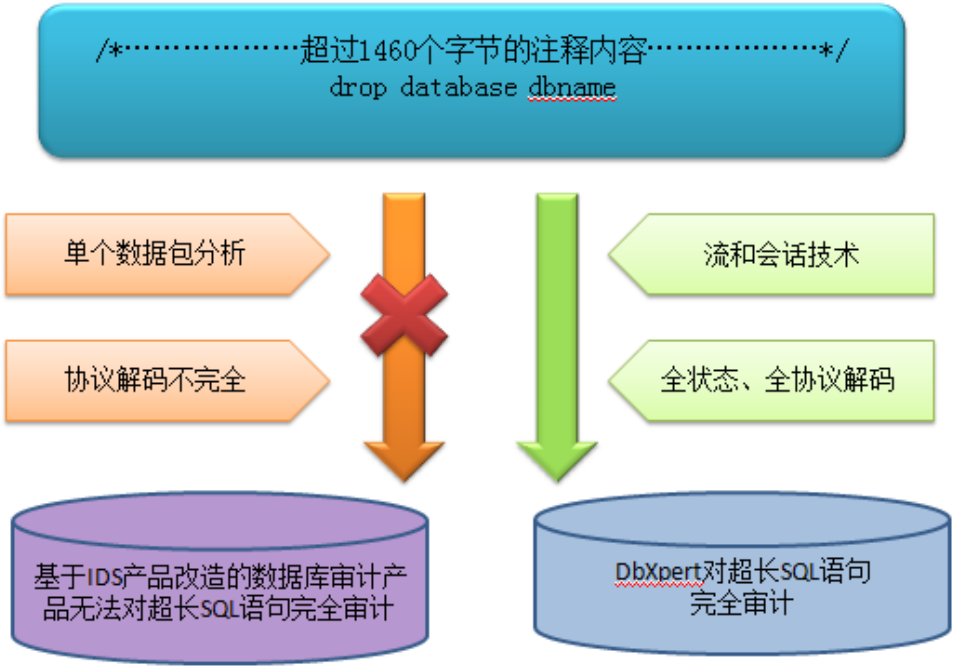
提供灵活的数据库访问行为来源限制，可选择忽略审计特定网络和主机产生的数据库SQL操作；亦可限制仅对特定“嫌疑”对象进行细粒度、全方位审计，包括记录整个数据库操作会话过程所有网络数据包。

覆盖主流商用数据库，包括：Oracle 8/9/10/11等、Sybase所有版本、SQL Server 2000/2005、Informix所有版本、DB2所有版本。

3.2.3 超长 SQL 语句审计

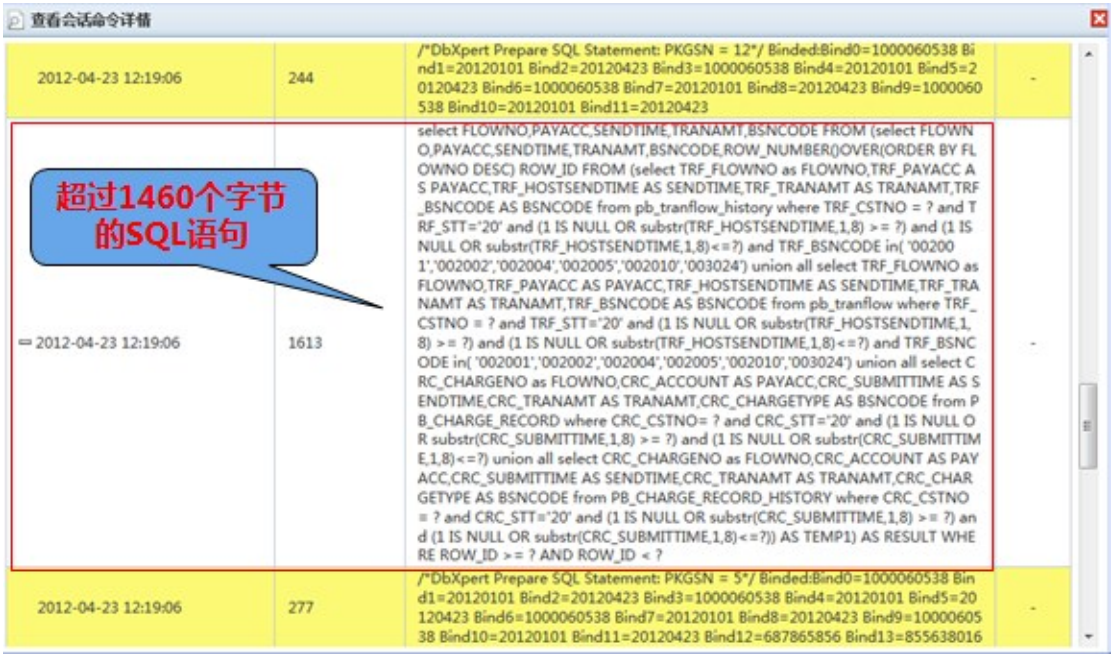
在以太网传输中，链路层所能承受的最大数据长度(MTU)为1500字节，除去IP/TCP头长度最大报文段长度有1460字节。若总长度大于1500字节，数据包将会被分片。所以我们把超过1460个字节的SQL语句称之为超长SQL语句。

目前国内数据库审计产品多数是基于IDS产品改造而成，只能对单个网络数据包进行分析，加之协议解码的不完全，使超长SQL语句无法审计，提供了逃避审计的通道，造成了审计数据的不完整。实际应用中由于SQL语句的长度无限制，使长SQL语句的使用非常普遍，形成了业务操作审计信息的缺失；同时，利用超长SQL语句特点以及SQL语句可注释功能，恶意攻击者可以构建出针对“初级简单数据库协议审计”的“逃避审计办法”，达成非法操作的目的。



数据库审计系统是基于流和会话技术，进行全状态、全协议解码，能完整的、细粒度的解析超长SQL语句。通过对超长SQL语句的完全审计，监控了恶意攻击者妄想通过逃避审计对数据库造成非法操作的途径，为安全事件的追溯提供了强有力的证据；同时也为实际业务中SQL语句的全面审计提供了保障。

超长SQL语句审计记录：



3.2.4 绑定变量解析技术

SQL语句允许通过符号占位，然后再通过对占位符号赋值的方式，完成SQL语句操作请求。绑定变量是替代SQL语句中的常量的替代变量。目前五大商用数据库管理工具与服务端之间数据库的查询大量使用变量绑定来完成，任何标准数据库管理工具，都会使用变量绑定对数据库进行管理。

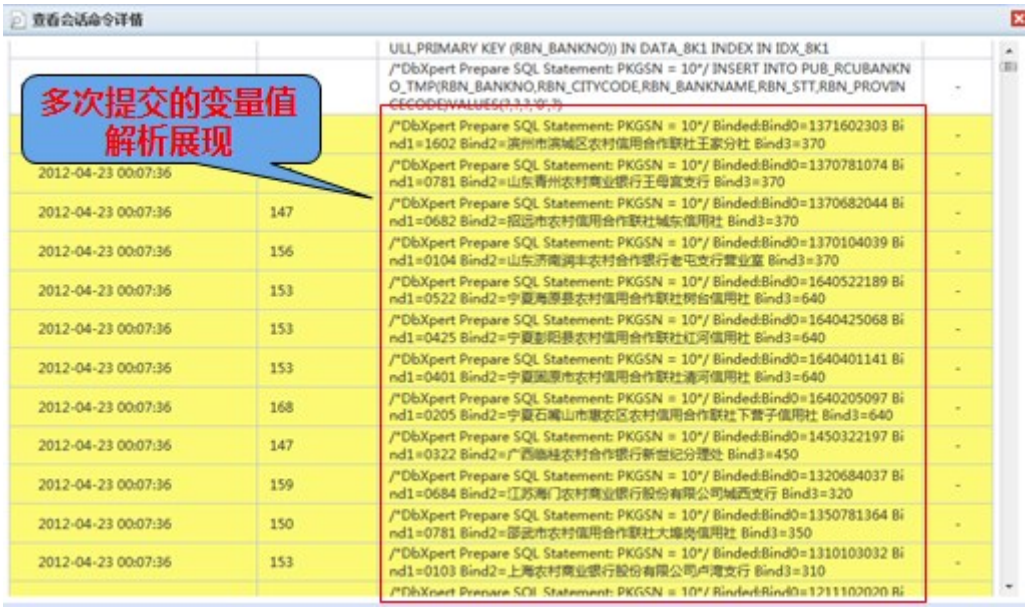
在使用变量绑定的数据库操作环境内，SQL语句仅仅是数据库操作动作，数据库操作涉及到的库和表，数据库数据操作关系等模态化硬解析固件，涉及到的数据库数据并不包含在SQL语句内。在现实业务活动过程中，数据库数据才同具体的财务和现实生活个体信息相关，而数据可能包含在变量绑定内。因此，变量绑定审计，成为数据库审计分析产品的必备和必需功能。只有实现变量绑定的数据库审计分析产品，才能定位SQL语句的操作客体，有能力解决中间件审计问题，具备真实可靠的有用性。

目前其他的旁路数据库审计厂商主要通过三层审计关联来解决中间件审计问题，这其实是一个误区。由于中间件应用没有一个统一的标准，因此要自动识别各种中间件的应用比较难，目前的做法大部分是通过对前端浏览器与WEB服务器之间的HTTP通讯协议进行分析，根据对URL、时间片及一些关键信息进行分析，然后再与后端的数据库操作进行关联来实现。这类厂商由于连最基本的协议解码和变量绑定都没有实现，数据库协议分析审计部分缺乏关联数据源，所谓关联审计根本不可行。

数据库审计系统是基于流和会话技术，进行全状态、全协议解码，能完整的、细粒度的解析绑定变量。可以精确定位到操作客体，真正审计到数据发生了什么事情。通过变量绑定以及SQL语句的全记录，可以

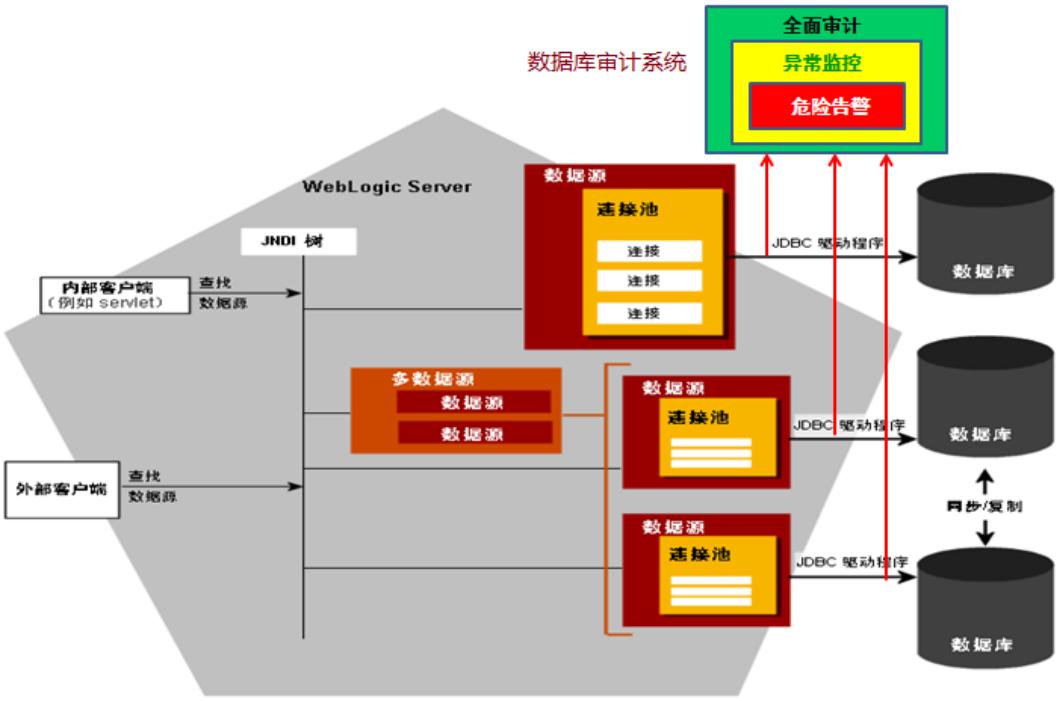
完整的重溯整个业务流程，追溯信息的来龙去脉，成为全球第一家通过变量绑定技术真正解决中间件审计问题的数据库审计厂商，为数据的完整性、有用性和准确性提供了强有力的技术保证和原始证据。

变量绑定审计记录：



目前DB2变量绑定特性：一次SQL语句提交，无限次变量提交，每次提交值都会产生数据变更，数据库审计系统能完整记录并准确关联（不是用流技术的其它同类产品基本无法实现）。

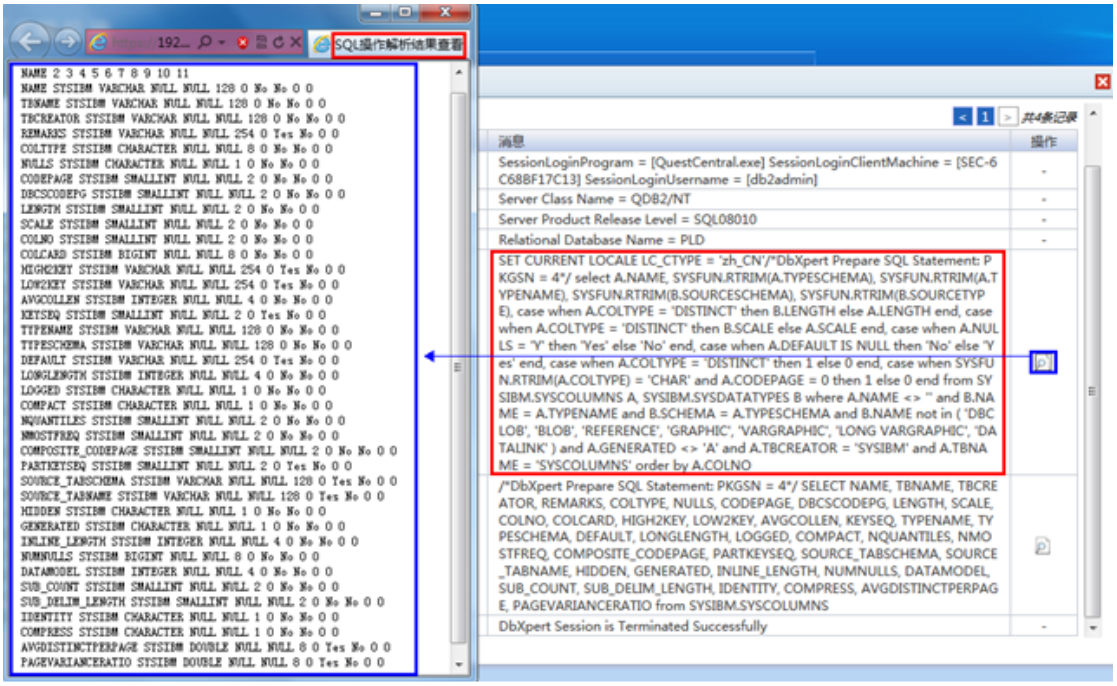
三层应用审计：



- 业务帐号审计
  - 业务账号：业务系统账号、网银帐号、流水帐号、银行卡号、手机号、邮箱帐号等；
  - 业务账号以SQL语句提交或以绑定变量值提交至数据库；
  - 数据库审计系统在完成深度解码的基础上，完整解析数据协议中的业务账号。
- 业务操作审计
  - 业务操作：登录(login)、查询(select)、添加(insert)、删除(delete/drop)、修改(update)、登出(logout)等；
  - 数据库审计系统在完成会话审计与深度解码的基础上，完整解析数据协议中的业务操作动作。

3.2.5 SELECT 返回值解析

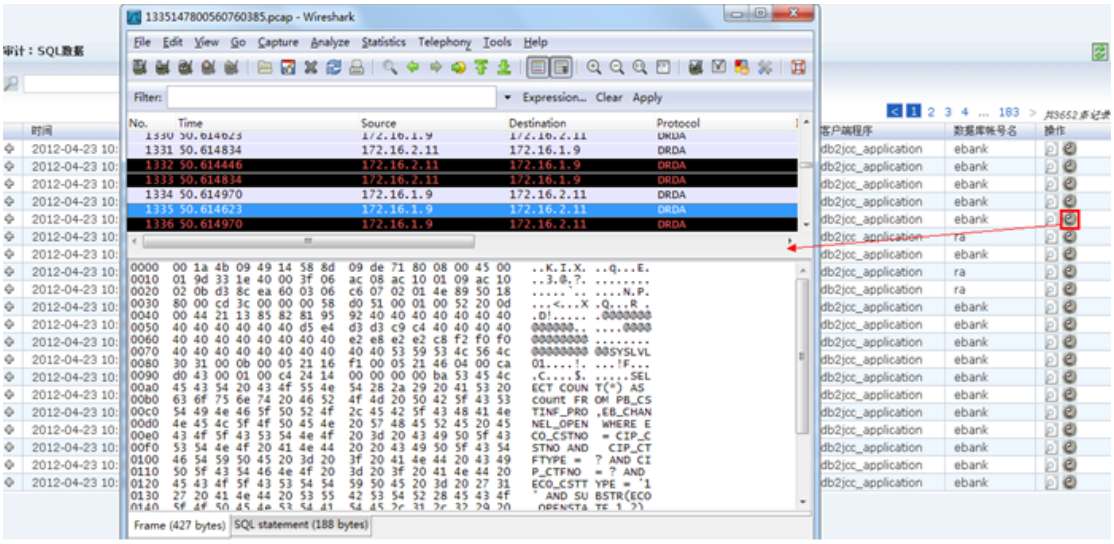
数据库审计系统基于流会话跟踪审计，实现SELECT返回值解析。通过记录访问的回应信息，可以有效的防止数据泄密和窃取，监视和控制被存取的数据。



3.2.6 原始流数据包记录（PCAP）

数据库审计系统不仅完整记录SQL语句，还能完整审计原始数据包，实现超级嗅探器功能。只有原始

数据才能还原真实的数据现场，提供无可抵赖的强有力证据。

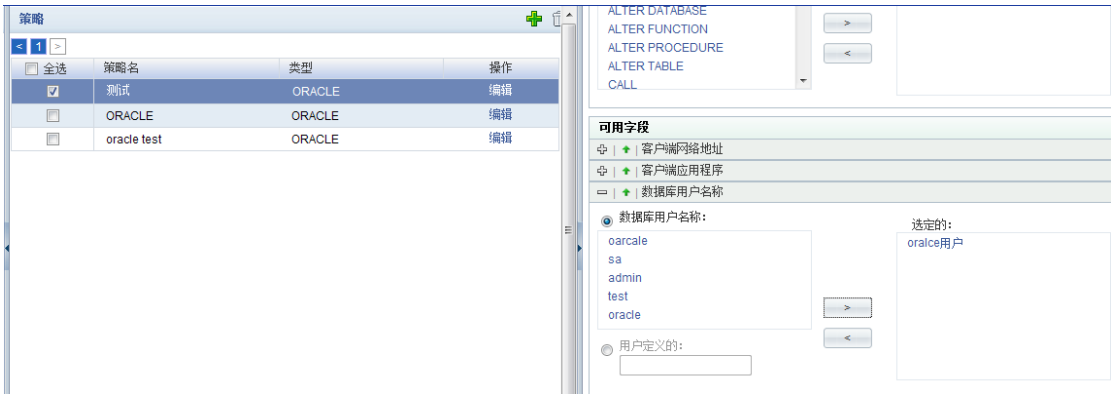


审计记录记录原始数据网络流量包，可下载至本地：

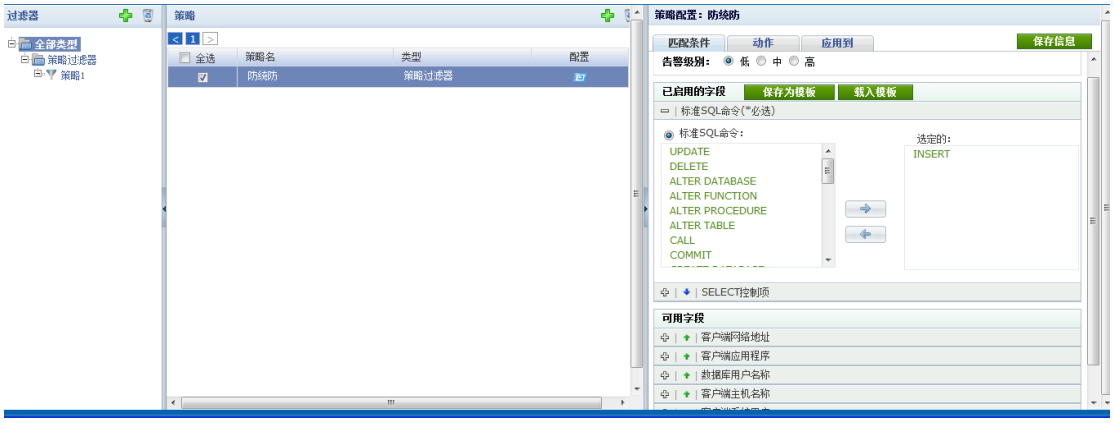
时间	来源地址	来源端口	客户端主机名	客户端用户名	数据库类型	目标地址	目标端口	客户端程序	数据库帐号名	操作
2011-09-24 16:19:21	192.168.1.22	2590	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:19:08	192.168.1.22	2588	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:19:08	192.168.1.22	2587	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:17:25	192.168.1.22	2585	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:17:10	192.168.1.22	2583	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:17:09	192.168.1.22	2582	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:16:13	192.168.1.22	2580	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:54	192.168.1.22	2578	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:53	192.168.1.22	2577	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.108	1521	plsqldev.exe	system	
2011-09-24 16:15:23	192.168.1.22	2574	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	
2011-09-24 16:15:23	192.168.1.22	2573	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.88	1521	plsqldev.exe	system	

3.2.7 灵活的数据库访问策略

提供来源（客户端）登录IP异常探测、数据库登录用户名称异常探测、数据库操作源终端异常探测、数据库操作源程序名称异常探测、数据库操作源终端用户名称异常探测。



提供数据库SQL语句执行时间、数据库操作闲置时间策略报警，提供数据库DML、DDL等操作影响行数策略报警，提供数据库SELECT SQL操作语句返回行数策略报警。

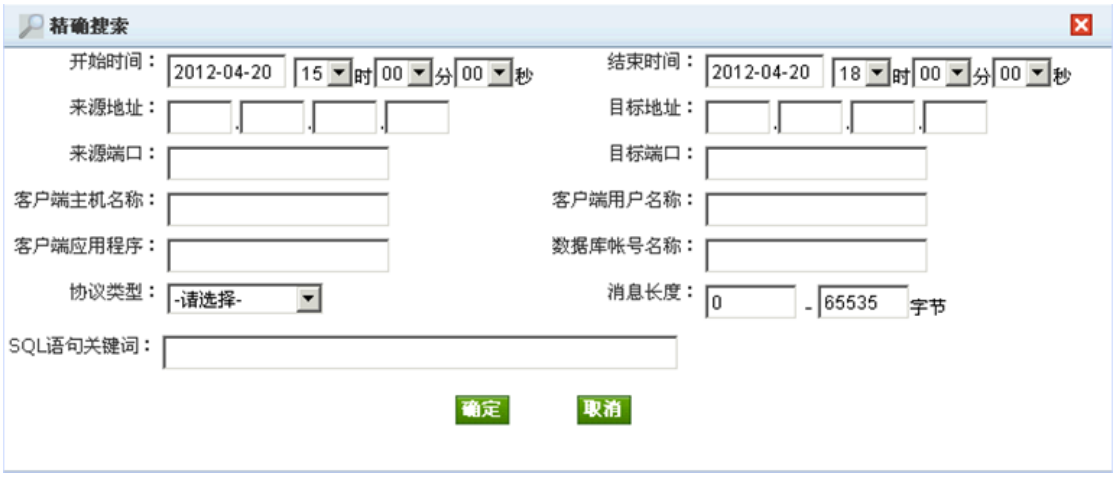


提供全方位的策略规则匹配，策略因子包括：数据库操作来源IP地址、数据库服务器IP/端口、数据库类型、数据库名称、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL操作语句（DDL、DML、DCL）、高级权限操作、存储过程、数据库表组（表、字段、值）、数据库SCHEMA、操作执行时间、操作返回条目大小等。

根据设定的数据库策略，可选择对关键资源操作行为进行数据包录像、深度分析解析开关。

3.2.8 全文检索功能

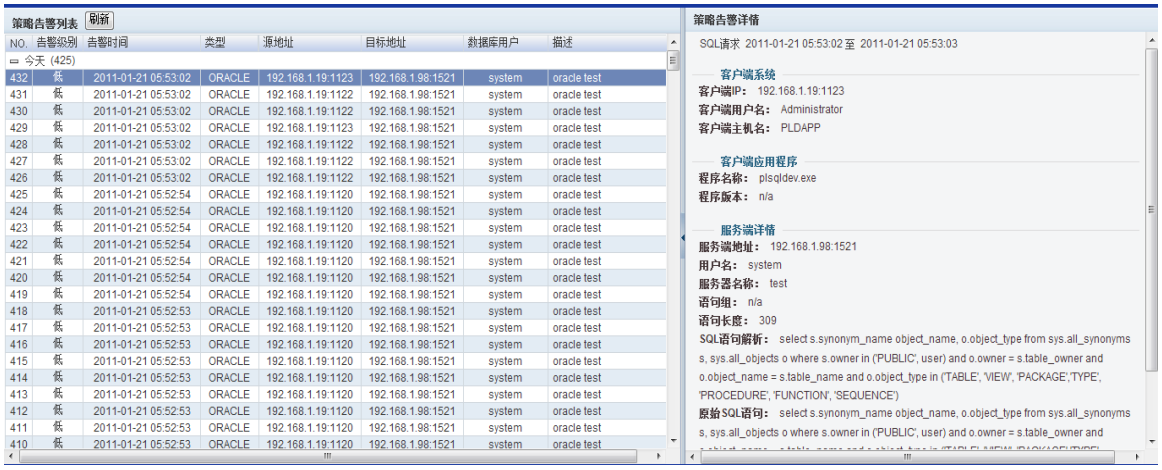
记录数据库会话详细细节，当发生数据库安全事件时，用户可根据数据库地址、源客户端地址、事件时间、SQL语句关键词、数据库账号、数据库地址等，快速检索定位操作会话。



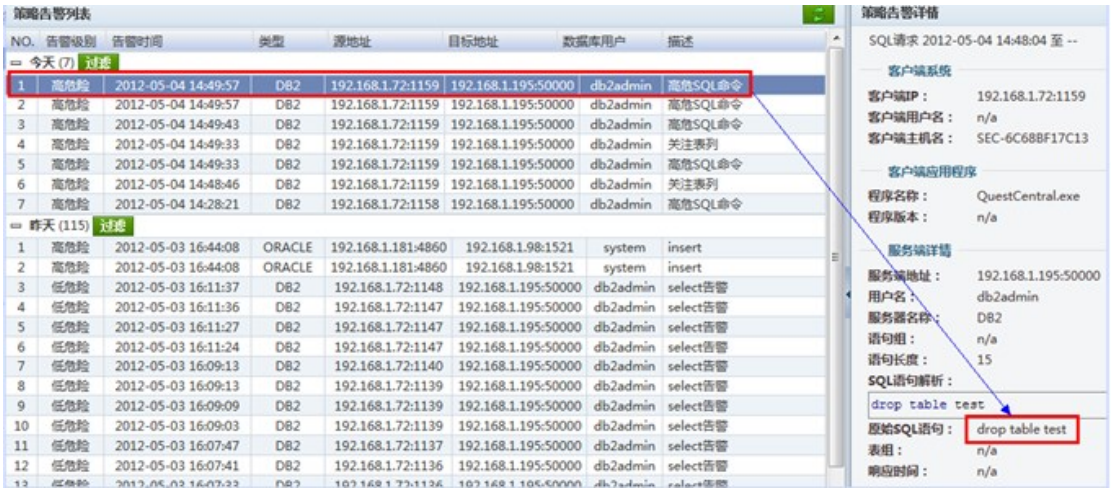
数据库审计系统通过细粒度的过滤条件，在海量数据中快速定位审计日志。检索条件越丰富，查询越快，定位更准。

3.2.9 异常告警、实时监控

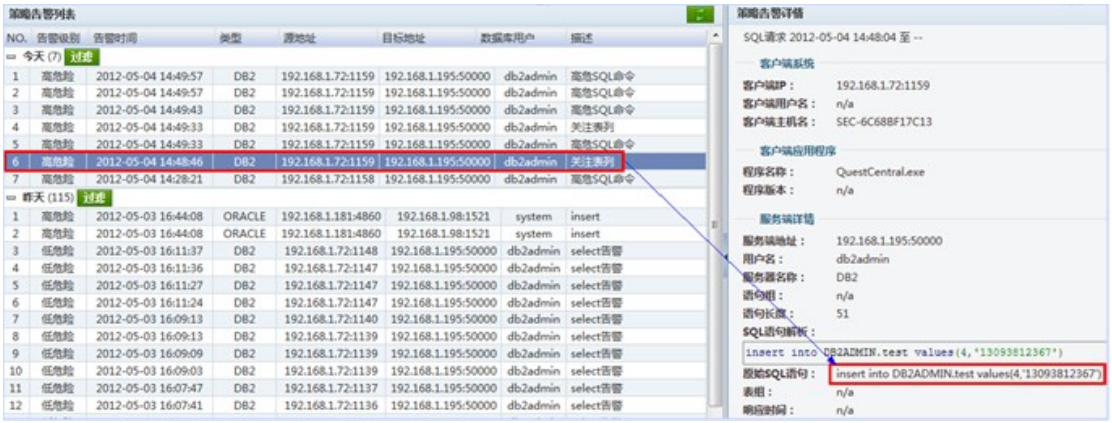
提供完善的违规实时告警，包括异常告警、违反策略告警等。及时发现数据库非法接入、SQL注入、数据泄密等安全事件。



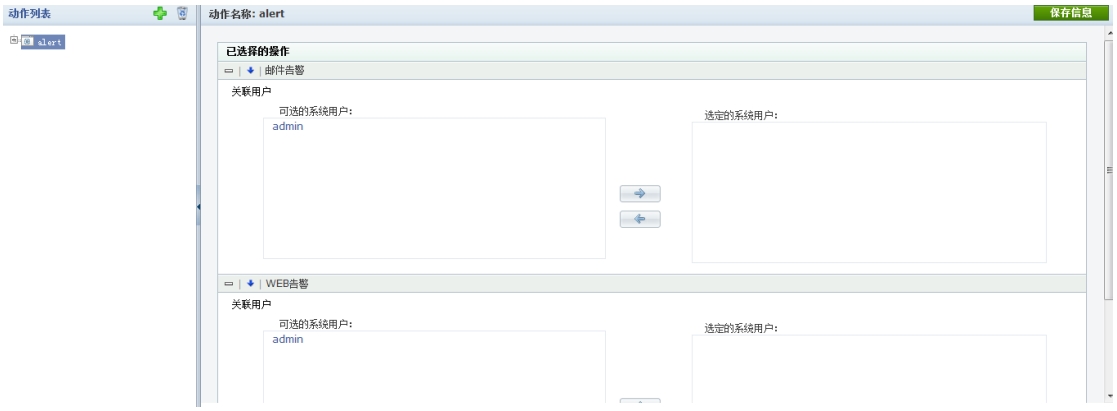
高危SQL命令告警，如对drop、delete等高危SQL命令进行实时告警。



关注表列告警，如对数据库表做过drop或delete动作，进行实时告警。



多形式的实时告警：当检测到可疑操作或违反审计规则的操作时，系统可以通过WEB告警、邮件告警等方式通知数据库管理员。



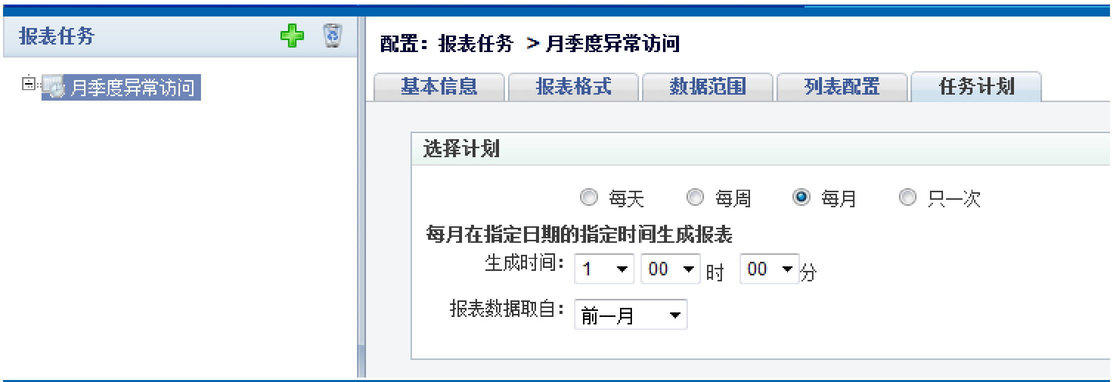
实时监控来自各个层面的所有数据库活动，包括网络流量、数据包、突发连接、并发连接、SQL语句的实时数量，并且提供实时的视图窗口查看数据库的运行状态。它可以帮助DBA更好的管理数据库。

3.2.10 业务跟踪审计

拥有业务跟踪审计的能力，对于整个业务流程的操作以及业务数据的删除、添加或修改进行完全审计。通过审计信息，可以重溯整个业务流程。

3.2.11 灵活的统一报表

可灵活定制报表格式和规范，可根据要求生成用户环境（如：数据库地址、数据库名称、访问源IP地址、用户名称、源程序名称、源终端名称等）自定义报表。



3.2.12 权职分离

《计算机信息系统安全等级保护数据库管理技术要求》、《企业内部控制规范》、SOX法案或PCI等法案法规中明确提出对工作人员进行职责分离，系统设置权限角色分离。

审计要求	CobiT (SOX)	PCI DSS	HIPAA	CMS ARS	GLBA	ISO 17799 (Basel II)	NERC	NIST 800-53 (FISMA)
1. 存取关键敏感数据 Access sensitive data (Successful/Failed SELECTs)		✓	✓	✓	✓	✓		✓
2. 改变图表Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓		✓	✓	✓	✓
3. 改变数据Data Changes (DML) (Insert, Update, Delete)	✓			✓		✓		
4. 安全例外Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓	✓	✓	✓
5. 账户、角色和许可Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓	✓	✓	✓

提供超级管理员、资产管理员和审计管理员权限分离；资产管理员可以添加数据库审计服务器、审计策略制定、审计记录查看等。审计管理员可以查看和审计数据库会话详细信息、统计分析报表、安全操作日志、维护日志。并支持角色按模块灵活授权。

4 产品应用

数据库审计系统的应用，可以让客户对产品的应用体现出其真正价值所在，其产品优势有：数据库服务器的应用优化、数据库服务器的运维正常运行、敏感数据信息的泄密防护和法律责任的规避。

4.1 数据库服务器的应用优化

数据库审计系统的部署，管理员可以通过管理平台的各种流量排名工具，来发现网络中的异常访问网络服务器行为、从而优化数据库服务器的对外应用。

4.2 数据库服务器的运维正常运行

数据库审计系统的部署，运维人员以及管理人员可以通过数据库审计系统的详细审计信息、访问者操作数据库的指令等，用于当数据库因为外部操作出现异常、错误以及报警时，来判断错误原因和帮助恢复服务器的正常运行。

4.3 敏感数据信息的泄密防护

数据库审计系统的部署，运维人员以及管理员可以通过数据库审计系统中的数据库审计信息，来发现数据库中的内部敏感资料的外泄企图和事实。

4.4 法律责任的规避

数据库审计系统的部署，可以审计数据库的各种不符合当前法律所允许的内容，满足相关部门对使用数据库设备的备案审计要求。