

## 华为 UMA-DB 数据库审计特性描述

**版权所有 © 华为技术有限公司 2012。 保留一切权利。**

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI 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](mailto:support@huawei.com)

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

# 目 录

<b>1 策略管理特性</b>	<b>4</b>
1.1 资产	4
1.2 白名单	6
1.3 对象	6
1.4 策略	7
1.5 动作	9
1.6 管理	10
<b>2 日志审计特性</b>	<b>11</b>
2.1 会话审计	11
2.2 策略告警	16
2.3 异常告警	16
2.4 系统事件	17
<b>3 统计特性</b>	<b>18</b>
3.1 概要	18
3.2 报表任务	18
3.3 报表统计	21
<b>4 监控特性</b>	<b>23</b>
4.1 实时监控	23
4.2 系统监测	23
4.3 最新策略告警	24
4.4 最新违规操作	24
4.5 最新系统事件	24
4.6 系统硬件运行状态	24

# 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。



资产组列表 资产列表

配置：资产 > ora (192.168.1.98)

资产信息 来源限制 信任程序 信任账号 记录控制 应用策略

基本信息

名称：ora

IP地址：192 . 168 . 1 . 98

数据库/版本：ORACLE / 9i

端口：1521

选择资产组：oracle

编码：UTF-8

审计状态

活动

禁用

【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。**

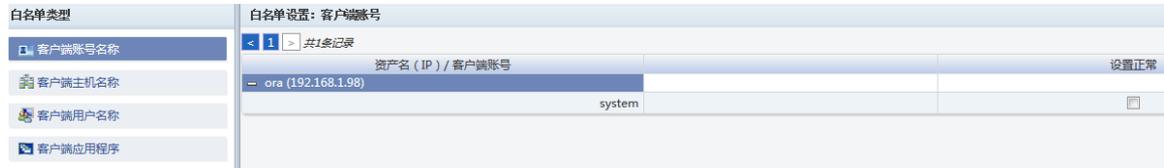


【应用策略】是查看应用在该数据库资产上的策略列表，可删除其已应用的策略。



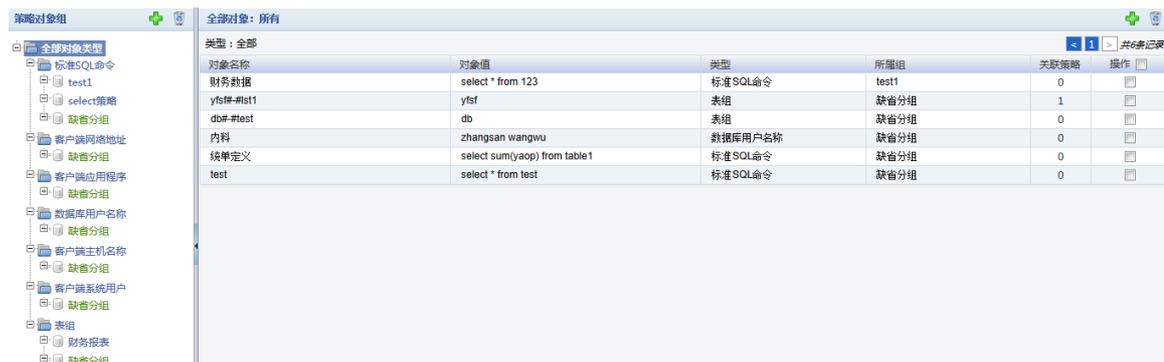
## 1.2 白名单

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。

配置：策略 > select from dba\_sql

匹配条件    动作    应用到    **保存信息**

告警级别：  低    中    高

已启用的字段    **保存为模板**    **载入模板**

[-] | 标准SQL命令(\*必选)

标准SQL命令：

INSERT	→ ←	选定的：
DELETE		UPDATE
ALTER DATABASE		ALTER FUNCTION
ALTER PROCEDURE		
ALTER TABLE		
CALL		
COMMIT		
CREATE DATABASE		

可用字段

+	+	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
+	+	SELECT控制项
+	+	表组

在【动作】中，可以选择要接收策略告警邮件的管理组：

配置：策略 > select from dba\_sql

匹配条件    **动作**    应用到    **保存信息**

[-] | 动作处理

选择动作：

内科主任告警	→ ←	管理员告警
		财务报表
		告诉XL

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。

配置：策略 > select from dba\_sql

匹配条件	动作	应用到	保存信息
资产组/资产	IP地址	类型	审计
- ORACLE			<input type="checkbox"/>
192.168.1.98	192.168.1.98	ORACLE 9i	<input type="checkbox"/>
192.168.1.88	192.168.1.88	ORACLE 10g	<input type="checkbox"/>
百度娘	192.168.2.122	ORACLE 11g	<input type="checkbox"/>
- sql2005			<input type="checkbox"/>
sql	192.168.1.98	SQL SERVER 2005	<input type="checkbox"/>
- MS SQLServer			<input type="checkbox"/>
ERP Database	192.168.1.132	SQL SERVER 2000	<input type="checkbox"/>

## 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。

动作列表

- 告警XL
- 财务报表
- 内科主任告警
- 管理员告警

动作名称: 告警XL

已选择的操作

邮件告警

关联用户

可选的系统用户:

admin

选定的系统用户:

peijun  
sstt  
youdao

WEB告警

关联用户

可选的系统用户:

admin  
peijun  
sstt  
youdao

选定的系统用户:

## 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。

审计: SQL数据

高级搜索 时间范围: 2011-11-01 00:00:00 - 2011-11-23 23:59:59

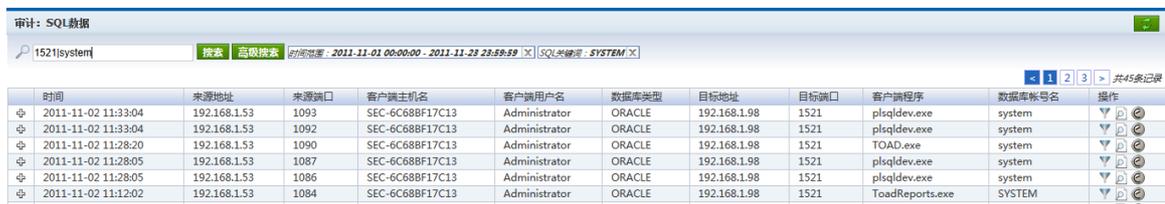
时间	来源地址	来源端口	客户端主机名	客户端用户名	数据库类型	目标地址	目标端口	客户端程序	数据库帐号名	操作
2011-11-02 11:33:04	192.168.1.53	1093	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	🔍
2011-11-02 11:33:04	192.168.1.53	1092	SEC-6C68BF17C13	Administrator	ORACLE	192.168.1.98	1521	plsqldev.exe	system	🔍
2011-11-02 11:28:20	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 11:21:202	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。





查看会话命令详情			
2011-11-02 11:04:40	26	ORA-01403: no data found	-
⇒ 2011-11-02 11:04:40	453	select tablespace_name, to_char(pct_free) pct_free, to_char(pct_used) pct_used, to_char(ini_trans) ini_trans, to_char(max_trans) max_trans, to_char(initial_extent) initial_extent, to_char(next_extent) next_extent, to_char(pct_increase) pct_increase, to_char(min_extents) min_extents, to_char(max_extents) max_extents, cluster_name from sys.all_tables where owner = :object_owner and table_name = :object_name	-
2011-11-02 11:04:40	33	Binded : Bind0=SYSTEM Bind1=HELP	-
2011-11-02 11:04:40	27	Execute Time := 0.004 sec	-
2011-11-02 11:04:40	26	ORA-01403: no data found	-
⇒ 2011-11-02 11:04:40	91	select * from sys.all_tables where owner = :object_owner and table_name = :object_name	-
2011-11-02 11:04:40	33	Binded : Bind0=SYSTEM Bind1=HELP	-
2011-11-02 11:04:40	27	Execute Time := 0.007 sec	-
2011-11-02 11:04:40	26	ORA-01403: no data found	-
⇒ 2011-11-02 11:04:40	103	select comments from sys.all_tab_comments where owner = :object_owner and table_name = :object_name	-
2011-11-02 11:04:40	33	Binded : Bind0=SYSTEM Bind1=HELP	-
2011-11-02 11:04:40	27	Execute Time := 0.003 sec	-
2011-11-02 11:04:40	26	ORA-01403: no data found	-
⇒ 2011-11-02 11:04:40	283	select col.*, com.Comments from sys.all_tab_columns col, sys.all_col_comments com where col.owner = :owner and col.table_name = :table_name and com.Owner (+) = :Owner and com.Table_Name (+) = :table_name and com.Column_Name (+) = col.Column_Name order by col.column_id	-
2011-11-02 11:04:40	33	Binded : Bind0=SYSTEM Bind1=HELP	-
2011-11-02 11:04:40	27	Execute Time := 0.007 sec	-
2011-11-02 11:04:40	26	ORA-01403: no data found	-
		select * from sys.all constraints where table name = :object name and owner = :	

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：

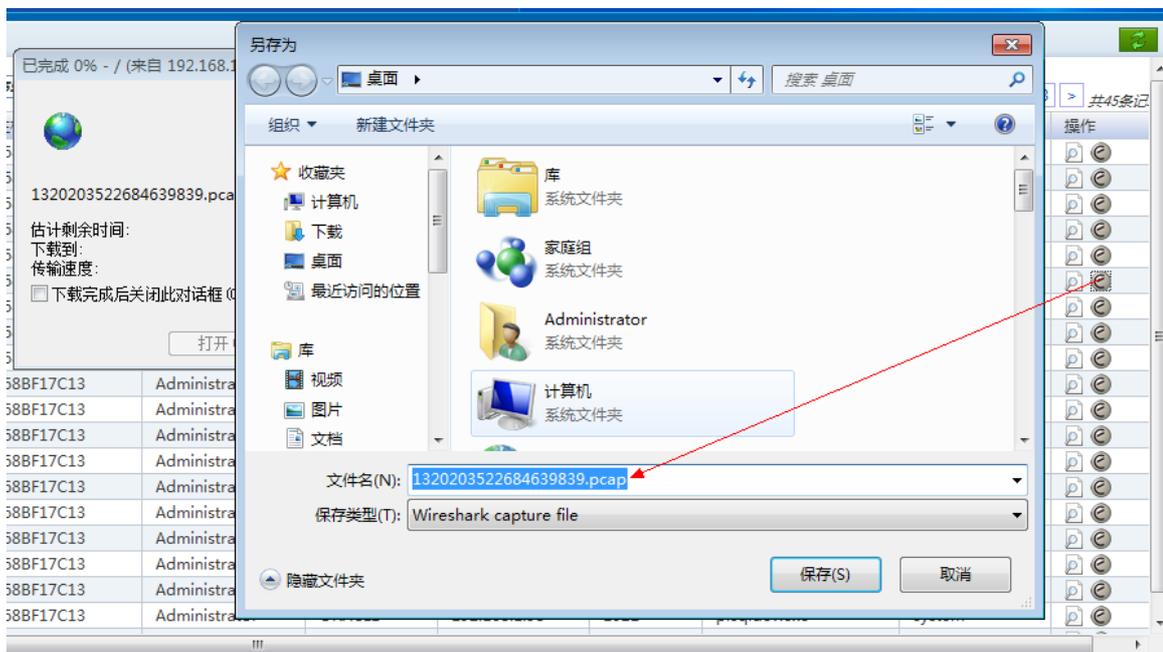
查看会话命令详情			
会话命令 - 来源地址 : 192.168.1.53:1161 目标地址 : 192.168.1.126:1433 客户端主机名 : - 客户端用户名 : 客户端程序 : - 数据库帐号 : -			
共66条记录			
执行时间	消息长度	消息	操作
⇒ 2011-11-21 11:59:16	138	Server info/error message: no=[5701], state=[2], level=[0], server=[GSQL], proc=[], msg=[已将数据库上下文更改为 'master'。]	-
2011-11-21 11:59:16	134	Server info/error message: no=[5703], state=[1], level=[0], server=[GSQL], proc=[], msg=[已将语言设置更改为 简体中文。]	-
⇒ 2011-11-21 11:59:16	21	SELECT @@LOCK_TIMEOUT	
⇒ 2011-11-21 11:59:16	669	IF (@@microsoftversion / 0x01000000) >= 9 AND ISNULL(IS_SRVROLEMEMBER(N'sysadmin'), 0) = 1 SELECT se.is_admin_endpoint AS N'AdminConnection' FROM sys.endpoints se INNER JOIN sys.dm_exec_connections dmc ON dmc.endpoint_id = se.endpoint_id WHERE dmc.session_id = @@spid ELSE SELECT CAST(0 AS BIT) AS N'AdminConnection'	
⇒ 2011-11-21 11:59:16	21	SELECT @@LOCK_TIMEOUT	
⇒ 2011-11-21 11:59:16	307	SELECT cfg.name AS [Name], cfg.configuration_id AS [Number], cfg.minimum AS [Minimum], cfg.maximum AS [Maximum], cfg.is_dynamic AS [Dynamic], cfg.is_advanced AS [Advanced], cfg.value AS [ConfigValue], cfg.value_in_use AS [RunValue], cfg.description AS [Description] FROM sys.configurations AS cfg	
⇒ 2011-11-21 11:59:16	21	SELECT @@LOCK_TIMEOUT	
⇒ 2011-11-21 11:59:16	22	SET LOCK_TIMEOUT 10000	-
⇒ 2011-11-21 11:59:16	73	SELECT CAST(SERVERPROPERTY('EngineEdition') AS int) AS [EngineEdition]	
⇒ 2011-11-21 11:59:16	12	use [master]	-
2011-11-21 11:59:16	138	Server info/error message: no=[5701], state=[1], level=[0], server=[GSQL], proc=[], msg=[已将数据库上下文更改为 'master'。]	-



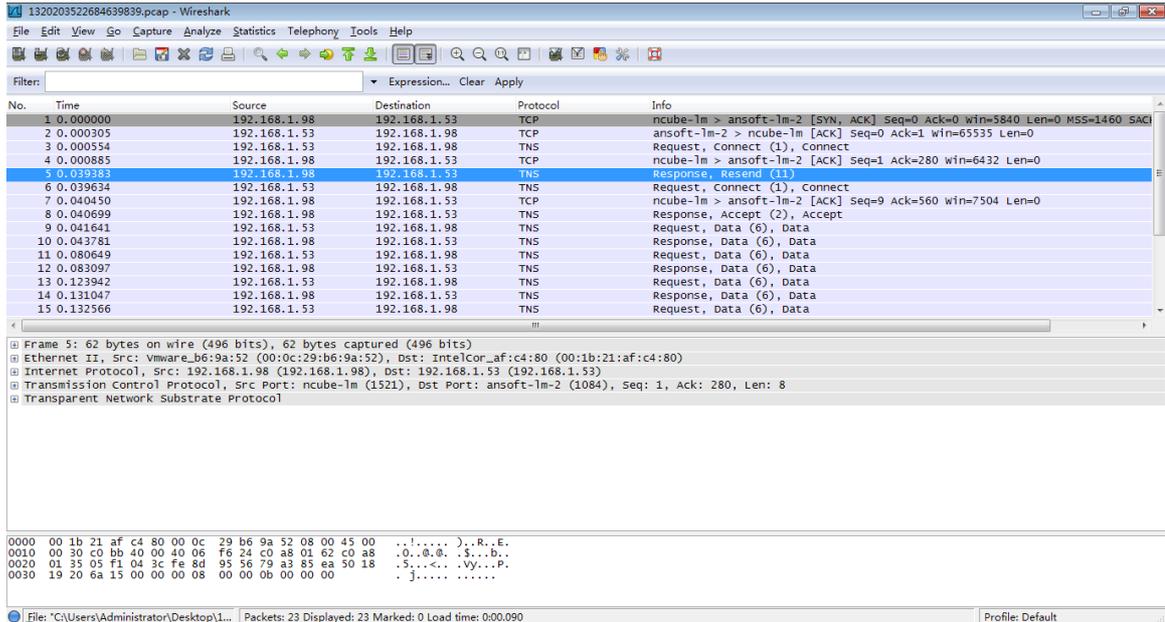
```

master Server[@Name='GSQL']/Database[@Name='master'] 1 90 3 0 0 master
model Server[@Name='GSQL']/Database[@Name='model'] 1 90 1 0 0 model
msdb Server[@Name='GSQL']/Database[@Name='msdb'] 1 90 3 0 0 msdb
tempdb Server[@Name='GSQL']/Database[@Name='tempdb'] 1 90 3 0 0 tempdb
    
```

**【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。

策略告警列表	策略告警详情																																																																																																								
<table border="1"> <thead> <tr> <th>NO.</th> <th>告警级别</th> <th>告警时间</th> <th>类型</th> <th>源地址</th> <th>目标地址</th> <th>数据库用户</th> <th>描述</th> </tr> </thead> <tbody> <tr> <td colspan="8">今天 (0) 过滤</td> </tr> <tr> <td colspan="8">昨天 (0) 过滤</td> </tr> <tr> <td colspan="8">以前 (38) 过滤</td> </tr> <tr> <td>1</td> <td>低</td> <td>2011-11-21 12:02:20</td> <td>SQL SERVER</td> <td>192.168.1.53:1160</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>2</td> <td>低</td> <td>2011-11-21 12:02:20</td> <td>SQL SERVER</td> <td>192.168.1.53:1164</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>3</td> <td>低</td> <td>2011-11-21 12:02:20</td> <td>SQL SERVER</td> <td>192.168.1.53:1165</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>4</td> <td>低</td> <td>2011-11-21 11:59:58</td> <td>SQL SERVER</td> <td>192.168.1.53:1165</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>5</td> <td>低</td> <td>2011-11-21 11:59:57</td> <td>SQL SERVER</td> <td>192.168.1.53:1161</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>6</td> <td>低</td> <td>2011-11-21 11:59:54</td> <td>SQL SERVER</td> <td>192.168.1.53:1161</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>7</td> <td>低</td> <td>2011-11-21 11:59:54</td> <td>SQL SERVER</td> <td>192.168.1.53:1161</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>8</td> <td>低</td> <td>2011-11-21 11:59:54</td> <td>SQL SERVER</td> <td>192.168.1.53:1161</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> <tr> <td>9</td> <td>低</td> <td>2011-11-21 11:59:51</td> <td>SQL SERVER</td> <td>192.168.1.53:1164</td> <td>192.168.1.126:1433</td> <td>N/A</td> <td>select告警</td> </tr> </tbody> </table>	NO.	告警级别	告警时间	类型	源地址	目标地址	数据库用户	描述	今天 (0) 过滤								昨天 (0) 过滤								以前 (38) 过滤								1	低	2011-11-21 12:02:20	SQL SERVER	192.168.1.53:1160	192.168.1.126:1433	N/A	select告警	2	低	2011-11-21 12:02:20	SQL SERVER	192.168.1.53:1164	192.168.1.126:1433	N/A	select告警	3	低	2011-11-21 12:02:20	SQL SERVER	192.168.1.53:1165	192.168.1.126:1433	N/A	select告警	4	低	2011-11-21 11:59:58	SQL SERVER	192.168.1.53:1165	192.168.1.126:1433	N/A	select告警	5	低	2011-11-21 11:59:57	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警	6	低	2011-11-21 11:59:54	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警	7	低	2011-11-21 11:59:54	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警	8	低	2011-11-21 11:59:54	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警	9	低	2011-11-21 11:59:51	SQL SERVER	192.168.1.53:1164	192.168.1.126:1433	N/A	select告警	<p>SQL请求 2011-11-21 11:58:56 至 2011-11-21 12:02:20</p> <p>客户端系统</p> <p>客户端IP: 192.168.1.53:1160 客户端用户名: n/a 客户端主机名: n/a</p> <p>客户端应用程序</p> <p>程序名称: n/a 程序版本: n/a</p> <p>服务端详情</p> <p>服务端地址: 192.168.1.126:1433 用户名: n/a 服务器名称: sql 语句组: n/a 语句长度: 18 SQL语句解析: select @@trancount 原始SQL语句: select @@trancount 表组: n/a 响应时间: n/a</p>
NO.	告警级别	告警时间	类型	源地址	目标地址	数据库用户	描述																																																																																																		
今天 (0) 过滤																																																																																																									
昨天 (0) 过滤																																																																																																									
以前 (38) 过滤																																																																																																									
1	低	2011-11-21 12:02:20	SQL SERVER	192.168.1.53:1160	192.168.1.126:1433	N/A	select告警																																																																																																		
2	低	2011-11-21 12:02:20	SQL SERVER	192.168.1.53:1164	192.168.1.126:1433	N/A	select告警																																																																																																		
3	低	2011-11-21 12:02:20	SQL SERVER	192.168.1.53:1165	192.168.1.126:1433	N/A	select告警																																																																																																		
4	低	2011-11-21 11:59:58	SQL SERVER	192.168.1.53:1165	192.168.1.126:1433	N/A	select告警																																																																																																		
5	低	2011-11-21 11:59:57	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警																																																																																																		
6	低	2011-11-21 11:59:54	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警																																																																																																		
7	低	2011-11-21 11:59:54	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警																																																																																																		
8	低	2011-11-21 11:59:54	SQL SERVER	192.168.1.53:1161	192.168.1.126:1433	N/A	select告警																																																																																																		
9	低	2011-11-21 11:59:51	SQL SERVER	192.168.1.53:1164	192.168.1.126:1433	N/A	select告警																																																																																																		

## 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。

NO.	告警级别	告警时间	类型	源地址	目标地址	数据库用户	描述
目前尚无数据							
目前尚无数据							
目前尚无数据							
1	低	2011-11-21 11:48:38	ORACLE	192.168.1.53:1157	192.168.1.98:1521	system	登录数据库账号异常
2	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1157	192.168.1.98:1521	system	登录源主机用户异常
3	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1157	192.168.1.98:1521	system	登录源主机名异常
4	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1157	192.168.1.98:1521	system	登录客户端异常
5	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1156	192.168.1.98:1521	system	登录数据库账号异常
6	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1156	192.168.1.98:1521	system	登录源主机用户异常
7	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1156	192.168.1.98:1521	system	登录源主机名异常
8	低	2011-11-21 11:48:37	ORACLE	192.168.1.53:1156	192.168.1.98:1521	system	登录客户端异常
9	低	2011-11-21 11:39:28	ORACLE	192.168.1.53:1154	192.168.1.98:1521	system	登录数据库账号异常
10	低	2011-11-21 11:39:28	ORACLE	192.168.1.53:1154	192.168.1.98:1521	system	登录源主机用户异常
11	低	2011-11-21 11:39:28	ORACLE	192.168.1.53:1154	192.168.1.98:1521	system	登录源主机名异常
12	低	2011-11-21 11:39:28	ORACLE	192.168.1.53:1154	192.168.1.98:1521	system	登录客户端异常
13	低	2011-11-21 11:39:02	ORACLE	192.168.1.53:1152	192.168.1.98:1521	system	登录数据库账号异常
14	低	2011-11-21 11:39:02	ORACLE	192.168.1.53:1152	192.168.1.98:1521	system	登录源主机用户异常
15	低	2011-11-21 11:39:02	ORACLE	192.168.1.53:1152	192.168.1.98:1521	system	登录源主机名异常
16	低	2011-11-21 11:39:02	ORACLE	192.168.1.53:1152	192.168.1.98:1521	system	登录客户端异常

SQL请求 2011-11-21 11:48:37 至 2011-11-21 11:48:38

客户端系统  
 客户端IP: 192.168.1.53:1157  
 客户端用户名: Administrator  
 客户端主机名: SEC-6C688F17C13

客户端应用程序  
 程序名称: plsqldev.exe  
 程序版本: n/a

服务端详情  
 服务端地址: 192.168.1.98:1521  
 用户名: system  
 服务器名称: ora  
 语句组: n/a  
 语句长度: 33  
 SQL语句解析:  
 [SessionLoginUsername = [system]  
 原始SQL语句: SessionLoginUsername = [system]  
 表组: n/a  
 响应时间: n/a

## 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。

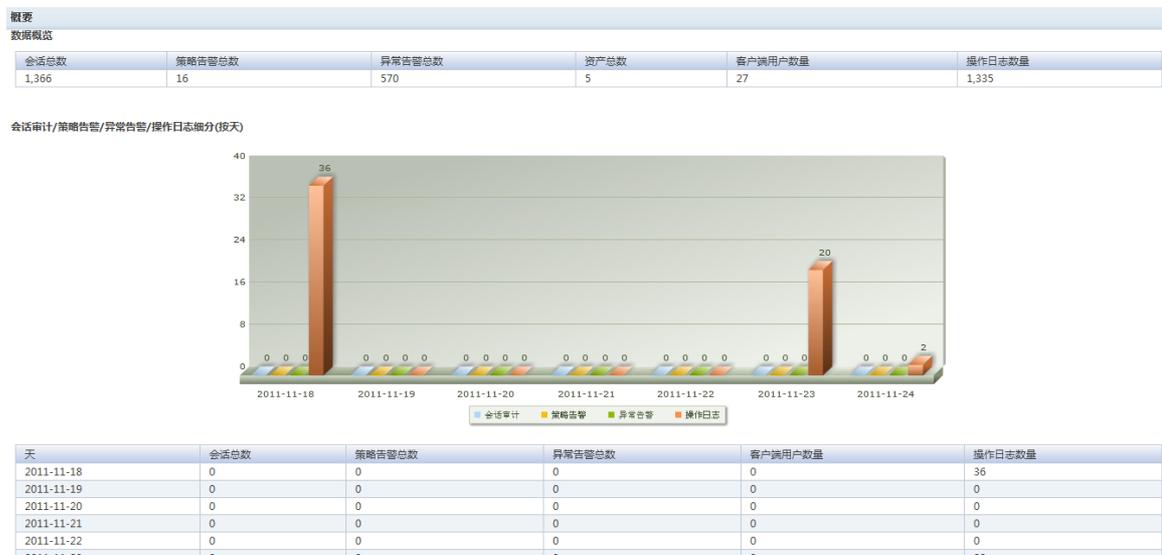
用户	事件级别	事件时间	用户IP	模块	内容	查看
admin	消息	2011-11-23 17:00:58	192.168.1.49	登录	使用用户名admin登录, 成功	🔍
admin	消息	2011-11-23 09:59:19	192.168.1.49	登录	使用用户名admin登录, 成功	🔍
--	错误	2011-11-23 09:59:15	192.168.1.49	登录	使用用户名admin登录-失败, 密	🔍
admin	消息	2011-11-22 17:08:06	192.168.1.49	统计报表	创建报表-月报表, 成功	🔍
admin	消息	2011-11-22 16:43:42	192.168.1.49	登录	使用用户名admin登录, 成功	🔍
--	错误	2011-11-22 16:43:39	192.168.1.49	登录	使用用户名admin登录-失败, 密	🔍
--	错误	2011-11-22 16:43:38	192.168.1.49	登录	使用用户名admin登录-失败, 密	🔍
admin	消息	2011-11-22 14:47:45	192.168.1.49	登录	使用用户名admin登录, 成功	🔍
admin	消息	2011-11-22 14:01:43	192.168.1.49	策略	更改策略select告警配置, 成功	🔍
admin	消息	2011-11-22 13:49:40	192.168.1.104	登录	使用用户名admin登录, 成功	🔍
admin	消息	2011-11-22 13:47:57	192.168.1.153	登录	使用用户名admin登录, 成功	🔍
admin	消息	2011-11-22 11:11:24	192.168.1.49	登录	使用用户名admin登录, 成功	🔍
admin	消息	2011-11-21 15:29:40	192.168.1.220	登录	使用用户名admin登录, 成功	🔍
admin	消息	2011-11-21 14:53:47	192.168.1.153	策略	删除策略动作faction, 成功	🔍
admin	消息	2011-11-21 14:52:42	192.168.1.153	策略	更改保存策略动作接口信息, 成	🔍
admin	消息	2011-11-21 14:52:13	192.168.1.153	策略	更改保存策略动作接口信息, 成	🔍
admin	消息	2011-11-21 14:52:06	192.168.1.153	策略	新增策略动作faction, 成功	🔍
admin	消息	2011-11-21 14:50:23	192.168.1.153	登录	使用用户名admin登录, 成功	🔍

事件时间: 2011-11-23 17:00:58  
 事件级别: 消息  
 用户: admin  
 用户IP: 192.168.1.49  
 系统模块: 登录  
 事件内容: 使用用户名admin登录, 成功

# 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。



## 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。

报表任务 + [trash]

配置：报表任务 > 月季度异常访问

选择计划

每天   
  每周   
  每月   
  只一次

在指定的时间生成报表一次

生成时间：2011-10-25 09 时 10 分

报表数据取自：最后30天

【基本信息】设置报表名称以及名称说明。

报表任务 + [trash]

配置：报表任务 > 月季度异常访问

基本信息

名称：月季度异常访问 \*

说明：一个月产生一次异常告警。

【报表格式】设置报表输出格式（支持 PDF 和 CSV）以及标题格式名。

报表任务 + [trash]

配置：报表任务 > 月季度异常访问

标题格式

报表标题：月季度异常访问 \*

标题样式：宋体 12点

子标题：10月份

输出格式

PDF   
  CSV

【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。

配置：报表任务 > 月季度异常访问

选择数据源

会话审计
  策略告警
  异常告警
  系统事件

数据模式

列表模式
  统计模式
 按 数据库类型 统计TOP 10

条件过滤器

已选的条件字段

可用的条件字段

- 告警级别
- 数据库类型
- 来源地址
- 来源端口
- 目标地址
- 目标端口
- 数据库用户
- 策略名称

【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。

配置：报表任务 > 月季度异常访问

已选的图表模块

3D柱状图模块

可用的图表模块

3D饼图模块

①标题：

②值显示： 数值  百分比(%)

①来源地址统计周报TOP10

来源地址	统计值
10.2.10.51	494
10.2.10.41	671
10.2.10.13	761
10.2.10.31	857
10.2.12.1	960
10.2.10.12	462
10.2.14.1	629
10.5.10.19	960
10.2.210.1	622
10.2.110.10	376
10.4.10.17	761
10.3.10.13	494

显示列表视图

【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

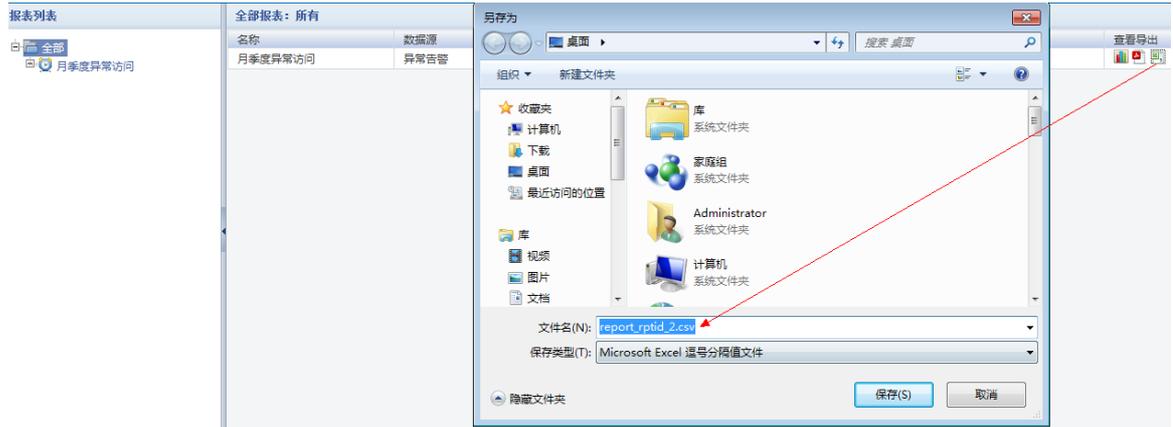
【报表统计】显示的是报表任务定制完后的效果，我们在该页面中可看到报表是否生效以及生效后的展现。

名称	数据源	计划	生成时间	查看导出
月季度异常访问	异常告警	生成于 2011-10-25 09:10:01, 20119时	2011-10-25 09:10:01	

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：



# 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。

