
# RG-DBS 500-A
# 全新数据库审计系统

如有疑问
扫一扫在线咨询

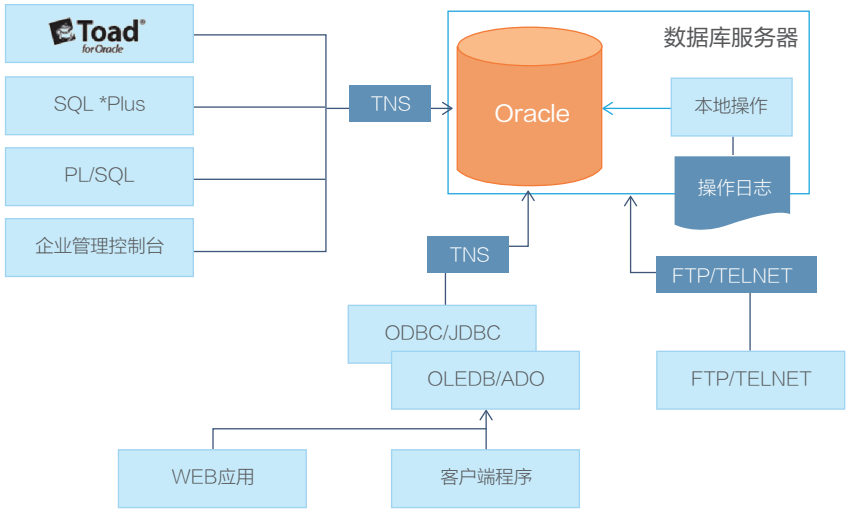
Ruijie Networks 锐捷

# 产品概述

RG-DBS系列对审计和事务日志进行审查，从而跟踪各种对数据库操作的行为。一般审计主要记录对数据库的操作、对数据库的改变、执行该项目操作的人以及其他的属性。这些数据库被记录到RG-DBS系列独立的平台中，并且具备较高的准确性和完整性。针对数据库活动或状态进行取证检查时，审计可以准确的反馈数据库的各种变化，对我们分析数据库的各类正常、异常、违规操作提供证据。

## 系统架构

锐捷RG-DBS系列作为全业务审计系统，支持各种数据库操作方案、网络操作方式。如下图所示，包括：基于客户端的链接审计、基于ODBC/JDBC等链接访问、本地操作、网络操作等。




**支持多种数据库类型：**

- 同时支持Oracle 8/9/10/11、DB2、INFORMIX、SYBASE、Microsoft SQL Server 97/2000/2005/2008、MYSQL、POSTGRESQL、CACHE；
- 国内唯一支持的厂商，cache正在成为高性能数据库应用场景的新宠等
- 同时支持多个系统数据库的审计
- 同时支持不同类型的数据库的审计

# 产品特性

## 独立的审计模式

在数据安全时代，独立的审计模式符合相关标准和法规的要求。锐捷RG-DBS系列采用独立的安全结构，通过交换机镜像完成数据的采集，不需要在应用系统、终端安装任何插件，其部署与运维不影响原有网络及应用。同时，锐捷RG-DBS系列采用三权分立的模式，这使得数据库维护或开发小组，安全审计小组的工作进行适当的分离。而且，审计工作不影响数据库的性能、稳定性或日常管理流程。审计结果独立存储于锐捷RG-DBS系列自带的存储空间中，避免了数据库特权用户或恶意入侵数据库服务器用户，干扰审计信息的公正性。

## 审计细腻度更深

**全面性：**针对业务层、应用层、数据库等各个层面的操作进行跟踪定位，包括数据库SQL执行情况、数据库返回值等。
**细粒度：**精确到表、对象、记录内容的细粒度审计策略，实现对敏感信息的精细监控。
**独立性：**基于独立监控审计的工作模式，实现了数据库管理与审计的分离，保证了审计结果的真实性、完整性、公正性。

## 审计语句分析和翻译

在实际项目中，有些单位有专门负责审计的机构，如在医院中，数据库审计系统权限由医院监管部门和信息科分别掌握，因数据库SQL语言及其它数据库语言如M语言的抽象性，非专业技术人员很难看懂语句的真实信息以及蕴含的风险，而专业技术人员不存在该问题，为更好的方便客户使用，锐捷RG-DBS系列提供了专业的数据分析和翻译界面。通过在配置中设置表和字段的中文别名，在翻译中以直观和易懂的语言显示审计的结果及语意关系，方便非专业技术人员的查看。

## 防二次泄密

在对数据库查询操作返回结果的审计中，返回信息包含了重要的敏感的信息，一旦被审计人员看到会造成信息的二次泄密，同时也会增加审计人员泄密敏感信息的可疑性。对审计结果中敏感字段进行系统级隐秘设置，可减少审计人员自身泄露敏感信息的可能性，同时也增加了数据的安全性和保密性。

## 分权管理

安全法规要求审计设备具有一定的权限控制，锐捷RG-DBS系列设置了权限角色分离，如系统管理员负责设备的运行设置；审计员负责查看相关审计记录及规则违反情况；规则配置员负责数据库审计安全规则的配置等。

## 事件准确定位

在信息安全及虚拟化背景时代下，单靠某一个信息去定位违规操作者已经成为不可能，如内网用户大多采用DHCP分配IP地址，没有做IP-MAC绑定及相应的准入规则，用户可通过更改操作系统名、IP地址、MAC地址等方式逃避追踪，传统的数据库审计定位往往局限于IP地址和MAC地址，很多时候不具备可信性。因此只有通过关联尽可能多的身份定位信息进行定位以及做一定的准入权限设置，其审计结果才具有可靠性，才能作为电子证据。锐捷RG-DBS系列可以对IP、MAC、操作系统用户名、使用的工具、应用系统账号等一系列进行关联分析，从而追踪到具体人。

## 返回结果

返回结果就是指某个查询操作所返回的数据，审计过程中可根据返回数据的内容、返回行数去直观的判断操作的危险性。锐捷RG-DBS系列可审计到双向数据，从客户端请求到服务器端的响应，做到双向审计。

## 事件关联性分析

锐捷RG-DBS系列可对响应事件进行关联，如根据IP关联出某段时间内该IP所触发的告警数量等；根据一段时间内的数据库或应用系统登录失败次数判断出暴力破解密码的可能性；根据账号的多次登录判断账号信息泄密或共享账号的可能性；相似SQL语句执行时间过长从而判断该语句设计的合理性等。根据事件关联性分析，自动涌现一批对客户具有实用价值的信息，帮助客户管理和维护好现有应用。

# 技术参数

| 功能名称 | 具体描述 |
| --- | --- |
| 硬件配置 | 采用独立的标准机架式硬件架构，软硬件一体化系统<br>采用全操作系统，内嵌数据库，用户无需另外安装操作系统及数据库管理系统<br>外观：标准1U机架式。一个DB9串口，不少于6个100/1000M 电口，其中一个管理口，其余的为审计口，硬盘1T。 |
| 基本要求 | 包括审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置 |
| | 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Cache、达梦等数据库的审计，满足所有信息化系统数据库的安全审计需要 |
| | 可支持同时审计多个不同类型的数据库,审计数据统一存储、查询、分析、统计 |
| 系统部署 | 采用旁路部署方式对原有网络不造成影响，网络审计产品的故障不影响被审计系统的正常运行 |
| | 本表中所有功能的实现，均无需在被审计数据库服务器上安装任何软件代理或插件，无需提供被审计数据库服务器的任何管理账号和密码 |
| | 系统支持分布式部署 |
| 审计能力 | 支持函数审计(sum求和函数等），防止进行数据库统计行为 |
| | 支持数据库绑定变量审计 |
| | 支持端口重定向的审计 |
| | 在无需重启数据库情况下，支持对MS SQLSserver 加密协议的审计 |
| | 支持服务器虚拟化的审计 |
| | 支持虚拟桌面操作的审计 |
| | 支持Telnet、FTP协议的审计 |
| | 支持所有应用http以及web报表审计，并能支持工号（账号）审计，能详细定位到人；重要关键页面可以通过执行审计url输出返回内容信息。同时支持和数据库访问关联。 |
| | 支持超长操作语句审计，针对传统型数据库，支持3万字节的审计而不截断，针对Cache数据库，支持50万字节长度不截断 |
| | 支持Cache数据库集成工具terminal、portal、studio、Sqlmanager、MedTrak工具的审计，其中Portal能审计到sql语句、查询Global、返回结果，Terminal能审计到M语句和返回结果 |
| | 中间件的支持，支持COM、COM+、DCOM组件的三层架构审计，能精确定位到人（工号、账号） |
| | 支持访问数据库的源主机名、源主机用户的审计 |
| | 支持SQL操作响应时间的审计 |
| | 支持Select操作返回结果及行数的审计 |
| | 支持数据库账号登陆成功、失败的审计 |
| | 支持数据库操作成功、失败的审计 |
| | 支持对执行时间长达48小时操作的审计 |

| 功能名称 | 具体描述 |
| --- | --- |
| 审计能力 | 支持对SQL注入、跨站脚本攻击等web攻击的识别与告警 |
| | 支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的SQL操作审计 |
| 审计策略支持 | 系统自带审计规则库，用户可自定义审计策略 |
| | 可提供通过子对象模式多级关联跨表跨字段的组合规则 |
| | 审计策略支持select、create、execute、insert、alter、call、pdate、drop、logout、delete、rollback、login、truncate、grant等数据库操作命令作为分项响应条件 |
| | 审计策略支持数据库语句执行时间、语句执行回应、最大操作语句长度等作为分项响应条件 |
| | 审计策略支持数据库客户端操作系统主机名及用户名、客户端进程、客户端MAC、客户端IP等作为分项响应条件 |
| | 审计策略支持数据库名、表、包、过程、函数、视图、字段、索引、数据库帐户（用户名）等作为分项响应条件 |
| | 审计策略支持数据库操作返回内容、返回行数作为分项响应条件 |
| | 审计策略支持数据库操作关键字作为分项响应条件 |
| 响应方式 | 完整真实地记录及存储审计事件信息 |
| | 系统管理界面告警 |
| | Syslog告警 |
| | SNMP trap告警 |
| | 邮件告警 |
| | 短信告警 |
| 事件查询统计 | 实时监控，提供实时告警信息，可对当前会话进行详细察看，有助于管理员及时处置 |
| | 审计数据支持18种以上查询条件，可支持按数据库操作命令（包括select、create等14个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（包括开始、结束日期）等为条件进行查询 |
| | 告警检索效率高达亿条数据分钟级 |
| | 支持按自定义关键字作为查询和统计条件 |
| | 支持条件之间的与、或、非逻辑组合查询 |
| | 实现对所有违规事件出现频率进行图形化的汇总统计分析，并提供对汇总结果的实时查询功能；可以对客户端使用的程序、客户端IP、用户名进行图形化排名展示，并生成报表 |
| | 支持自定义报表 |
| | 可集成等级保护报表，确保能通过信息安全等级保护的评测 |
| | 支持以Word、PDF、xls等格式的报表导出 |
| | 可对可疑监控对象的操作语句进行回放，方便追溯 |

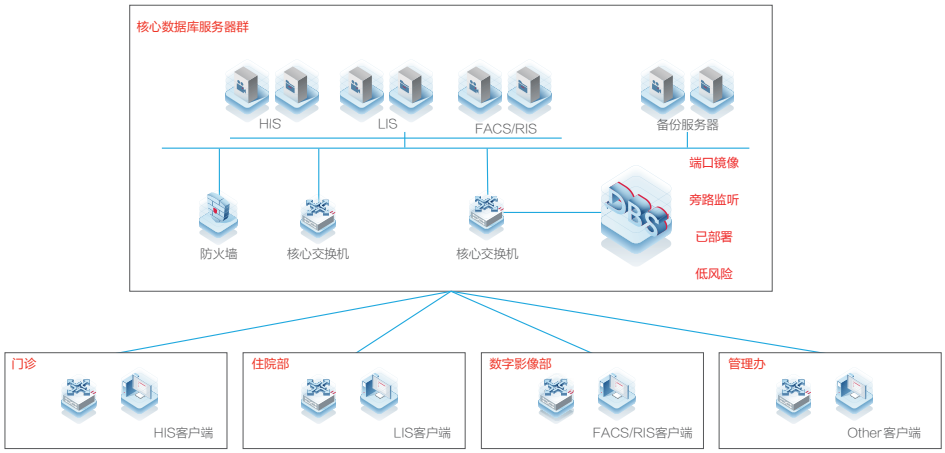
| 功能名称 | 具体描述 |
| --- | --- |
| 安全功能 | 审计报表加密设置,采用国际通用的AES 256位加密算法 |
| | 审计结果隐秘设置，通过*号对审计结果中的重要信息进行隐秘处理，防止非法权限查看 |
| | 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能 |
| | 系统本身具备能发现未知仿冒进程工具、防范非法IP地址、防范暴力破解登录用户密码、设置系统黑白名单等安全功能 |
| | 管理员登陆支持静态口令认证，支持密码的复杂性管理，比如大小写、数字、特殊字符、长度等 |
| | 能够对连续失败登陆进行自动锁定，锁定时间可设置 |
| 配置管理 | 采用B/S管理方式，全中文界面 |
| | 提供系统升级功能，能够通过升级包的方式实现升级 |
| | 提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式 |
| | 能够实现对自动备份、手动备份审计数据的恢复还原 |
| | 支持对审计数据存储容量达到一定阀值后，对老记录的自动删除功能 |
| | 翻译功能：实现对SQL语句转换成中文自然语言的描述功能，便于不同层次人员理解报警内容 |
| | 提供磁盘存储容量不足、磁盘Raid故障等自动邮件报警 |
| | 提供设备自身CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能 |
| | 提供审计策略和配置的导入导出 |
| | 系统预留接口以作维护及二次开发之用 |
| 第三方接口 | 支持Syslog方式向外发送审计日志 |
| | 支持SNMP Trap方式向外发送审计日志 |
| | 支持与第三方邮件系统对接 |
| | 外置短信猫，支持GSM卡 |
| | 支持第三方短信平台对接 |
| | 支持与FTP服务器对接（备份还原） |
| | 支持NTP时间同步 |

# 典型应用

为了完全不影响数据库系统自身运行与性能，数据库安全审计系统应支持采用旁路监听或模式，具体可分为核心交换机网络监听模式、网桥模式和数据库系统主机上实施监听模式。

## 交换机网络监听模式

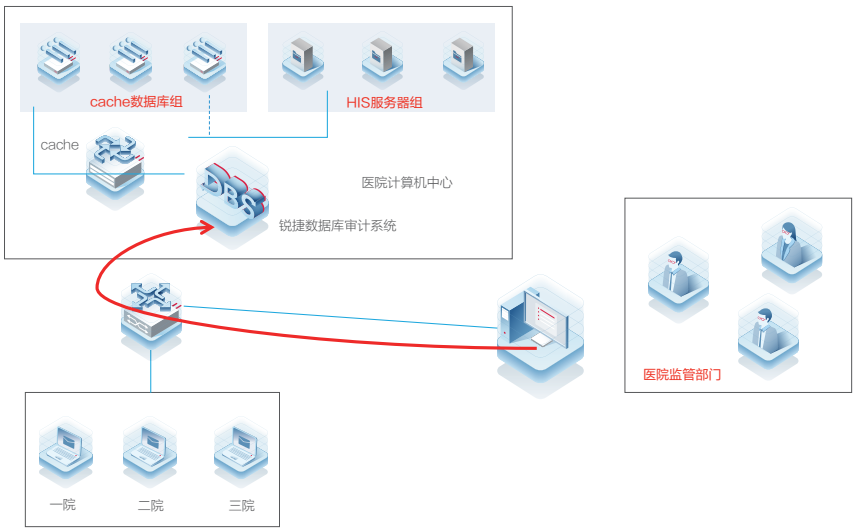
通过在核心交换机上设置端口镜像模式或采用TAP分流监听模式，使安全审计引擎能够监听到所有用户通过交换机与数据库进行通讯的全部操作。具体部署结构如图所示。




交换机网络监听模式审计系统部署示意图

## 集中管理平台部署模式

过去在大型审计项目集中管理中，无法实现对数据库审计设备系统的集中管理、维护，监控、预警 ，审计中心很难得到有效的汇总报告，设备出现故障无法及时准确定位、权限分散的管理模式使管理维护成本居高不下等问题，锐捷提供了业界最为领先的数据库审计集中管理和技术手段，彻底解决了大型数据库审计项目面临的部署、管理、监控、预警以及日志方面的问题。




集中管理平台部署示意图

# 订购信息

**RG-DBS 500-A全新数据库审计系统**

| 本产品订购信息 | |
|---|---|
| 型号 | 描述 |
| RG-DBS 500-A | RG-DBS 500-A主机(1U) |