# 绿盟数据库审计系统

# 产品白皮书

# 目录

# 一. 产品概述

绿盟数据库审计系统-NSFOCUS Database Audit System（简称 DAS）是能够实时监视、记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理系统。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部网络行为记录，提高数据资产安全。

# 二. 产品综述

DAS 是一款专业、实时进行数据库访问监视与审计的数据库安全设备。能够多角度分析数据库活动，并对异常的行为具有告警通知、审计记录、时候追踪分析功能。DAS 独立于数据库进行配置和部署，这种方式能够在不影响数据库的前提下，达到安全管理的目的。DAS 支持灵活的部署模式，包括旁路和多级部署模式。

与传统数据库审计产品中的 SQL 处理机制（依赖于正则表达式、字符串等技术识别 SQL）不同，DAS 完全模拟数据库的词法、语法（lex/yacc）解析，可以精准、智能的识别 SQL 类型，从而灵活的构建行为模型，且能够快速、准确的配置和定位策略。此外，通过智能的 SQL 识别，采用启发式风险评估，能够及时发现数据库操作的潜在风险，从而能够实现事后对数据库操作记录进行合规性分析。

由于数据库系统的庞大和复杂，数据库自身存在各种各样的漏洞，出于应用系统的稳定性等考虑，数据库系统往往不能及时升级补丁修复漏洞，这就给黑客对数据库的攻击提供了便利条件。DAS 通过漏洞攻击特征识别技术，在不需要数据库做任何补丁、升级工作的前提下，即可实现对 400 种以上的数据库漏洞攻击行为进行准确监测，及时告警。

DAS 能够通过易用的配置，达到细粒度访问审计配置的目的，直接在 DAS 上对数据库用户权限进行细粒度划分，对于违反细粒度策略的访问行为进行审计、告警，从而确保数据库操作达到合规性要求。

DAS 可监视数据库访问，实施访问策略，对异常的行为进行实时告警，并帮助事后分析来自于内外部的数据库攻击行为。此外，DAS 还提供强大的数据库活动审计功能，从多个角度灵活呈现数据库的活动情况，有助于对数据库现状进行分析。

DAS 能够获取详细的用户信息，它能与应用系统用户对接，将数据库行为定为到应用用户，能够获取访问数据库的用户 IP、MAC 以及操作系统信息，从而将针对数据库的行为定为到具体的人和地点。

# 三. 产品优势

## 3.1 灵活的数据库审计配置策略

DAS 提供了灵活和易于操作的策略配置管理。策略配置为高效而全面地实现数据库安全审计起到了决定性的作用。

DAS 有以下多种配置策略；

**全面审计策略：**所有的数据库请求都会被审计，保证审计的全面性；

**审计过滤策略：**在某些高吞吐量场景，过高的负载将使实时处理和存储压力过大，通过系统提供的白名单过滤、白名单规则可以对常规安全语句、安全来源实现审计过滤，使系统能够在过载的情况下，集中在危险或异常的 SQL 语句审计上；

**重点语句告警策略：**无论是否执行全面审计的策略，系统都可以对需要重点监视的语句进行特殊对待，可以通过黑名单、正则表达、重点用户、重点 IP、返回行数等策略完成对重点关注对象和行为的定义，对这些重点对象和行为的语句可以将其放入到告警审计中，可以通过 syslog、snmp、邮件或短信等多种途径对这些语句进行告警。

## 3.2 强大数据库入侵检测能力

DAS 提供了强大的入侵检测能力，对入侵行为进行重点告警；DAS 对入侵检测行为提供了大量的检测策略定义方法，包括：

A. 危险客户端登录：通过 IP、用户、数据库客户端工具、时间等多维定义可能具有入侵风险的登录；

B. 危险访问行为：通过用户、敏感对象、时间、返回行数、操作是否有 Where、是否使用了系统对象、高危操作子等多种方式定义了危险访问行为；

C. SQL 注入：系统提供了系统性的 SQL 注入库，以及基于正则表达式或语法抽象的 SQL 注入描述扩展；

D. 漏洞攻击库：系统提供了针对数据库漏洞进行攻击的描述模型，使对这些典型的数据库攻击行为被迅速发现；

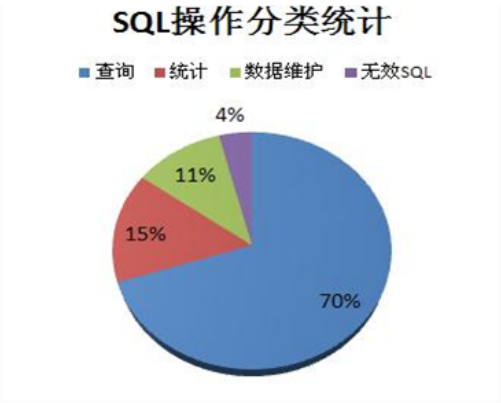
E. 黑名单：提供准确而抽象的方式，对系统中的特定访问 SQL 语句进行描述，使这些 SQL 语句出现时能够迅速报警。

## 3.3 全方面、细粒度审计分析

DAS 提供了大量预定义的分析和追踪报告供不同需求的管理者使用；分析的内容涵盖了：

- 提供丰富的、精细的审计数据分析和追踪报告
  - 关键敏感对象的访问分析
  - DB 实例访问综合分析
  - IP(MAC)行为分析和追踪
  - 用户行为分析和追踪
  - SQL 行为分析和追踪（基于精细 SQL 解析和分类）
  - SESSION 会话分析和追踪、回溯
- 提供精确、实时的危害性行为分析和追踪
  - 新类型 SQL（新型攻击）发现和分析追踪
  - SQL 注入风险分析和追踪
  - 精细访问告警分析和追踪
  - DB 漏洞攻击行为分析和追踪
  - 高危操作分析和追踪
  - 大规模数据泄漏分析和追踪
  - 批量数据篡改行为分析和追踪。
- 提供准确详细的数据库应用系统性能分析和追踪
  - SQL 报文流量分析和追踪
  - TOP N SQL 分析

例如关键敏感对象的访问分析：




**关键敏感对象访问行为分析和追踪**

全部展开 全部收起

| 统计时间 | DB用户 | OS用户 | IP(MAC) | 操作 | 操作语句 |
|---|---|---|---|---|---|
| 2012-10-23 10:10:15 | SYS | admin | 192.168.1.20 (E2-97-5A-0B-87-WW) | 数据维护 | 查看语句 |
| SQL: SELECT TO_CHAR(END_DATE,'#')FROM TF_O_SPECIAL_DEAL WHERE USER_ID=:1 AND PARTITION_ID=MOD(:2,0)AND SYSDATE BETWEEN START_DATE AND END_DATE; | | | | | |
| 2012-10-23 10:10:15 | SYS | admin | 192.168.1.201 (B8-97-5A-0B-87-8B) | 统计分析 | 查看语句 |
| 2012-11-23 12:10:15 | SCOTT | optor | 192.168.1.10 (RT-ED-5A-0B-87-8B) | 对象管理 | 查看语句 |
| SQL: SELECT COUNT(*)FROM TD_B_OBJECT WHERE ATTR_TYPE='#'; | | | | | |
| 2012-11-23 13:10:15 | USER0 | amdin | 192.168.1.33 (3R-56-5A-0B-87-8B) | 统计分析 | 查看语句 |
| 2012-11-12 13:12:14 | USER1 | test | 192.168.1.24 (7U-97-5A-0B-87-8B) | 对象管理 | 查看语句 |
| SQL: SELECT S.TABLE_OWNER,S.TABLE_NAME FROM SYS.ALL_SYNONYMS S WHERE S.SYNONYM_NAME=:B2 AND S.OWNER=:B1 AND ROWNUM=0; | | | | | |
| 2012-11-32 10:32:15 | TEST | test | 192.168.1.13 (TU-97-4T-0B-87-RT) | 查询 | 查看语句 |
| SQL: UPDATE UCR_ACT1.ODCT#B8EZ4GKCQ2GEATHC SET CUST_NAME=:1 WHERE CUST_ID=:2 AND PARTITION_ID=:3; | | | | | |

## 3.4 准确的应用用户关联能力

DAS 是国内首个可以做到 100%应用关联审计准确率的同类产品。

DAS 通过应用层访问和数据库操作请求进行多层业务关联审计，实现访问者信息的完全追溯，包括：操作发生的应用用户、URL、客户端的 IP、请求报文等信息，通过多层业务关联审计更精确地定位事件发生前后所有层面的访问及操作请求，使得追责、问责到具体操作人变得现实，真正做到数据库操作行为可监视,违规操作可追溯。

DAS 提供的关联方法，避免了传统关联中基于时间匹配所造成的大量错审现象，使应用用户与 SQL 语句实现实时、准确关联；也使针对应用用户危险行为描述、审计和实时告警成为可能。

## 3.5 完备的系统持续在线保障

DAS 全方位确保设备本身的高可靠性，包括但不限于：

- 物理保护：关键部件采用冗余配置（如：冗余电源等）。
- 系统故障保护：内置监测模块准实时地监测设备自身的健康状况。
- 不间断的管理保护：在进行策略配置情况下，能保持网络的连接和保护。
- 不丢包：基于硬件加速的接口卡，在高速环境下实现 100%数据包捕获。

# 四. 产品功能

## 4.1 审计模式支持

当用户与数据库进行交互的过程中，DAS 系统能实时审计用户行为，并根据预定义策略对用户行为进行监测，任何被监测到的违规操作都可以被记录和告警。

DAS 系统中支持的工作模式是数据库活动审计模式。数据库活动审计模式是非入侵防护模式，所有的数据包会全部放行，能够显示策略的风险等级和“执行结果”，但不会真正的执行策略动作。这是一种通过“旁路”方式对被保护的数据库进行记录和审计的模式。这种模式对来自网络的数据库操作，支持的安全策略包括告警（Alarm）审计。

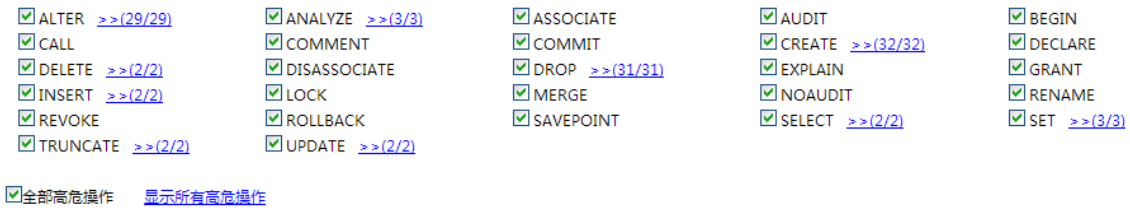
## 4.2 全面的实时审计

DAS 突破了传统审计产品 5 要素的审计能力瓶颈，将可审计要素提升至 7 个方向

| | |
|---|---|
| Who | 真实的数据库帐号、主机名称、操作系统帐号、应用账户等 |
| What | 什么对象数据被访问了，什么操作被执行了 |

| | |
|---|---|
| When | 每个事件发生的具体时间 |
| When | 事件的来源和目的，包括 IP 地址、MAC 地址等 |
| Where | 通过哪些应用程序或第三方工具进行的操作 |
| Range | 该操作执行的影响是多大范围，如查询的记录行数，或修改删除的行数 |
| Resultset | 结果集，例如查询操作的返回内容 |

精细全面的 SQL 行为分析:最关键的 DAS 通过对捕获的 SQL 语句进行精细的 SQL 语法分析,并根据 SQL 的行为特征和关键词特征对 SQL 语句进行自动分类，从而可以轻松的将大量系统生成的不同的 SQL 语句有效的“归类”到几百个甚至几十个类别范围内，从而使对审计结果的分析更精确、更可用。主要 SQL 类别如下图所示：




## 4.3 完备的双向审计

DAS 系统提供对双向数据包的解析、识别，不仅能够识别用户的请求，还能够对数据库的应答做了详细的统计，包括命令执行的时长、影响行数、应答码等信息。

以下是 DAS 系统中对错误 SQL 信息的统计：


能够对用户的访问行为进行回放：

```
[登录] 2012-8-5 14:05:11 > login sys(IP:192.168.1.245 MAC:705AB65DE811)
[请求] 2012-8-5 14:05:23 > SELECT USER FROM DUAL;
[回应] 2012-8-5 14:05:23 > 成功(1 row fetched)
[请求] 2012-8-5 14:05:23 > BEGIN DBMS_OUTPUT.DISABLE;END;
[回应] 2012-8-5 14:05:23 > 成功
[请求] 2012-8-5 14:05:23 > SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,
DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE(UPPER('#')LIKE UPPER(PRODUCT))
AND(UPPER(USER)LIKE USERID);
[回应] 2012-8-5 14:05:23 > 成功(no data)
[请求] 2012-8-5 14:05:24 > SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE
(UPPER('#')LIKE UPPER(PRODUCT))AND((UPPER(USER)LIKE USERID)OR(USERID='#'))
AND(UPPER(ATTRIBUTE)='#');
[回应] 2012-8-5 14:05:24 > 成功(1 row fetched)
[请求] 2012-8-5 14:05:24 > BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:1,NULL);END;
[回应] 2012-8-5 14:05:24 > 成功
```

## 4.4 细粒度的审计规则

DAS 提供了可配置的细粒度的审计规则，可以根据系统的需要，确定不同的审计策略，包括：

TraceLog 审计的内容：SQL 语句、SQL 语句参数、执行结果（成功、失败和详细的失败原因）、被影响的记录、详细的查询结果集、事务状态、会话登录和登出信息等。

审计的范围：对象、操作（上百种操作可选）、SQL 分类类型（基于 DAS 对 SQL 的分类结果进行筛选）、用户、指定的客户端（IP、MAC）、客户端工具或应用系统等。

提供了实时的风险评估引擎、漏洞攻击监测引擎、细粒度访问监测引擎的告警数据。

## 4.5 黑白名单和例外策略

DAS 建立所有被保护数据库的活动基线，包括 DML、DDL、DCL、只读活动（SELECT）以及已存在程序的使用。

DAS 通过学习模式以及 SQL 语法分析构建动态模型，形成白名单，此外，为了完善用户访问数据库的正常模型，还允许 DAS 管理者对通过对已经识别的 SQL 信息进行操作，完善黑白名单的策略，包括，将未识别 SQL 归入到黑白名单以及将黑白名单中的信息互相调换。

DAS 允许对黑白名单配置不同的策略。对白名单只允许设置审计类策略和放行，对黑名单可以进行全部的告警策略。当 DAS 检测到用户提出的请求和行为模型出现差异时，DAS 将根据用户的配置进行警告操作。

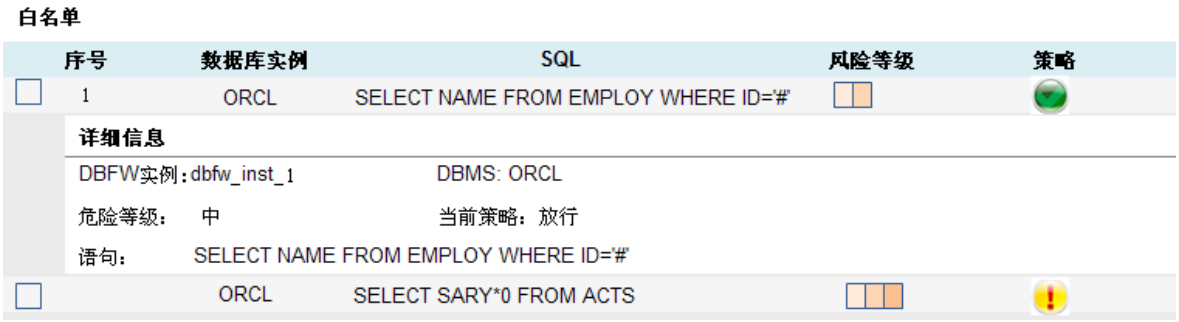



图 2-4 白名单列表

此外，DAS 还能够对所有策略指定例外机制，在此时间范围内，对应规则将失效。

## 4.6 大数据量日志记录

由于 DAS 采用了基于 SQL 语法的分析和重写的归一化技术，只保留了 SQL 语句中的本质特征的一份副本，而仅需大量保存各 SQL 语句动态的条件值或参数，因此，DAS 能够存储尽可大量的日志数据。

DAS 能够存储数据量大小，因硬盘大小而不同，例如 1TBG 的硬盘，DAS 可以存储的数据量能够达到 10 亿条，是同类产品的 4~5 倍。

## 4.7 应用用户关联审计

对于 B/S 架构的应用系统而言，用户通过 WEB 服务器实现对数据库的访问，传统的数据库审计系统只能审计到 WEB 服务器的相关信息，无法识别是哪个原始访问者发出的请求。DAS 通过关联应用层的访问和数据库层的访问操作请求，可以追溯到应用层的原始访问者及请求信息（如：操作发生的 URL、客户端的 IP 等信息），产品主要根据时间片、关键字等要素进行信息筛选，以确定符合数据库操作请求的 WEB 访问，通过三层审计更精确地定位事件发生前后所有层面的访问及操作请求。

| 数据库实例 | 数据库版本 | 服务器IP | 端口号 | 最后登录时间 | 客户端IP | 系统用户 | 数据库用户 | 会话数 | 活跃会话数 |
|---|---|---|---|---|---|---|---|---|---|
| ORCL24 | 10.2.0.1 | 192.168.1.24 | 1521 | 2013-08-12 14:29:32 | 192.168.1.116 | Administrator | CSC | 6 | 0 |
| ORCL24 | 10.2.0.1 | 192.168.1.24 | 1521 | 2013-08-09 16:50:51 | 192.168.1.69 | admin | LYJ | 43 | 1 |
| ORCL24 | 10.2.0.1 | 192.168.1.24 | 1521 | 2013-08-09 16:12:01 | 192.168.1.186 | Administrator | csc | 17 | 4 |
| ORCL24 | 10.2.0.1 | 192.168.1.24 | 1521 | 2013-08-09 15:52:54 | 192.168.1.186 | Administrator | CSC | 6 | 0 |
| ORCL24 | 10.2.0.1 | 192.168.1.24 | 1521 | 2013-08-09 15:03:55 | 192.168.1.69 | admin | lyi | 1 | 0 |

## 4.8 SQL 操作回放

DAS 允许安全管理员对过去某一时段的事件进行回放，真实展现当时的完整操作过程，便于分析和追溯系统安全问题。

很多安全事件或者与之关联的事件在发生一段时间后才引发相应的人工处理，这个时候，作为独立审计的 DAS 就发挥特别的作用. 因为所有的 FTP、telnet、SSH、数据库操作等事件都保存后台(包括相关的告警)，对相关的事件做定位查询，缩小范围，使得追溯变得容易。

sql 操作的回放：

```
[登录] 2012-8-5 14:05:11 > login sys(IP:192.168.1.245 MAC:705AB65DE811)
[请求] 2012-8-5 14:05:23 > SELECT USER FROM DUAL;
[回应] 2012-8-5 14:05:23 > 成功(1 row fetched)
[请求] 2012-8-5 14:05:23 > BEGIN DBMS_OUTPUT.DISABLE;END;
[回应] 2012-8-5 14:05:23 > 成功
[请求] 2012-8-5 14:05:23 > SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,
DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE(UPPER('#')LIKE UPPER(PRODUCT))
AND(UPPER(USER)LIKE USERID);
[回应] 2012-8-5 14:05:23 > 成功(no data)
[请求] 2012-8-5 14:05:24 > SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE
(UPPER('#')LIKE UPPER(PRODUCT))AND((UPPER(USER)LIKE USERID)OR(USERID='#'))
AND(UPPER(ATTRIBUTE)='#');
[回应] 2012-8-5 14:05:24 > 成功(1 row fetched)
[请求] 2012-8-5 14:05:24 > BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:1,NULL);END;
[回应] 2012-8-5 14:05:24 > 成功
```

## 4.9 完整的数据备份和还原操作

DAS 能够对 SQL 日志、运行期数据和策略中心的数据进行自动备份、手动备份、备份还原以及数据自动清理功能。

自动备份是周期性的对 SQL 日志、运行期数据和策略中心的数据进行备份，并且可以根据配置，将归档文件上传到 FTP 服务器并且设置上传成功后是否删除归档文件。同时要设置归档文件的保留天数，或占用文件系统比例（如 20%），如果超过该保留限制，则自动的删除最旧的归档文件。

手动归档需要指定事件发生时间段，根据时间段寻找符合条件的时间的事件文件进行归档。

## 4.10 多形式的告警方式

对于违反告警及审计规则的信息，系统提供了多形式的预警，包括通过手机短信、邮件、屏幕、以及 SYSLOG、SNMP 等发送到日志审计平台或其它相应的网管中心平台。根据风险等级的不同，采取不同的告警方式。

## 4.11 全面系统管理能力

### 1.1.1 系统配置管理

DAS 提供 WEB 管理页面，数据库安全管理员在不需要安装任何客户端软件的情况下，基于标准的浏览器即可完成对 DAS 的相关配置管理，主要包括网络管理、容灾管理、安全管理、数据库和审计实例管理等。

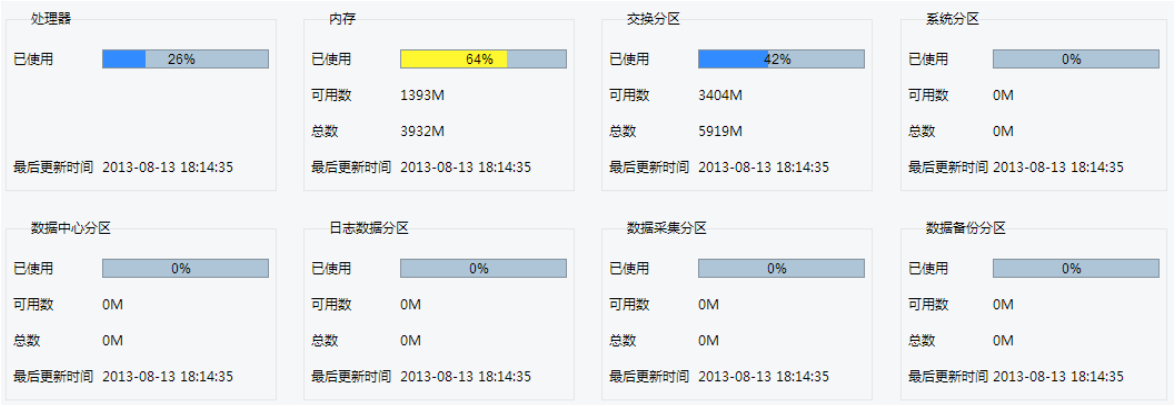
### 1.1.2 系统日志审计

提供针对审计设备自身的操作日志进行详细记录，满足相关法令规范要求。

### 1.1.3 系统状态查询和审计

DAS 系统能够接收本系统以及其它第三方服务系统通过 syslog、trap 等方式发送过来的系统状态信息。用户无需使用客户端软件即可发现审计设备的系统资源、引擎状态进行监测，对发现问题的内容提供便利。

资源监控情况：



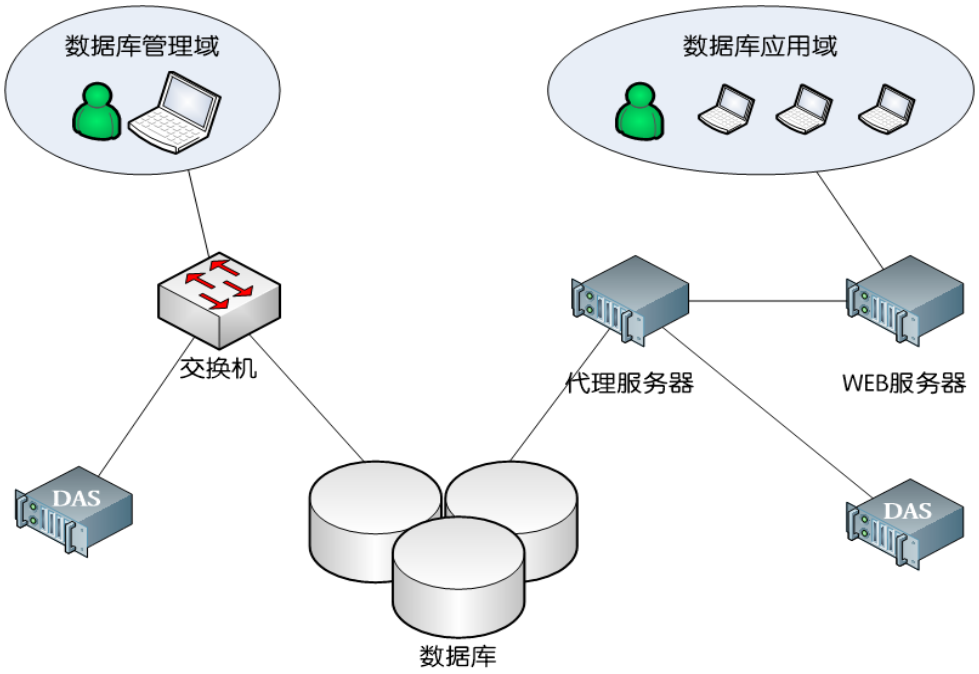

引擎监控情况：


# 五. 典型部署模式

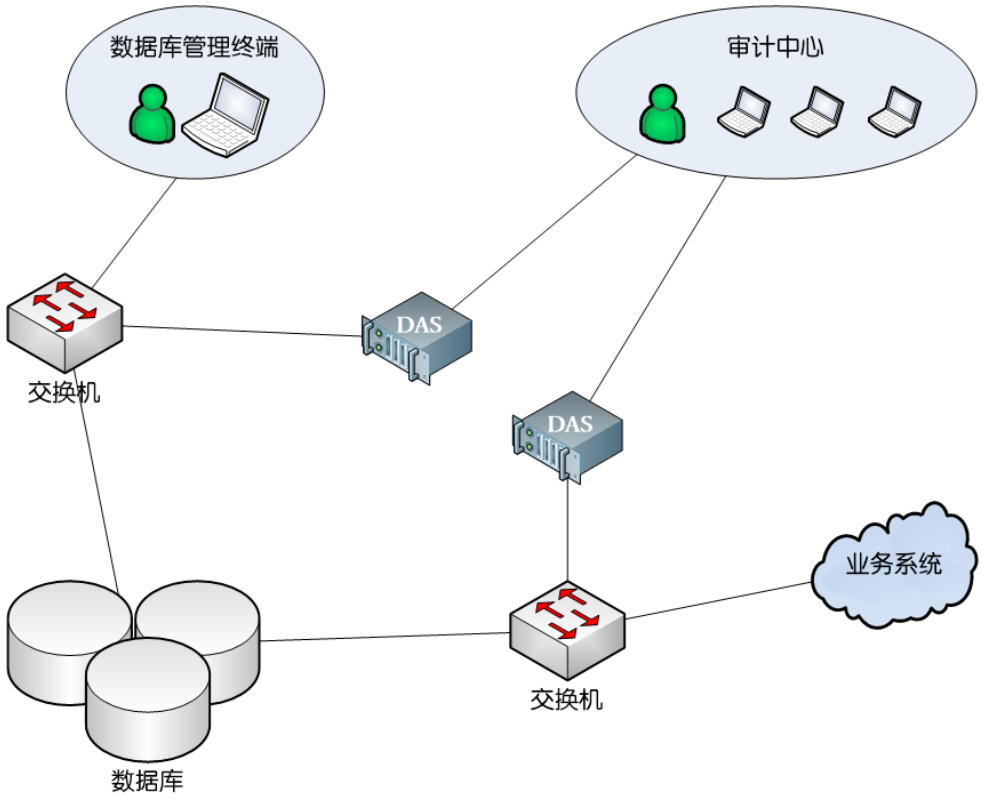
## 5.1 旁路模式

DAS 在旁路模式下，通过端口镜像、网络嗅探器、集线器、TAP 等，达到将访问被保护数据库的流量复制一份到 DAS 审计服务器上。另外，还有一种特殊的旁路模式，是在客户端到被保护数据库链路上的堡垒机或者代理服务器上，通过 TCP/IP 协议探测形式，将获取的数据包信息复制（发送）一份到与堡垒机并行的审计服务器上。

DAS 在旁路模式下的网络拓扑图如下所示：



## 5.2 多级部署模式




系统支持对多个数据库审计节点的集中审计管理，能够实现复杂网络环境下的数据库操作审计。

DAS 的多级部署中，各个“探针点”负责记录和分析对数据库的操作信息以及数据库的响应，将这些数据发送给审计中心。而审计中心负责汇集所有“探针点”捕获的信息，存储并管理 log 文件，生成各种审计报表和合规性报告，同时提供接口负责与第三方系统的“整合”处理。此外，DAS 管理员可以通过审计中心管理、配置安全控制和审计策略和模式。在多极部署模式下，一个审计中心可以收集多台审计设备的信息，在审计中心完成审计信息的存储、告警和分析。