UNIS D2000-G系列数据库审计系统

用户FAQ

目 录

本文档介绍 D2000-G20 产品的用户常见问题及解答。

1 硬件类 FAQ

D2000-G20

D2000-G20 标配支持多达 16 个千兆以太口，同时可以通过选配接口板将整机接口数量扩展到 48 个千兆以太口或 16 个千兆以太口和 8 个万兆以太光口。

设备主控板上有 8 个 10/100/1000BASE-T 自适应以太网电口、8 个 1000BASE-X 以太网光口、2 个 USB 接口和 1 个 Console 接口。具体结构如图 1 所示。

图1 D2000-G20

2 售前 FAQ

什么是数据库审计？

以某种方式记录数据库的操作行为。系统采用的是旁路接入方式，其他还包括串联在线式，旁路+软探针式，数据库日志抽取式。

为什么数据库自身都有审计日志，还需要我们的什么产品？

- 数据库自身开启完整的日志记录将非常影响性能，极端情况下会消耗 40%左右的服务器性能。
- 不能对指定的操作行为进行预警。
- 在出现安全事件时，数据库自身记录的日志属于删除的重点对象。
- 在许多法律法规中要求第三方的日志记录工具。

能发现什么？不能发现什么？

因为我们采用的是旁路接入的方式，所以只能记录通过网络传输且不加密的流量。比如通过数据库工具对数据库的操作，那么我们能完整的记录；而如果是通过远程桌面的方式对数据库的操作就无法记录。记录内容包括：存储过程、绑定变量、库、表、字段、数据库用户名、主机名、IP、MAC、语句执行时长。

数据库审计能做什么？

就目前的产品我们能实现以下内容：

- 业务审计（医院就是防统方）。
- 运维审计（全审计）。
- 安全审计（比如特权账号）。
- 辅助决策（性能分析）。
- 行为审计（如 telnet）。

什么是业务审计？

交通违章的删除，涉及数据库的删除操作；医院的统方，涉及数据库的查询操作；国土土地申报系统数据的修改，涉及修改操作；财政系统颁发会计证，涉及数据库的增加操作。不难看出以上的操作涉及了数据库的增删改查，这些操作不会对数据库的安全产生任何影响，但实际上却对用户的业务带来了巨大的风险。

针对业务审计我们有哪些案例？

- 举不胜举的统方案例。
- 厦门某医院收费费率被修改。
- 财政的手工平账，申请金额与审批金额建立关联审计。
- 土地报批系统的恶意错误与竞争性删除。
- 某些业务审计涉及客户秘密不一一列举。

业务审计从何入手

- 前期先了解有哪些业务。
- 问用户业务上关心什么。
- 哪些流程需要审批。
- 哪些数据是敏感的。
- 亲自了解一下业务系统。

用户需要三层关联怎么办？

- 引导用户是关键业务操作的关联，不是所有操作的关联。

- 如果需要全部操作的关联，1 实际意义不大，大量的关键信息被无用的操作所淹没；2 费用很高。
- 具体实现找技术人员详细了解。

有什么优势？

- 全审计。
- 针对不同 HIS 系统专属的防统方规则。
- 积累沉淀的数据库安全运维策略。
- 每天上亿级数据量下的快速查询。
- 明晰的实时数据分析功能。
- 准确的数据库语句翻译。
- 提供可直接提交安全报告。
- 具有强大的技术力量为用户提供数据分析挖掘服务。
- 富有技术底蕴的相似度语句。

3 售后 FAQ

为什么管理界面中有的内容显示不出来？

浏览器兼容性问题，请选择高版本火狐浏览器。

产品升级需要做哪些步骤？

- 获得合适的产品升级包。
- 和厂家制订好升级失败的处置方案，跟相关部门单位协商获得升级时间窗口。
- 在非业务繁忙期，通过管理页面将升级包上传在线升级。
- 升级成功，清空浏览器缓存，登录验证升级版本是否正确。

为什么在使用过程中突然无法访问？

- 可否 ping 通。
- 查看本机到设备的管理网络是否可达。
- SSH 50000 端口是否被重置？如果被重置说明系统高负载奔溃了，该现象已极少出现。
- 请尝试重启设备，需等待若干时间，系统可能处于数据库修复中。

为什么在实时语句中查看不到数据？

- 监听配置没有配置，填写监听配置；如果配置了，检查配置端口与 ip 是否正确。
- 检测是否勾选了网卡监听、监听服务是否正常使用。
- 系统时间与审计系统时间不一样，建议校正一下审计系统的时间。

- 确认交换机的镜像端口是否正常。

在事件查看页面选择某一条记录点击事件追踪，展示出来的是没有语句内容的空页面？

该事件刚刚生成，其他信息还未入库，稍微等待（2-3 秒）一会儿刷新即可。

查看修改的配置内容，发现没有更新？

系统采用多标签页的方式，修改内容保存后，页面未进行刷新，显示的还是未保存的内容，只要刷新下页面，或者关闭页面重新打开，就可以看到更新后的内容。

页面展示的数据中包含乱码？如解析内容中出现“？”“TT”等

该现象正常，属于协议包中的数据，并非用户输入的内容。

触发规则的事件不能正常对外告警（邮件、syslog等）

数据流是否正常，ids 是否正常运行，规则是否添加成功，规则内容是否正确，如均正常，请联系开发人员。

根据页面展示的语句来配置规则时，直接复制语句来配置规则不生效？

根据页面展示的语句来配置规则时，会有可能因为页面展示的语句与真实原始语句存在差异（标点符号、特殊字符前后为美观而添加了空格），直接复制语句来配置规则可能导致匹配不成功。

例如原始语句是 select value from v$sesstat where sid = :sid order by statistic#

页面显示为 SELECT value FROM v$sesstat WHERE sid = : sid ORDER BY statistic#

差别在: sid，原始语句是没用中间的空格的，而展示在页面上为了展示效果有，暂时没有解决方案，配置规则时，请避免在规则内容中添加标点符号和特殊字符。