

UNIS D2000-G2 系列数据库审计系统

故障处理手册

目 录

1 简介	1
1.1 故障处理注意事项	1
1.1 收集设备运行信息	1
2 硬件类故障处理	3
2.1 设备出现死机问题	3
3 数据库故障处理	4
3.1 数据库损坏问题	4
3.2 登录时提示“设备时间不对”	4
4 升级故障处理	5
4.1 升级文件不合法问题	5
4.2 升级失败	5
5 监听服务故障处理	5
5.1 监听服务停止	5
6 审计故障处理	6
6.1 审计不到任何数据问题	6
7 审计查询故障处理	6
7.1 实时查询无数据的问题	6
7.2 查询显示“暂无数据”的问题	7
7.3 查询超时的问题	7
8 规则故障处理	7
8.1 有满足规则的语句记录，但不触发告警的问题	7
9 告警通知故障处理	8
9.1 接收不到任何告警通知的问题	8

1 简介

本文档介绍 UNIS 数据库审计系统软、硬件常见故障的诊断及处理措施。

1.1 故障处理注意事项

- 请务必确定使用的浏览器为火狐浏览器。
- 更换和维护设备部件时，请佩戴防静电手腕，以确保您和设备的安全。
- 设备正常运行时，建议在完成重要功能的配置后，及时备份配置，以便设备出现故障后能迅速恢复。
- 设备出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），搜集信息越全面、越详细，越有利于故障的快速定位。
 - 根据实际情况检查镜像流量。
 - 记录具体的故障现象、故障时间、配置信息。
 - 记录完整的网络拓扑。
 - 记录现场采取的故障处理措施（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
 - 记录故障处理过程中使用的所有串口命令行显示信息。
 - 搜集设备的日志信息、DEBUG 信息。
 - 记录设备故障时电源、硬盘、风扇指示灯的状态，或给现场设备拍照记录。

1.1 收集设备运行信息



说明

设备运行过程中会产生日志信息、系统 DEBUG 信息，并且有捕获监听流量等方式，协助判断异常原因。

表1-1 设备运行信息介绍

分类	获取方式	内容
日志信息	使用默认的sec、sys、audit账户登录来查看日志；	运行日志、操作日志
系统DEBUG信息	在审计设备的API列表中选择“系统DEBUG信息点击下载”	系统负载和启动时间,内存占用,磁盘信息,网卡插拔记录,TOP,网卡信息,网络链接信息,网卡实时数据,系统启动信息,数据库日志,sph日志,捕包引擎,apache日志,前后台调用日志,OTHER其他信息
设备网络捕包	在审计设备的API列表中选择“设备网络捕包”	捕获审计设备监听口流量，确认流量是否有问题

1.1.1 系统日志

使用 **sys** 账户登录，至“系统配置”-“运行日志”页面，可查询指定范围的所有运行日志。

使用 **sec** 账户登录，至“系统配置”-“操作日志”页面，可查询指定范围的 **audit** 账户的操作日志。

使用 **audit** 账户登录，至“系统配置”-“运行日志”页面，可查询指定范围的 **sec**、**sys** 账户的操作日志。

图1-1 系统日志



时间	日志类型	日志信息	行为	操作者	登录IP
2017-12-26 16:51:07	配置修改	修改报警级别响应策略成功	修改报警级别为高可疑的响应策略为: syslog.snmp.windowsms.mail	sec	10.4.8.117
2017-12-26 16:42:11	配置修改	设置邮件服务器成功	设置邮件服务器地址: smtp.163.com, 端口: 25, 发件人: sunyh@heidun.net, 收件人: sunyh@heidun.net	sec	10.4.8.117
2017-12-26 16:41:02	用户登录	登录系统成功	登录用户名为: sec	sec	10.4.8.117
2017-12-26 16:40:58	用户退出	用户退出系统	退出用户名为: sys	sys	10.4.8.117
2017-12-26 16:26:00	配置修改	添加地址池成功	添加地址池地址p列表	sys	10.4.8.117
2017-12-26 16:24:54	配置修改	修改系统日志策略成功	修改日志级别为用户登录的响应策略为: syslog.snmp.mail.windowsms	sys	10.4.8.117
2017-12-26 16:02:44	配置修改	修改系统日志策略成功	修改日志级别为配置修改的响应策略为: syslog.snmp.mail.windowsms	sys	10.4.8.117
2017-12-26 16:02:17	配置修改	修改系统日志策略成功	修改日志级别为用户登录的响应策略为: syslog.snmp.mail.windowsms	sys	10.4.8.117
2017-12-26 16:02:09	配置修改	修改系统日志策略成功	修改日志级别为配置修改的响应策略为: syslog.snmp.mail.windowsms	sys	10.4.8.117
2017-12-26 16:01:56	用户登录	登录系统成功	登录用户名为: sys	sys	10.4.8.117
2017-12-26 16:01:52	用户退出	用户退出系统	退出用户名为: sec	sec	10.4.8.117
2017-12-26 16:01:50	配置修改	修改报警级别响应策略成功	修改报警级别为高可疑的响应策略为: syslog.snmp.windowsms.mail	sec	10.4.8.117
2017-12-26 16:01:41	配置修改	设置SNMP配置成功	设置snmp库的IP: 10.4.8.117, 端口: 162, 版本: 1, 团体名: public	sec	10.4.8.117
2017-12-26 16:01:25	配置修改	设置邮件服务器成功	设置邮件服务器地址: smtp.163.com, 端口: 25, 发件人: sunyh@heidun.net, 收件人: sunyh@heidun.net	sec	10.4.8.117
2017-12-26 16:00:45	配置修改	设置邮件服务器成功	设置邮件服务器地址: smtp.qq.com, 端口: 25, 发件人: sunyh@heidun.net, 收件人: sunyh@heidun.net	sec	10.4.8.117

1.1.2 DEBUG 信息

在浏览器地址栏中输入 **https://设备 IP/API** 访问审计的 **API** 页面。

图1-2 API 列表

系统API列表

设备网络捕包

数据库维护

系统DEBUG信息 点击下载

工号与处方查询分析

内置报表配置

SQLSERVER二次规则匹配

选择“系统 **DEBUG** 信息 点击下载”，收集设备所有类别的调试日志信息。

1.1.3 设备网络捕包

在 API 页面中，选择“设备网络捕包”，填写认证码“tcpdump”后进入捕包页面。

图1-3 捕包

请根据实际情况选择网卡、目标主机 IP、协议类型、目标主机端口、捕包大小，为保证捕包的完整性，请先停止审计设备的进程，最后点击“开始捕包”。

注意事项：该页面捕包的捕包数目上限为 3 个，包的大小为设置的捕包大小，请在完成捕包下载后，清空捕包目录，并启动审计设备进程，保证设备的正常运行。

2 硬件类故障处理

2.1 设备出现死机问题

2.1.1 故障描述

Web 页面和后台设备都不能访问，设备出现死机状态。

2.1.2 故障处理步骤

设备出现死机的时候请按照以下步骤检查：

- (1) 硬盘指示灯 HDD 是否闪烁；
- (2) 网卡指示灯是否闪烁；
- (3) 电源指示灯是否正常；
- (4) 串口是否能正常连接；

- (5) 串口连接上是否有错误日志输出；
- (6) 直连管理口是否能 ping 通管理口地址；
- (7) 直连备用口是否能 ping 通 1.0.0.1；
- (8) 设备连接显示屏和键盘，是否有错误打印，是否能正常交互；
- (9) telnet 测试 443 端口是否能连接上；
- (10) 设备是否异常报警声音；
- (11) 请将以上信息全部记录下来，如果串口、管理口直连都无任何反应，请将电源线拔掉等待大约 1 分钟，再插上电源线对设备进行硬重启，重启过程中建议连接显示屏，并观察重启过程中是否有错误信息输出，随时拍照记录；
- (12) 如果操作以上步骤后系统不能正常启动，请联系代理商或当地技术工程师进行处理，并提供记录的信息给他们。

3 数据库故障处理

3.1 数据库损坏问题

3.1.1 故障描述

在 Web 管理界面操作时，提示如下信息：

- (1) 系统硬盘损坏；
- (2) 数据库文件修复中；
- (3) 数据库没有启动。

3.1.2 故障处理步骤

- (1) 系统硬盘损坏：请联系代理商或当地技术工程师进行处理，更换硬盘，如果需要对历史数据进行查询，在保存归档备份数据的情况下，可通过“历史数据回档客户端”来查询历史数据；
- (2) 数据库文件修复中：一般由于异常断电等原因导致，请耐心等待修复完成；
- (3) 数据库没有启动：请联系代理商或当地技术工程师进行处理，并提供收集的 DEBUG 信息给他们。

3.2 登录时提示“设备时间不对”

3.2.1 故障描述

在系统登录页面，提示“设备时间不对”，且无法登录。

3.2.2 故障处理步骤

出现该提示，是因为设备时间在激活文件生效时间之前，需联系代理商或当地技术工程师进行确认和处理。

4 升级故障处理

4.1 升级文件不合法问题

4.1.1 故障描述

系统升级时，出现如下提示：

- (1) 失败，上传了非加密的升级包；
- (2) 失败，上传的升级包解压错误；
- (3) 失败，上传的升级包错误；
- (4) 上传文件大小不能超过 1G；
- (5) 上传的升级包应为.bin 文件。

4.1.2 故障处理步骤

- (1) 出现此问题，一般是因为下载时文件名被截断导致检测失败，或者选错非升级包文件进行上传导致的，请确认升级包是否正确，确认后重新上传升级包；
- (2) 如果升级还是失败，请向相关人员重新索要升级包。

4.2 升级失败

4.2.1 故障描述

升级结束后，页面提示“升级失败”，或再次访问设备时，弹出消息提醒“系统升级”。

4.2.2 故障处理步骤

- (1) 请在弹出的窗口中点击下载升级日志，或使用 sys 帐号登录，在“系统信息”页面，点击“查看日志”，查看升级过程的具体信息；
- (2) 需联系代理商或当地技术工程师，提供该升级日志进行确认和处理。

5 监听服务故障处理

5.1 监听服务停止

5.1.1 故障描述

在运行状态页面，发现监听服务为停止状态；

5.1.2 故障处理步骤

- (1) 请使用 audit 账户登录，至“系统管理”-“操作日志”页面，查看是否有用户操作停止服务；

- (2) 如果没有，使用 **sys** 账户登录，至“系统管理”-“进程管理”页面，点击“启动所有进程”或“重启服务”；
- (3) 如还是无法启动监听服务，或过段时间，又出现此情况且非人为操作，需联系代理商或当地技术工程师，提供系统 **DEBUG** 信息进行确认和处理。

6 审计故障处理

6.1 审计不到任何数据问题

6.1.1 故障描述

完成相关配置后，在实时语句查询中无查询结果。

6.1.2 故障处理

此问题一般是因为配置问题导致不能正常审计到数据。请按照如下操作检查处理：

- (1) 确认镜像流量是否正确（是否包含目标审计对象的双向流量）；
- (2) “策略中心”-“网络配置”页面中的监听网卡是否正常设置并接入镜像数据；
- (3) “策略中心”-“监听配置”页面中的各项配置是否按照实际情况正确配置；
- (4) “策略中心”-“监听配置”-“指定源 IP 审计”页面中的配置是否正确；
- (5) “运行状态”或者“进程管理”页面中的监听服务是否启动；
- (6) “策略中心”-“事件定义”页面中的规则中的规则动作是否设置为丢弃；
- (7) “审计中心”-“SQL 模板”页面中的 SQL 模板是否大量或者全部设置为“丢弃此类语句”。

如果检查以上步骤后，仍然审计不到数据，请联系代理商或当地技术工程师处理。

7 审计查询故障处理

7.1 实时查询无数据的问题

7.1.1 故障描述

“运行状态”有审计数据入库，但是在“实时查询”中查询不到数据。

7.1.2 故障处理步骤

此问题有可能是 2 种原因导致：

- (1) 数据量太大了，入库延时，请稍等一下，然后再查询。
- (2) 提供的查询项输入错误，不符合条件，请确认正确后再查询。

如果检查以上步骤后，仍然查询不到数据，请联系代理商或当地技术工程师处理。

7.2 查询显示“暂无数据”的问题

7.2.1 故障描述

进行实时查询或者历史查询时，弹出提示“暂无数据”。

7.2.2 故障处理

如果系统内确实无数据，是不会有提示的，显示暂无数据说明系统异常，请收集 DEBUG 信息并联系代理商或当地技术工程师处理。

7.3 查询超时的问题

7.3.1 故障描述

进行实时查询或者历史查询时，弹出提示：“查询超时”。

7.3.2 故障处理

出现此问题，一般是查询的数据量超量，导致查询超时。需修改查询条件，缩小查询范围，再进行查询。

8 规则故障处理

8.1 有满足规则的语句记录，但不触发告警的问题

8.1.1 故障描述

配置规则后，审计查询中有满足规则的语句记录，但没有触发该规则的告警。

8.1.2 故障处理步骤

规则没有被触发的原因比较多，遇到这种情况，请依次按照如下进行检查处理：

- (1) 规则是否配置正确，是否满足告警条件；
- (2) 查看该语句记录中是否有触发的其它规则，这种情况是由于不同的规则优先级不一样，触发了高级别的规则，将导致低级别的规则没有触发；
- (3) 确认 SQL 模板中是否有此类语句，并被设置为安全；
- (4) 检查系统当日触发的告警数量是否超过上限，如果超过规则告警上限，引擎就会不触发告警，每条规则每日被触发次数上限为 10000 条；
- (5) 确认该语句的 SQL 模板编号是否为 0（词法解析失败），默认情况下词法解析失败的 SQL 语句不会触发规则。

如按以上步骤操作后，仍然有问题，请联系代理商或当地技术工程师处理。

9 告警通知故障处理

9.1 接收不到任何告警通知的问题

9.1.1 故障描述

查看告警接收服务器，没有接收到任何告警。

9.1.2 故障处理

此问题一般是告警通知配置的问题，请按照以下步骤进行处理：

- (1) 检查是否正确配置日志响应和事件响应，如没有配置，即使有对应日志产生或对应规则触发，系统也不会发送告警通知；
- (2) 如果有配置日志响应和事件响应，请检查是否配置正确，包含告警通知的接收目标(邮箱、syslog 服务器、snmp 服务、windows message 服务等)是否配置正确；
- (3) 请检查对应的规则等级或日志分类是否已配置告警动作（snmp、syslog、邮件、windows message 等）。

如按以上步骤操作后，仍然有问题，请联系联系代理商或当地技术工程师处理。