文章
Nicky Zhu · 一月 18, 2021 阅读大约需 4 分钟

活用数据库审计日志跟踪数据操作

在最近的项目里，多方同时连接同一个数据库并执行增删改查等各项数据操作。研发人员不时发现一些数据在不合规的情况下被新增甚至删除。因此，在实际工作中会有监控数据操作以便识别和处理异常操作的需求。本文将以监控和识别删除操作为例，介绍如何通过IRIS的审计功能实现对数据操作的监控和查询。

注意事项

在应用审计功能之前，必须注意的是：
1. 开启审计功能会事无巨细地记录每一条对应的操作（如被执行的SQL），因此对于存储空间的需求将急剧增加。举例而言，仅开启对XDBCStatement的监控后，对于一张只由5个简单（整型，VARCHAR型）字段构成的表中插入100万条记录，在Audit数据库中将占用300～400MB的空间。在因业务所需确实需要开启审计功能时，必须预先分配更多磁盘空间给IRIS Audit数据库，并在审计功能开启期间定时巡检磁盘空间，避免因日志占满磁盘导致其他数据无法写入引发系统挂起的故障。
2. 在研发环境中多人、多单位需要连接数据库时，应为不同的开发者和数据来源分配独立的数据库账户和权限，避免多人共用超级账户，导致数据异常时难以追踪异常操作究竟从何而来。也就意味着为不同角色的开发、测试、用户等参与者开启独立的用户，分配各自所需的的数据库权限以及管理数据库账户这样一系列项目正常运行所依赖的实践并不能被审计功能所替代。在项目进展过程中，您更希望见到的，一定不是出现问题后再来跟踪问题和耽误工期，而是通过良好的协作规程和研发习惯减少非技术问题出现的概率。

IRIS中的审计功能

IRIS提供了
丰富的数据库审计功能
，用于记录从系统权限变更到数据删除的各类操作，用户可通过我们的**官方文档**查看系统支持的各类审计事件。
对于SQL操作而言，可用到的审计事件包括三大类：
- %System/%SQL/DynamicStatement 可捕获通过动态SQL执行的SQL操作
- %System/%SQL/EmbeddedStatement 可捕获通过嵌入式SQL执行的SQL操作
- %System/%SQL/XDBCStatement 可捕获通过第三方（JDBC/ODBC）SQL连接执行的SQL操作

开启数据库审计

1. 由于默认安装时IRISAUDIT数据库通常位于IRIS安装目录，空间有限，因此在需要开启审计时，应先将IRISAUDIT数据库从系统安装目录迁移到空间更充裕的数据库目录

2. 在System Administration -> Security -> Auditing -> Configure System Events下，开启对%System/%SQL/XDBCStatement的监控，如下图

以下是系统审计事件的列表:

过滤器: 页面大小: 0 最大行数: 1000 结果: 51 页面: 1 的 1

	事件名称	Enabled	Total	Written		
»	%Ensemble/%Message/ViewContents	是	7	7	重置	更改状态
	%Ensemble/%Production/ModifyConfiguration	是	12	12	重置	更改状态
	%Ensemble/%Production/StartStop	是	1	1	重置	更改状态
	%Ensemble/%Schema/Modify	是	0	0	重置	更改状态
	%System/%DirectMode/DirectMode	否	6	0	重置	更改状态
	%System/%Login/JobEnd	否	857	0	重置	更改状态
	%System/%Login/JobStart	否	492	0	重置	更改状态
	%System/%Login/Login	否	848	0	重置	更改状态
	%System/%Login/LoginFailure	是	0	0	重置	更改状态
	%System/%Login/Logout	否	16	0	重置	更改状态
	%System/%Login/TaskEnd	否	448	0	重置	更改状态
	%System/%Login/TaskStart	否	0	0	重置	更改状态
	%System/%Login/Terminate	否	2	0	重置	更改状态
	%System/%SMPExplorer/Change	否	0	0	重置	更改状态
	%System/%SMPExplorer/ExecuteQuery	否	0	0	重置	更改状态
	%System/%SMPExplorer/Export	否	0	0	重置	更改状态
	%System/%SMPExplorer/Import	否	0	0	重置	更改状态
	%System/%SMPExplorer/ViewContents	否	0	0	重置	更改状态
	%System/%SQL/DynamicStatement	否	348	0	重置	更改状态
	%System/%SQL/EmbeddedStatement	否	0	0	重置	更改状态
	%System/%SQL/PrivilegeFailure	否	0	0	重置	更改状态
	%System/%SQL/XDBCStatement	是	29	29	重置	更改状态
	%System/%Security/ApplicationChange	是	0	0	重置	更改状态
	%System/%Security/AuditChange	是	4	3	重置	更改状态
	%System/%Security/AuditReport	是	0	0	重置	更改状态
	%System/%Security/DBEncChange	是	0	0	重置	更改状态
	%System/%Security/DocDBChange	是	0	0	重置	更改状态
	%System/%Security/DomainChange	是	0	0	重置	更改状态
	%System/%Security/KMIPServerChange	是	0	0	重置	更改状态
	%System/%Security/LDAPConfigChange	是	0	0	重置	更改状态

vascript:zenPage.doChangeStatus('%25System%5C/%25SQL%5C/XDBCStatement')%3B

3.
预先配置好删除AuditLog的任务，以便在AuditLog过大时清除数据
系统虽然自带定时删除Audit数据库的任务，但其默认的触发条件为在Journal发生切换时才执行，因此不适用于需要扩展监控范围导致审计库将剧增的情况，应配置额外的任务便于随时执行。

并将其设置为按需启动

4.

待可疑操作发生时，使用SQL工具或portal在%SYS命名空间下运行如下SQL：

```
SELECT
ID, AuditIndex, Authentication, CSPSessionID, ClientExecutableName, ClientIPAddress,
Description, Event, EventData, EventSource, EventType, GroupName, JobId, JobNumber, N
amespace, OSUsername, Pid, Roles, RoutineSpec, Status, SystemID, UTCTimeStamp, UserIn
fo, Username
FROM %SYS.Audit
where Description = 'SQL DELETE Statement'
order by UTCTimeStamp desc
```

即可找到最近的删除操作。通过Truncate table或delete语句执行的操作均可由该日志捕获到。如需监控insert或update等操作，在上述Description字段的选择上加入对insert或update语句的筛选即可。
通过这些日志，可以查看到操作发生的时间，来源IP和数据库用户等信息，如下所示：

5. 必须再次提醒各位，一旦开启对语句的监控，Audit数据库会快速增长，需要每日甚至每日多次巡检，确保磁盘空间不会被占满导致系统崩溃。
   一旦发现Audit所在磁盘占有量过大（例如大于80%）或Audit库本身的占用过大（例如大于20G），即应运行步骤3中 配置的任务，然后对Audit库进行压缩和截断操作释放空间。

#API #数据转换语言（DTL） #错误处理 #监视 #SQL #数据库 #系统管理 #InterSystems IRIS

源URL: https://cn.community.intersystems.com/post/%E6%B4%BB%E7%94%A8%E6%95%B0%E6%8D%AE%E5%BA%93%E5%AE%A1%E8%AE%A1%E6%97%A5%E5%BF%97%E8%B7%9F%E8%B8%AA%E6%95%B0%E6%8D%AE%E6%93%8D%E4%BD%9C