**数据库防水坝分析报表**



**杭州美创科技有限公司**

**2021-09-01**

**目录**

[1.概述 3](#_Toc81498296)

[1.1时间范围 3](#_Toc81498297)

[1.2分析对象 3](#_Toc81498298)

[1.3主要内容 3](#_Toc81498299)

[2.SQL语句执行分析 4](#_Toc81498300)

[2.1登录失败的客户端IP分布(Top50) 4](#_Toc81498301)

[2.2操作类型分布 5](#_Toc81498302)

[2.3代码对象操作事件（TOP50） 5](#_Toc81498303)

[2.4危险操作访问事件 6](#_Toc81498304)

[2.5敏感SQL访问事件（TOP50） 6](#_Toc81498305)

[2.6执行次数排行TOP50 6](#_Toc81498306)

[2.7SQL语句数量变化趋势 7](#_Toc81498307)

[3.风险事件分析 7](#_Toc81498308)

[3.1目标风险分析（TOP10） 8](#_Toc81498309)

[3.2风险内容分析（TOP10） 9](#_Toc81498310)

[3.3风险发生时间趋势分析 10](#_Toc81498311)

# 1.概述

## 1.1时间范围

本次监测周期为2020年12月1日 - 2020年12月31日期间（以下简称为本期）。

## 1.2分析对象

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 数据库名称 | 数据类型 | 数据库IP与端口 |
| 1 | 测试数据库1 | Oracle | 192.168.1.1:1521 |
| 2 | 测试数据库2 | RdsMysql | 192.168.1.1:3306 |
| 3 | 测试数据库3 | Sqlserver | 192.168.1.1:1433 |

## 1.3主要内容

本报告从SQL语句执行、风险事件角度对数据库进行综合分析。总体概况如下：

SQL语句：共执行了SQL语句0条，约0.00条/天，0.00条/分。其他主要指标如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DDL操作数量** | **DML操作数量** | **执行失败数量** | **账号个数** | **客户端IP个数** | **客户端工具个数** |
| 1 | 1 | 1 | 1 | 1 | 1 |

风险事件：总告警次数0.1万，频率0.00万次/天。其他主要指标如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **高风险次数（单位：万）** | **中风险次数（单位：万）** | **低风险次数（单位：万）** | **最多告警的数据库** | **最多告警名称** | **最多告警的客户端IP** |
| 1 | 1 | 1 | db1 | name1 | 127.0.0.1 |

# 2.SQL语句执行分析

本章将根据SQL语句执行情况对数据库态势进行分析，SQL语句执行的总体情况如下：

## 2.1登录失败的客户端IP分布(Top50)

详细信息

|  |  |
| --- | --- |
| 客户端IP | 登录失败次数 |
| ip1 | 10 |
| ip1 | 15 |
| ip1 | 20 |
| ip1 | 30 |
| ip1 | 40 |

## 2.2操作类型分布

详细信息

|  |  |
| --- | --- |
| **操作类型** | **语句数量** |
| Select | 10 |
| Logout | 20 |
| Login | 30 |
| Alter | 40 |
| Update | 50 |
| Insert | 123 |

## 2.3代码对象操作事件（TOP50）

|  |  |  |  |
| --- | --- | --- | --- |
| 客户端IP | 数据库名称 | SQL语句 | 次数 |
| ip1 | 测试数据库1 | select \* from t | 192 |
| ip2 | 测试数据库2 | select \* from t | 3306 |

## 2.4危险操作访问事件

详细信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 客户端IP | 规则名称 | 应用程序名 | 数据源名 | SQL语句 | 次数 |
| ip1 | 规则名称1 | 应用程序名1 | 测试数据库1 | select \* from t | 192 |
| ip2 | 规则名称2 | 应用程序名2 | 测试数据库2 | select \* from t | 3306 |

## 2.5敏感SQL访问事件（TOP50）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 排名 | 客户端IP | 数据库IP | 敏感SQL | 风险次数 |
| 1 | IP1 | IP1 | select \* from t | 192 |
| 2 | IP2 | IP2 | select \* from t | 3306 |

## 2.6执行次数排行TOP50

|  |  |  |
| --- | --- | --- |
| 排名 | SQL模板 | 执行次数 |
| 1 | select \* from t | 192 |
| 2 | select \* from t | 3306 |

## 2.7 SQL语句数量变化趋势

详细信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 时间 | SQL语句总量 | DDL操作数量 | DCL操作数量 | DML操作数量 | 执行失败数量 |
| 12月1日 | 12 | 192 | 12 | 12 | 12 |
| 12月2日 | 3306 | 12 | 12 | 12 | 12 |

# 3.风险事件分析

## 3.1目标风险分析（TOP10）

详细信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 目标 | 风险总数 | 高 | 中 | 低 |
| 1 | ip1 | 192 | 12 | 12 | 12 |
| 2 | ip2 | 12 | 12 | 12 | 12 |
| 3 | ip3 | 12 | 12 | 12 | 12 |

## 3.2风险内容分析（TOP10）

详细信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 风险内容 | 风险总数 | 高 | 中 | 低 |
| 1 | 新终端登陆 | 192 | 12 | 12 | 12 |
| 2 | 权限变更 | 12 | 12 | 12 | 12 |

## 3.3风险发生时间趋势分析

详细信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 时间 | 风险总数 | 高 | 中 | 低 |
| 4月1日 | 192 | 12 | 12 | 12 |
| 4月2日 | 12 | 12 | 12 | 12 |
| 4月3日 | 12 | 12 | 12 | 12 |
| 4月4日 | 12 | 12 | 12 | 12 |
| 4月5日 | 12 | 12 | 12 | 12 |