**ZL01新型数据安全治理赛参赛手册**

1. **赛题介绍**

|  |  |
| --- | --- |
| 序号 | 服务器名称 |
| 1 | 数据脱敏 |
| 2 | 敏感数据识别 |
| 3 | 数据备份 |
| 4 | 数据供给隔离 |
| 5 | 勒索病毒灾后有效恢复 |
| 6 | 数据安全共享 |

1. **赛题操作说明**
2. **赛题1：数据脱敏**

本题主要考察参赛选手按照给定脱敏规则对数据库中指定字段进行脱敏的能力。

1、服务器资源列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 用途 | IP地址 | 系统账号 |
| 1 | 数据库 | Oracle 库 | 192.168.1.100 | root/P@ssw0rd |

2、数据库信息列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 数据库服务名 | ORACLE\_SID | 数据库账号密码 |
| 1 | 数据库 | ORCLTT | ORCLTT | orcltt/orcltt |

3、赛题要求

按照下表要求对数据库中的数据进行脱敏。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 库 | 表 | 字段 | 要求 |
| 1 | orcltt | 个人联系信息 | Mobile | 值为手机号的：  替换最后四位数字 |
| 2 | orcltt | 合同基本信息 | ContractAmount | 全部匿名化: \*\*\*\*\*\*\*\*\*\* (10个\*) |
| 3 | orcltt | 交易对手信息 | Account | 替换为“100000” |
| 4 | orcltt | 金额信息 | CTCurrency | 值为“人民币”的：  替换为“元”;  其他值的：  替换为“其他” |

1. **赛题2：敏感数据识别**

本题主要考察参赛选手识别数据库中指定敏感类型的字段能力。

1. 服务器资源列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 用途 | IP地址 | 系统账号 |
| 1 | 数据库 | Oracle 库 | 192.168.1.100 | root/P@ssw0rd |

2、数据库信息列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 数据库服务名 | ORACLE\_SID | 数据库账号密码 |
| 1 | 数据库 | ORCLTT | ORCLTT | orcltt/orcltt |

3、赛题要求

考察使用各种算法匹配记录的能力。对数据库中涉及下表列出的敏感类型的数据进行识别操作，并将每种敏感类型数据的识别规则相关信息记录在操作机桌面上的《ZL02敏感数据识别结果表》中（字段中混杂错误数据，错误数据在30%以内）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **敏感**  **类型** | **数据**  **库名** | **表名** | **字段名** | **识别规则**  **（正则/字典/无规律）** | **正则表达式** | **字典** |
| 用户  ID | DB | Table | ID | **正则** | **[A-Za-z]{6}\d{6}** | **/** |
| 地址 | DB | Table | Address | **无规律** | **/** | **/** |
| 性别 | DB | Table | gender | **字典** | **/** | **男|man|male|女|woman|female** |

注：上表内容仅为示例，非考试内容，敏感类型、数据库名、表名、字段名已提供，选手仅需填写表格中的识别规则、正则表达式、字典三列内容。

1. **赛题3：数据备份**

本题主要考察参赛选手备份、恢复数据库的能力。

1. 服务器资源列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 用途 | IP地址 | 系统账号 |
| 1 | 数据库A | Oracle A库 | 1.1.1.100 | root/P@ssw0rd |
| 2 | 数据库B | Oracle B库 | 1.1.1.101 | root/P@ssw0rd |
| 3 | 备份管理服务器 | 备份管理 | 192.168.1.100 | root/P@ssw0rd |
| 4 | 备份介质服务器 | 备份介质 | 1.1.1.202 | root/P@ssw0rd |

2、数据库信息列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 数据库服务名 | ORACLE\_SID | 数据库账号密码 |
| 1 | 数据库A | ORCLTT | ORCLTT | orcltt/orcltt |
| 2 | 数据库B | ORCL\_primary | ORCL | orcltt/orcltt |

3、赛题要求

（1）分别将1、2号两台主机的数据库备份至4号主机；

（2）将1号主机的备份数据，恢复到2号主机的数据库中；

（3）将2号主机的备份数据，恢复到1号主机的数据库中；

（4）完成比赛。

1. **赛题4：数据供给隔离**

本题主要考察参赛选手共享不同网段数据库中数据的能力。

1. 服务器资源列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 用途 | IP地址 | 系统账号 |
| 1 | 数据库A | Oracle A库 | 1.1.1.100 | root/P@ssw0rd |
| 2 | 数据库B | Oracle B库 | 192.168.1.200 | root/P@ssw0rd |
| 3 | 服务器 | 数据管理 | 1.1.1.201/  192.168.1.201 | root/P@ssw0rd |

2、数据库信息列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 数据库服务名 | ORACLE\_SID | 数据库账号密码 |
| 1 | 数据库A | ORCLTT | ORCLTT | orcltt/orcltt |

3、赛题要求

（1）1号、2号主机在不同的网段，将1号主机的数据库，共享给2号主机；

（2）启动2号主机的数据库；

（3）完成比赛。

1. **赛题5：勒索病毒灾后有效恢复**

本题主要考察参赛选手在生产环境被勒索病毒感染后，恢复生产数据库的能力。

1. 服务器资源列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 用途 | IP地址 | 系统账号 |
| 1 | 数据库服务器 | Oracle 库 | 1.1.1.100 | root/P@ssw0rd |
| 2 | 数据库  验证服务器 | Oracle 库 | 192.168.1.200 | root/P@ssw0rd |
| 3 | 备份服务器 | 数据备份管理 | 1.1.1.201/  192.168.1.201 | root/P@ssw0rd |

2、数据库信息列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 数据库服务名 | ORACLE\_SID | 数据库账号密码 |
| 1 | 数据库服务器 | ORCLTT | ORCLTT | orcltt/orcltt |

3、赛题要求

（1）定时备份1号主机的数据库至3号主机数据库（备份频率自己设计）；

（2）开始答题后的40分钟内，平台将自动模拟1号主机的数据库感染毒；

（3）参赛选手需编写SQL脚本验证1号主机数据库是否感染病毒；发现1号主机数据库感染病毒后，参赛选手需对3号主机的备份数据进行恢复、排查病毒感染情况；

（4）参赛选手需选择3号主机中最新的一份安全数据，恢复或挂载到2号主机，并启动数据库。

完成比赛

1. **赛题6：数据安全共享**

本题主要考察参赛选手在保证数据安全的要求下，从生产环境安全共享数据到开发测试环境的能力。

1. 服务器资源列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 用途 | IP地址 | 系统账号 |
| 1 | 生产服务器 | Oracle 库 | 1.1.1.100 | root/P@ssw0rd |
| 2 | 数据服务器 | 数据管理 | 1.1.1.201 | root/P@ssw0rd |
| 3 | 数据存储服务器 | 数据存储池 | 1.1.1.202 | root/P@ssw0rd |
| 4 | 脱敏服务器 | 脱敏软件 | 1.1.1.203 | root/P@ssw0rd |
| 5 | 脱敏用数据库 | 脱敏库 | 1.1.1.101 | root/P@ssw0rd |
| 6 | 开发测试用库 | 开发测试库 | 1.1.1.102 | root/P@ssw0rd |

2、数据库信息列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务器名称 | 数据库服务名 | ORACLE\_SID | 数据库账号密码 |
| 1 | 生产数据库 | ORCLTT | ORCLTT | orcltt/orcltt |

3、赛题要求

（1）在2号主机部署数据管理软件，利用3号主机作为存储池；

（2）在4号主机部署脱敏软件；

（3）获取1号主机的数据库数据，挂载或共享到5号主机，并启动数据库。按如下要求进行数据脱敏：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 库 | 表 | 字段 | 要求 |
| 1 | orcltt | 个人联系信息 | Mobile | 全部匿名化: \*\*\*\*\*\*\*\*\*\*\*(11个\*) |
| 2 | orcltt | 合同基本信息 | Currency | 全部匿名化:  \*\*\*\*\*\*\*\*\*\* (10个\*) |
| 3 | orcltt | 交易对手信息 | CustomerName | 全部匿名化:  \*\*\*\*\*\*\*\*\*\* (10个\*) |
| 4 | orcltt | 金额信息 | CTAccount | 全部匿名化:  \*\*\*\*\*\*\*\*\*(9个\*) |

（4）将脱敏后的数据，挂载或共享到6号主机，并启动数据库；

（5）完成比赛。

1. **评分细则**

|  |  |  |  |
| --- | --- | --- | --- |
| **赛题** | **计分项** | **计分项说明** | **总分** |
| 1 | 数据脱敏准确率 | 正确脱敏的字段数/待脱敏的数据字段总数\*100分  注：一个字段内的所有数据准确脱敏视为答对，否则视为打错不计入得分 | 100分 |
| 2 | 敏感字段识别率 | 正确识别的敏感字段数/待识别的敏感字段总段\*100分 | 100分 |
| 3 | 1号主机数据库成功恢复数据到2号主机 | 恢复成功，且与1号主机数据库数据相同得50分，  未恢复或数据恢复不准确得0分 | 50分 |
| 2号主机数据库成功恢复数据到1号主机 | 恢复成功，且与2号主机数据库数据相同得50分，  未恢复或数据恢复不准确得0分 | 50分 |
| 4 | 完成数据供给 | 供给数据库可用，且与1号主机数据库数据相同得100分；  供给数据库不可用，或与1号主机数据库数据不相同得0分 | 100分 |
| 5 | 成功恢复安全数据 | 验证数据库可用，且与生产数据库数据相同，得50分；  验证数据库不可用，或与生产数据库数据不同，得0分 | 50分 |
| 安全数据与中毒操作的  时间间隔 | 时间间隔：小于5分钟，得50分；  时间间隔：5~20分钟，得25分；  时间间隔：大于20分钟，得0分 | 50分 |
| 6 | 成功共享数据到  开发测试库 | 开发测试库可用，且数据库完整，得50分；  开发测试库不可用，或数据库不完整，得0分 | 50分 |
| 按要求数据脱敏 | 正确脱敏的字段数/待脱敏的数据字段总数\*50分 | 50分 |