|  |  |
| --- | --- |
|  | **2021** |
|  |  |

|  |  |
| --- | --- |
| **测试用例** | |
|  |  |
|  | |

密级：内部

|  |
| --- |
| 适用范围：华夏数据库V7 |

送检单位：华夏银行（北京）科技有限公司

**版权声明**

本文档归华夏银行（北京）科技有限公司（简称“华夏银行”）版权所有，并保留对本手册及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外,其著作权或其他相关权利均属于华夏银行（北京）科技有限公司。未经华夏银行（北京）科技有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。本文档中的信息归华夏银行（北京）科技有限公司所有并受著作权法保护。

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。华夏银行公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但华夏银行公司不对本手册中的遗漏、不准确或错误导致的损失和损害承担责任。

信息更新

本文档及其相关资料（以下文中称为“文档”）仅用于为最终用户提供信息，并且随时可由华夏银行更改或撤回。

出版时间

本文档于2021年5月由华夏银行（北京）科技有限公司编写。

**文档修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 日期 | 修订者 | 修订说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1. 华夏数据库安全性功能性测试 5](#_Toc20062995)

[1.1. 数据库防火墙功能测试原理图 5](#_Toc20062996)

[1.2. 数据库防火墙功能测试 6](#_Toc20062997)

[1.2.1. 测试场景1 6](#_Toc20062998)

[1.2.2. 测试场景2 9](#_Toc20062999)

[1.2.3. 测试场景3 11](#_Toc20063000)

[1.2.4. 测试场景4 13](#_Toc20063001)

[1.2.5. 测试场景5 15](#_Toc20063002)

[1.2.6. 测试场景6 17](#_Toc20063003)

[1.2.7. 测试场景7 19](#_Toc20063004)

[1.2.8. 测试场景8 21](#_Toc20063005)

[1.2.9. 测试场景9 22](#_Toc20063006)

[1.2.10. 测试场景10 26](#_Toc20063007)

[1.2.11. 测试场景11 29](#_Toc20063008)

[1.2.12. 测试场景12 31](#_Toc20063009)

[1.2.13. 测试场景13 33](#_Toc20063010)

[1.2.14. 测试场景14 35](#_Toc20063011)

[1.2.15. 测试场景15 37](#_Toc20063012)

[1.2.16. 测试场景16 38](#_Toc20063013)

[1.3. 数据库动态脱敏功能测试 40](#_Toc20063014)

[1.3.1. 使用“partial”函数及pattern方式脱敏 40](#_Toc20063015)

[1.3.2. 使用“partial”函数脱敏 41](#_Toc20063016)

[1.3.3. 使用“random”函数脱敏 43](#_Toc20063017)

[1.4. 数据库动态加密功能测试 45](#_Toc20063018)

[1.4.1. 使用“aes”函数加密 45](#_Toc20063019)

[1.4.2. 使用“SM4”函数 CBC加密 46](#_Toc20063020)

[1.4.3. 使用“SM4”函数 CFB加密 48](#_Toc20063021)

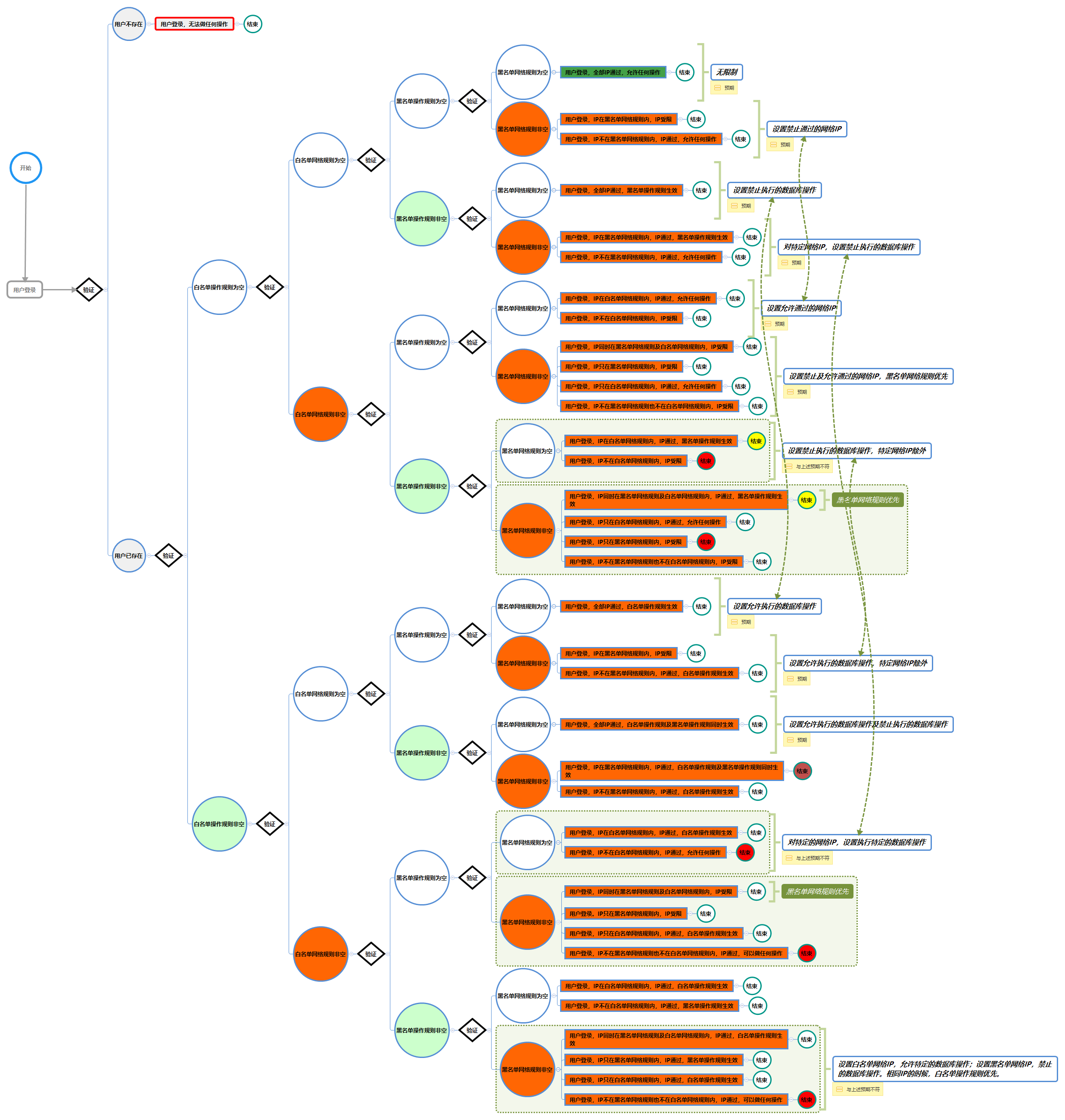
[1.5. 数据库加密访问功能测试 50](#_Toc20063022)

[1.5.1. 数据库通信加密 50](#_Toc20063023)

[1.5.2. 数据库安全防护通信加密 60](#_Toc20063024)

# 华夏数据库安全性功能性测试

## 数据库防火墙功能测试原理图



数据库安全访问控制从用户权限维、SQL操作维、网络访问权限维、黑名单、白名单五个维度进行安全访问控制。

## 数据库防火墙功能测试

### 测试场景1

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.1 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景1 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、配置白名单网络规则、配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行白名单内操作 | 否 | 否 | | 2 | 白名单内IP，执行白名单外操作 | 是 | 是 | | 3 | 黑名单内IP，执行黑名单内操作 | 是 | 是 | | 4 | 黑名单内IP，执行黑名单外操作 | 否 | 否 | | 5 | 黑名单内IP与白名单内IP相同，执行白名单内操作与黑名单内操作 | 白名单否  黑名单是 | 白名单否  黑名单是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图：      用例4截图：      用例5截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景2

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.2 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景2 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、配置白名单网络规则、配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行白名单内操作 | 否 | 否 | | 2 | 白名单内IP，执行白名单外操作 | 是 | 是 | | 3 | 白名单外IP，执行黑名单内操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景3

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.3 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景3 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、配置白名单网络规则、不配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行白名单内操作 | 否 | 否 | | 2 | 白名单内IP，执行白名单外操作 | 是 | 是 | | 3 | 黑名单内IP，执行操作 | 是 | 是 | | 4 | 黑名单内IP与白名单内IP相同，执行白名单内操作与黑名单内操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图：      用例4截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景4

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.4 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景4 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、配置白名单网络规则、不配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行白名单内操作 | 否 | 否 | | 2 | 白名单内IP，执行白名单外操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景5

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.5 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景5 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、不配置白名单网络规则、配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 黑名单内IP，执行黑名单内操作 | 是 | 是 | | 2 | 黑名单内IP，执行非黑非白的操作 | 是 | 是 | | 3 | 黑名单外IP，执行白名单外操作 | 是 | 是 | | 4 | 黑名单外IP，执行白名单内操作 | 否 | 否 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图：      用例4截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景6

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.6 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景6 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、不配置白名单网络规则、配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 任意IP，执行白名单内操作 | 否 | 否 | | 2 | 任意IP，执行白名单外操作 | 是 | 是 | | 3 | 任意IP，执行黑名单内操作 | 是 | 是 | | 4 | 任意IP，执行黑名单外操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图：      用例4截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景7

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.7 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景7 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、不配置白名单网络规则、不配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 黑名单内IP，执行操作 | 是 | 是 | | 2 | 黑名单外IP，执行白名单内操作 | 否 | 否 | | 3 | 黑名单外IP，执行白名单外操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景8

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.8 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景8 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：配置白名单操作内容、不配置白名单网络规则、不配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 任意IP，执行白名单内操作 | 否 | 否 | | 2 | 任意IP，执行白名单外操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景9

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.9 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景9 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、配置白名单网络规则、配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行操作 | 否 | 否 | | 2 | 黑名单内IP，执行操作 | 是 | 是 | | 3 | 非黑非白名单IP，执行任意操作 | 是 | 是 | | 4 | 白名单内IP与黑名单内IP相同，执行操作与黑名单内操作 | 白名单否  黑名单是 | 白名单否  黑名单是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图：      用例4截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景10

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.10 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景10 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、配置白名单网络规则、配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行黑名单内操作 | 是 | 是 | | 2 | 白名单内IP，执行黑名单外操作 | 否 | 否 | | 3 | 白名单外IP，执行操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景11

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.11 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景11 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、配置白名单网络规则、不配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行操作 | 否 | 否 | | 2 | 黑名单内IP，执行操作 | 是 | 是 | | 3 | 非黑非白名单的IP，执行任何操作 | 是 | 是 | | 4 | 黑名单内IP与白名单内IP相同，执行操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图：      用例4截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景12

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.12 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景12 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、配置白名单网络规则、不配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 白名单内IP，执行操作 | 否 | 否 | | 2 | 白名单外IP，执行操作 | 是 | 是 |   相关配置截图：  用例1截图：      用例2截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景13

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.13 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景13 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、不配置白名单网络规则、配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 黑名单内IP，执行黑名单内操作 | 是 | 是 | | 2 | 黑名单外IP，执行黑名单外操作 | 否 | 否 | | 3 | 黑名单外IP，执行操作 | 否 | 否 |   相关配置截图：  用例1截图：      用例2截图：      用例3截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景14

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.14 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景14 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、不配置白名单网络规则、配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 任意IP，执行黑名单内操作 | 是 | 是 | | 2 | 任意IP，执行黑名单外操作 | 否 | 否 |   相关配置截图：  用例1截图：      用例2截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景15

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.15 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景15 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、不配置白名单网络规则、不配置黑名单操作内容、配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 黑名单内IP，执行操作 | 是 | 是 | | 2 | 黑名单外IP，执行操作 | 否 | 否 |   相关配置截图：  用例1截图：      用例2截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 测试场景16

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.2.16 | 测试日期 | 2019年4月09日 |
| 测试项目 | 测试场景16 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 规则配置：不配置白名单操作内容、不配置白名单网络规则、不配置黑名单操作内容、不配置黑名单网络规则。 | | |
| 测试步骤 | 1. 服务端，配置文件。 2. 服务端重启华夏数据库安全组件服务使配置生效。 3. 发送测试数据包。 4. 查看拦截效果是否正常。 | | |
| 预期结果 | 所有拦截效果正常 | | |
| 测试结果 | 执行用例如下：   |  |  |  |  | | --- | --- | --- | --- | | 用例 | 数据包内容 | 预期拦截 | 实际拦截 | | 1 | 任意IP，执行操作 | 否 | 否 |   相关配置截图：  用例1截图： | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

## 数据库动态脱敏功能测试

### 使用“partial”函数及pattern方式脱敏

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.3.1 | 测试日期 | 2019年4月09日 |
| 测试项目 | 使用partial函数对数据表的某列进行脱敏，脱敏规则采用正则表达式“\w+”（对数字、字母、下划线及加号进行脱敏） | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 1. 脱敏的数据表dsg\_product\_imagery已存在数据库 2. 配置信息中用户信息及数据库连接信息已配置 | | |
| 测试步骤 | 1. 配置文件中增加对数据表某列的控制 2. 指定type为“mask”，function为“partial”，pattern为“\w+” 3. 保存配置文件      1. 停止dsg服务：/huatengbase/dsg/bin下执行./dsg-stop 2. 启动dsg服务：/huatengbase/dsg/bin下执行./dsg-start -config /huatengbase/dsg/etc/test\_hu\_0404.conf 3. 指定的用户登录/huatengbase/dsg/bin下执行   ./dsgsh -user user17 -password userp -host 127.0.0.1 -port 9002   1. 查看表信息   SelectTLLATITUDE PRODUCTCODE from ds\_product\_imagery where TLLATITUDE like '24.0675%'; | | |
| 预期结果 | 指定列的数字、字母、下划线、加号使用“\*”号替换，其他符号不替换 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 使用“partial”函数脱敏

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.3.2 | 测试日期 | 2019 年 04月 09日 |

|  |  |
| --- | --- |
| 测试项目 | 使用partial函数对数据表的某列进行脱敏，使用“\*”号替换，不设定脱敏规则 |
| 测试人员 | \*\*龙 |
| 前置条件 | 1. 脱敏的数据表dsg\_product\_imagery已存在数据库 2. 配置信息中用户信息及数据库连接信息已配置 |
| 测试步骤 | 1. 配置文件中增加对数据表某列的控制 2. 指定 type 为“mask”，function 为“partial” 3. 保存配置文件      1. 停止dsg服务：/huatengbase/dsg/bin下执行./dsg-stop 2. 启动dsg服务：/huatengbase/dsg/bin下执行./dsg-start -config /huatengbase/dsg/etc/ test\_hu\_0404.conf 3. 指定的用户登录/huatengbase/dsg/bin下执行   ./dsgsh -user user17 -password userp -host 127.0.0.1 -port 9002  7. 查看表数据信息  SelectTLLATITUDE BROWSERIMG from ds\_product\_imagery where TLLATITUDE like '24.0675%'; |
| 预期结果 | 指定列的每一个字符均被“\*”替换 |

|  |  |
| --- | --- |
| 测试结果 |  |
| 测试结论 | ■通过 □不通过 |
| 备注 |  |

### 使用“random”函数脱敏

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.3.3 | 测试日期 | 2019年04月09日 |
| 测试项目 | 使用random函数对数据表的某列进行脱敏 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 1. 脱敏的数据表dsg\_product\_imagery已存在数据库 2. 配置信息中用户信息及数据库连接信息已配置 | | |
| 测试步骤 | 1. 配置文件中增加对数据表某列的控制 2. 指定type为“mask”，function为“random” 3. 保存配置文件      1. 停止dsg服务：/huatengbase/dsg/bin下执行./dsg-stop 2. 启动dsg服务：/huatengbase/dsg/bin下执行./dsg-start -config /huatengbase/dsg/etc/ test\_hu\_0404.conf 3. 指定的用户登录/huatengbase/dsg/bin下执行   ./dsgsh -user user17 -password userp -host 127.0.0.1 -port 9002   1. 查看表信息   SelectTLLATITUDE SATELLITEID from ds\_product\_imagery where TLLATITUDE like '24.0675%'; | | |
| 预期结果 | 指定列的每个字符均被一个随机的ascii码替换 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

## 数据库动态加密功能测试

### 使用“aes”函数加密

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.4.1 | 测试日期 | 2019 年 04月 09日 |
| 测试项目 | 通过密钥对数据表的某列进行加密 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 1. 加密的数据表dsg\_product\_imagery存在数据库 2. 配置信息中用户信息及数据库连接信息已配置 | | |
| 测试步骤 | 配置文件中增加对数据表某列的控制 | | |

|  |  |
| --- | --- |
|  | 1. 指定 type 为“encryption”，function 为“aes”，指定密钥值 key， 2. 保存配置文件      1. 停止dsg服务：/huatengbase/dsg/bin下执行./dsg-stop 2. 启动dsg服务：/huatengbase/dsg/bin下执行./dsg-start -config /huatengbase/dsg/etc/test\_hu\_0404.conf 3. 指定的用户登录/huatengbase/dsg/bin下执行   ./dsgsh -user user17 -password userp -host 127.0.0.1 -port 9002   1. 查看表信息   SelectTLLATITUDE PRODUCTID from ds\_product\_imagery where TLLATITUDE like '24.0675%'; |
| 预期结果 | 指定列的数据被加密，以密文的方式显示。 |
| 测试结果 |  |
| 测试结论 | ■通过 □不通过 |

### 使用“SM4”函数 CBC加密

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.4.2 | 测试日期 | 2019年 04月 09日 |
| 测试项目 | 通过密钥对数据表的某列进行加密 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 1. 加密的数据表dsg\_product\_imagery存在数据库 2. 配置信息中用户信息及数据库连接信息已配置 | | |
| 测试步骤 | 1. 配置文件中增加对数据表某列的控制 2. 指定 type 为“encryption”，function 为“sm4”，加密模式为 cbc，指定密钥值 key， 3. 保存配置文件      1. 停止dsg服务：/huatengbase/dsg/bin下执行./dsg-stop 2. 启动dsg服务：/huatengbase/dsg/bin下执行./dsg-start -config /huatengbase/dsg/etc/test\_hu\_0404.conf 3. 指定的用户登录/huatengbase/dsg/bin下执行   ./dsgsh -user user17 -password userp -host 127.0.0.1 -port 9002   1. 查看表信息   SelectTLLATITUDE GEOMWKT from ds\_product\_imagery where PRODUCTID = '3476871'; | | |
| 预期结果 | 指定列的数据被加密，以密文的方式显示。 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过 □不通过 | | |
| 备注 |  | | |

### 使用“SM4”函数 CFB加密

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.4.3 | 测试日期 | 2019 年 04月09日 |
| 测试项目 | 通过密钥对数据表的某列进行加密 | | |
| 测试人员 | \*\*龙 | | |
| 前置条件 | 加密的数据表dsg\_product\_imagery存在数据库  配置信息中用户信息及数据库连接信息已配置 | | |
| 测试步骤 | 1. 配置文件中增加对数据表某列的控制 2. 指定 type 为“encryption”，function 为“SM4”，加密模式为：cfb，指定密钥值 key， 3. 保存配置文件 | | |
|  | 1. 停止dsg服务：/huatengbase/dsg/bin下执行./dsg-stop 2. 启动dsg服务：/huatengbase/dsg/bin下执行./dsg-start -config /huatengbase/dsg/etc/test\_hu\_0404.conf 3. 指定的用户登录/huatengbase/dsg/bin下执行   ./dsgsh -user user17 -password userp -host 127.0.0.1 -port 9002   1. 执行sql   SelectTLLATITUDE STARTTIME from ds\_product\_imagery where PRODUCTID = '3476871'; | | |
| 预期结果 | 指定列的数据被加密，以密文的方式显示。 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过 □不通过 | | |
| 备注 |  | | |

## 数据库加密访问功能测试

### 数据库通信加密

#### 通信加密

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.1 | 测试日期 | 2019年04月09日 |
| 测试项目 | 确认数据库环境 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8  确认数据库环境符合配置条件 | | |
| 测试步骤 | 1. 输入检测环境语句，确认环境符合配置条件   Huatengbase[(none)]> select version();  Huatengbase[(none)]> show variables like 'have%ssl%';  Huatengbase[(none)]> show variables like 'port';  Huatengbase[(none)]> show variables like 'datadir'; | | |
| 预期结果 | 环境符合配置条件 | | |
| 测试结果 | 环境符合配置条件 | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 生成server端证书

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.2 | 测试日期 | 2019年04月09日 |
| 测试项目 | 服务端证书正确生成 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 创建存放证书文件目录 2. cd /huatengbase 3. mkdir ssl 4. cd ssl 5. 在数据库文件data下创建ssl文件夹   cd /huatengbase/cloudbase/cloudsql/data  mkdir ssl;   1. 使用openssl工具，正确生成服务端证书，生成过程安装如下指令进行操作： 2. openssl genrsa 2048 > ca-key.pem 3. openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca.pem 4. openssl req -newkey rsa:2048 -days 3600 -nodes -keyout server-key.pem -out server-req.pem 5. openssl rsa -in server-key.pem -out server-key.pem 6. openssl x509 -req -in server-req.pem -days 3600 -CA ca.pem -CAkey ca-key.pem -set\_serial 01 -out server-cert.pem | | |
| 预期结果 | 成功服务端证书创建 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 生成client端证书

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.3 | 测试日期 | 2019年04月09日 |
| 测试项目 | 生成客户端证书 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 创建客户端证书，运行如下命令：  1、 openssl req -newkey rsa:2048 -days 3600 -nodes -keyout client-key.pem -out client-req.pem  2、 openssl rsa -in client-key.pem -out client-key.pem  3、openssl x509 -req -in client-req.pem -days 3600 -CA ca.pem -CAkey ca-key.pem -set\_serial 01 -out client-cert.pem | | |
| 预期结果 | 成功生成客户端证书 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 修改证书用户组权限并验证

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.4 | 测试日期 | 2019年04月09日 |
| 测试项目 | 成功修改证书位置，并配置数据库启动文件 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 修改证书文件位置，执行如下指令   cp ca.pem \*.pem /huatengbase/cloudbase/cloudsql/data/ssl/ -v   1. 修改证书用户组，执行如下指令   chown -v cloudsql.cloudsql {ca,\*}.pem   1. 执行验证ssl证书语句，查看状态执行如下指令   openssl verify -CAfile ca.pem server-cert.pem client-cert.pem | | |
| 预期结果 | 证书文件所属用户组成功修改，验证为ok状态 | | |
| 测试结果 | 1. 证书文件所属用户组成功修改，验证为ok状态 | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 生成openssl公有与私有key

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.5 | 测试日期 | 2019年04月09日 |
| 测试项目 | 生成mykey文件并修改用户组 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 生成公有私有key，命令如下： 2. openssl genrsa -out mykey.pem 1024 3. openssl rsa -in mykey.pem -pubout -out mykey.pub 4. 修改用户组与权限 5. chmod 400 mykey.pem 6. chmod 444 mykey.pub 7. /huatengbase/cloudbase/cloudsql/data/ssl下执行：   chmod 600 client-key.pem server-key.pem ca-key.pem   1. 移动文件的到/huatengbase/cloudbase/cloudsql/data/ssl下   cp mykey.pub mykey.pem /huatengbase/cloudbase/cloudsql/data/ssl/   1. 修改/huatengbase/cloudbase/cloudsql/data/ssl下文件权限   chown -v cloudsql.cloudsql mykey.pem mykey.pub | | |
| 预期结果 | 成功创建mykey文件并修改所属用户组 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 配置cnf文件，使ssl配置生效

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.6 | 测试日期 | 2019年04月09日 |
| 测试项目 | 配置cnf文件，使ssl生效 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 使用vi编辑cnf文件，插入如下配置信息   [cloudsqld] ###项下增加以下代码###  ssl-ca=/huatengbase/cloudbase/cloudsql/data/ssl/ca.pem  ssl-cert=/huatengbase/cloudbase/cloudsql/data/ssl/server-cert.pem  ssl-key=/huatengbase/cloudbase/cloudsql/data/ssl/server-key.pem  bind-address=\*  sha256\_password\_private\_key\_path=/huatengbase/cloudbase/cloudsql/data/ssl/mykey.pem sha256\_password\_public\_key\_path=/huatengbase/cloudbase/cloudsql/data/ssl/mykey.pub   1. 重启服务后，进入数据库运行查看ssl功能   show variables like 'have%ssl%'; | | |
| 预期结果 | 正确配置cnf文件，重启服务后ssl功能开启 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 创建ssl专用用户并连接数据库

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.7 | 测试日期 | 2019年04月09日 |
| 测试项目 | 创建ssl专用用户，并验证用户 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 创建ssl专用用户，并刷新权限表   grant all on \*.\* to test@'%' identified by 'test' require ssl; FLUSH PRIVILEGES;   1. 从服务器打包SSL客户端证书文件，下载至navicat所在客户端 2. 连接属性中，选择验证SSL，加载证书连接测试 | | |
| 预期结果 | 成功创建用户，Navicat工具加载客户端证书后可连接登陆数据库 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 抓包测试SSL功能连接

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.8 | 测试日期 | 2019年04月09日 |
| 测试项目 | 抓包测试SSL连接，数据信息被加密 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 打开wireshark工具，navicat工具，使用SSL连接数据库 2. 开启wireshark抓包功能，连接数据库运行查询SQL语句 3. 停止抓包，分析TCP流中数据 | | |
| 预期结果 | 执行查询语句，查出中文信息，在wireshark捕获数据包中无法查看到明文数据，信息全部被加密处理 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 抓包测试无SSL功能连接

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.1.9 | 测试日期 | 2019年04月09日 |
| 测试项目 | 抓包测试无SSL功能连接，数据信息为明文 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1. 打开wireshark工具，navicat工具，使用正常用户登陆数据库 2. 开启wireshark抓包功能，连接数据库运行查询SQL语句 3. 停止抓包，分析TCP流中数据 | | |
| 预期结果 | 执行查询语句，查出中文信息，在wireshark捕获数据包中，查看到明文数据，该SQL语句信息为明文 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

### 数据库安全防护通信加密

#### 客户端文件上传

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.2.1 | 测试日期 | 2019年04月09日 |
| 测试项目 | 正确上传数据库安全组件所需要client端证书等文件 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1、将数据库服务器中的client证书（client-cert.pem;client-key.pem）等文件上传至华夏数据库安全组件服务器/huatengbase/ssl/下 | | |
| 预期结果 | 正确上传华夏数据库安全组件证书文件 | | |
| 测试结果 | 与实际一致 | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### ssl方式连接数据库

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.2.2 | 测试日期 | 2019年04月09日 |
| 测试项目 | 配置华夏数据库安全组件的conf文件，使ssl通道连接数据库生效 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8  正确配置conf文件 | | |
| 测试步骤 | 1. 进入华夏数据库安全组件安装目录etc中，使用vi命令打开配置文件添加如下client证书的绝对路径与ssl专用用户名密码   内容如下：  <connections>  <connection string="user=test;password=test;host=192.168.1.11;port= 13306;db=cetcdb;ssl-cert=/huatengbase/ssl/client-cert.pem;ssl-key=/huatengbase/ssl/client-key.pem"/></connections>  红色字体即为client客户端文件路径配置信息，client客户端文件在这里一定要填写绝对路径   1. 停止安全组件 2. 启动华夏数据库安全组件连接数据库 3. 进入目录 /huatengbase/dsg/bin 目录下，执行启动命令：   ./dsg-start -config ../etc/test\_hu\_0404.conf | | |
| 预期结果 | 华夏数据库安全组件启动正常，可以正确连接目标数据库 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 使用ssl的模式查询数据

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.2.3 | 测试日期 | 2019年04月09日 |
| 测试项目 | 使用ssl模式正确登录华夏数据库安全组件，并可查询数据 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8  华夏数据库安全组件的ssl配置正确启用 | | |
| 测试步骤 | 1.登录华夏数据库安全组件：  进入目录 /huatengbase/dsg/bin 目录下，执行登录命令：  ./dsgsh -host localhost-user user16 -password userp -port 9002  2.查询数据：  执行查询SQL语句验证是否成功登录数据库：  select STARTTIME from ds\_product\_imagery where PRODUCTID = '3476871'; | | |
| 预期结果 | 正确登录华夏数据库安全组件并查询出数据 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |

#### 抓包测试SSL功能连接

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 1.5.2.4 | 测试日期 | 2019年04月09日 |
| 测试项目 | 抓包测试SSL连接，数据信息被加密 | | |
| 测试人员 | 刘静静 | | |
| 前置条件 | Huatengbase 版本：7.3.8 | | |
| 测试步骤 | 1.打开wireshark工具，华夏数据库安全组件使用SSL连接数据库  2.开启wireshark抓包功能，华夏数据库安全组件登录连接数据库运行查询SQL语句  3.停止抓包，分析TCP流中数据 | | |
| 预期结果 | 执行查询语句，查出中文信息，在wireshark捕获数据包中无法查看到明文数据，信息全部被加密处理 | | |
| 测试结果 |  | | |
| 测试结论 | ■通过□不通过 | | |
| 备注 |  | | |