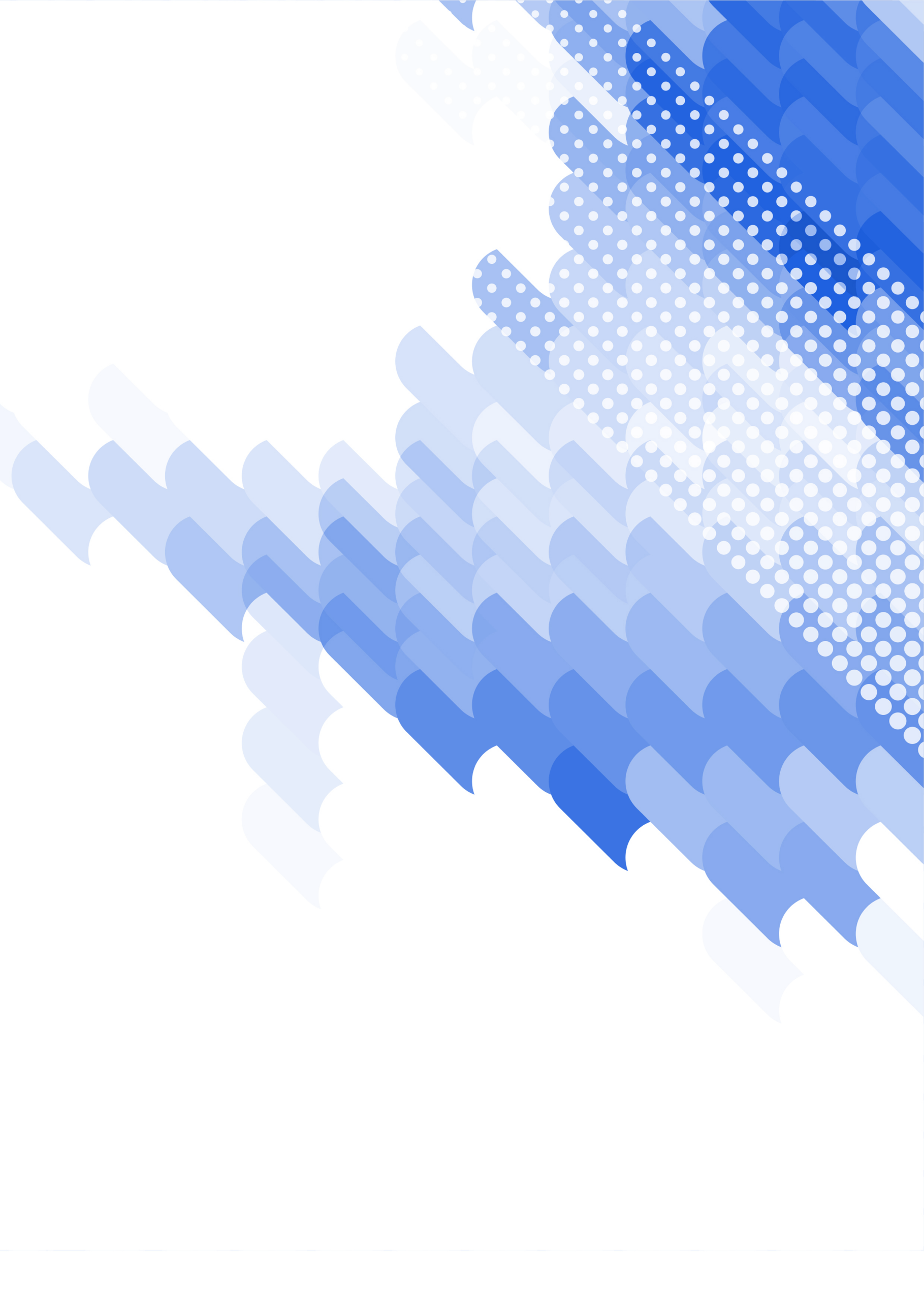
****

上海万雍科技股份有限公司

2024年10月16日

www.vanytech.com

**浙江工贸大学2024年三季度运维巡检  
统计报告**

## 说明

该巡检报告是上海万雍科技股份有限公司为服务期内客户提供的贴心服务之一，暂定在每个季度以及开学、长节假日返校期间提供的日常巡检服务。该巡检服务旨在通过各项系统、数据库、日志、功能测试等检查内容，及时发现问题以保障客户系统的正常运行，因为系统运行受到环境、网络、安全等方面影响，巡检正常不代表绝对避免系统问题出现，但可以大幅降低问题出现的概率，感谢用户的支持和帮助。

目录

[说明 2](#_Toc6360)

[一、 信息 4](#_Toc7057)

[二、 巡检内容 4](#_Toc17130)

[1. 安全性检查 4](#_Toc1288)

[1.1 审核用户 4](#_Toc542)

[1.2 系统入侵检查 4](#_Toc15546)

[2. 资源检查 4](#_Toc17088)

[3. 数据库检查 5](#_Toc27851)

[4. 系统检查 5](#_Toc24900)

[三、 巡检报告 5](#_Toc30527)

[1. 安全性检查 5](#_Toc14734)

[2. 资源检查 6](#_Toc2700)

[3. 数据库检查结果 8](#_Toc8639)

[4. 系统检查 9](#_Toc2001)

[4.1 状态检查 9](#_Toc13324)

[4.2 系统运行概况 10](#_Toc12210)

[四、 巡检结果 10](#_Toc10412)

[1. 运行环境 10](#_Toc29480)

[2. 运行环境Html巡检报告 10](#_Toc18406)

[3. 业务系统可用性 11](#_Toc28617)

[五、业务运维事项列表 11](#_Toc32184)

[六、系统运维统计报告 13](#_Toc6994)

[七、优化建议 15](#_Toc9151)

##### 信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **巡检时间** | **季度** | **客户单位** | **环境** | **巡检人员** | **电话** |
| 2024/10/16 | Q3 | 浙江工贸大学 | - 消息中心 | 柳毓琳 | 15317265303 |

##### 巡检内容

###### 安全性检查

* 1. 审核用户
* 查询特权用户，输出信息应为root或其他有记录的特权用户；
* 查询可以远程登录的帐号信息，输出信息应为root或其他有记录的用户；
* 查询空密码账户，输出用户记录并上报，必要时可清理删除；
  1. 系统入侵检查
* 登录日志检查
* 检查登录过主机的IP列表次数，排查是否有异常IP(归属地在国外、登录次数过多等)；
* 检查登陆失败的IP列表跟尝试次数。短时多次登陆失败可以认定为爆破攻击。记录报告并制定处理计划；
* 计划任务检查
* 检查计划任务列表中是否有无记录的任务。如果有，则需要确认该任务的功能。如果任务为下载、运行未知进程、创建其他的定时任务、写ssh后门等功能的话，则可以判断为主机已被入侵。必须立即记录报告并处理；

###### 资源检查

* 检查当前主机资源状态信息：CPU、内存、系统时间、网络连接状态；
* 检查占用RAM或CPU前十的进程信息；
* 获取主要分区磁盘使用信息、获取中间件服务运行状态等；

###### 数据库检查

* 检查数据库备份脚本的运行状态，确认备份可用性；
* 检查数据库系统日志（定期查询日志可在数据库出现异常前及时规避问题）；
* 核查业务占用实例数据量、当前数据库的活跃连接数、缓存命中率、慢SQL；

###### 系统检查

定期检查各系统主要功能模块的运行状态与参数，可有效避免系统在不知情的情况下出现故障问题，导致不必要的影响与损失。

##### 巡检报告

###### 安全性检查

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 1 | 172.17.5.117 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 2 | 172.17.5.118 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 3 | 172.17.5.119 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 4 | 172.18.126.23 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 5 | 172.17.5.120 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 6 | 172.18.126.22 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 7 | 172.18.126.24 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 8 | 172.17.5.116 | 异常特权账户 | ✔ |  |  |
| 异常远程账户 | ✔ |  |  |
| 空密码账户 | ✔ |  |  |
| 爆破记录 | ✔ |  |  |
| 异常计划任务 | ✔ |  |  |

###### 资源检查

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 1 | **172.17.5.117** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✔ |  |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 2 | **172.17.5.118** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✘ | 内存使用率：88.6% |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 3 | **172.17.5.119** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✔ |  |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 4 | **172.18.126.23** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✔ |  |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 5 | **172.17.5.120** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✔ |  |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 6 | **172.18.126.22** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✔ |  |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 7 | **172.17.5.116** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✔ |  |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 8 | **172.18.126.24** | CPU使用率 < 80% | ✔ |  |  |
| 内存使用率 < 80% | ✘ | 内存使用率：89.8% |  |
| TOP10进程信息 | ✔ |  |  |
| 僵尸进程 | ✔ |  |  |
| 服务器时间 | ✔ |  |  |
| 防火墙状态 | ✔ |  |  |
| ESTABLISHED < 1000 | ✔ |  |  |
| 磁盘分区占用 < 80% | ✔ |  |  |

###### 数据库检查结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **数据库服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 1 | 172.18.126.24 | 数据库状态 | ✔ |  |  |
| Innodb 索引命中率 > 80% | ✔ |  |  |
| 慢SQL占比 < 10 % | ✔ |  |  |
| 活跃连接数使用率 < 80% | ✔ |  |  |
| 备份状态 | ✔ |  |  |
| 系统日志 | ✔ |  |  |
| 当前版本 | mysql Ver 14.14 Distrib 5.7.36, for linux-glibc2.12 (x86\_64) using EditLine wrapper | | |
| **实例** | **实例大小GB** | **数据量（条数）** | |
| data\_center | 0.35 GB | 1088903 | |
| messagecenter | 0.19 GB | 282996 | |
| messagecenter\_340 | 24.82 GB | 33627732 | |
| messagecenter\_test | 0.00 GB | 6686 | |
| zabbix\_proxy | 0.01 GB | 7415 | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **数据库服务器** | **巡检内容** | **巡检结果** | **问题** | **处理** |
| 2 | 172.17.5.119 | 数据库状态 | ✔ |  |  |
| Innodb 索引命中率 > 80% | ✔ |  |  |
| 慢SQL占比 < 10 % | ✔ |  |  |
| 活跃连接数使用率 < 80% | ✔ |  |  |
| 备份状态 | ✔ |  |  |
| 系统日志 | ✔ |  |  |
| 当前版本 | mysql Ver 8.0.33 for Linux on x86\_64 (MySQL Community Server - GPL) | | |
| 实例 | **实例大小GB** | **数据量（条数）** | |
| huatinglake\_portal\_v2\_3\_1 | 1.87 GB | 6587660 | |
| performance\_schema | 0.00 GB | 2985165 | |

###### 系统检查

4.1 状态检查

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **主要功能模块（检查点）** | **检查结果** | **问题** | **处理** |
| 1 | 万雍人脸识别数据安全保护系统 | H5界面与管理后台 | ✔ |  |  |
| 算法核验 | ✔ |  |  |
| 应急上传与后台导入 | ✔ |  |  |
| 第三方下发状态 | ✔ |  |  |
| 数据同步 | ✔ |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **主要功能模块（检查点）** | **检查结果** | **问题** | **处理** |
| 2 | 消息中心 | H5界面与管理后台 | ✔ |  |  |
| 消息发送功能 | ✔ |  |  |
| 消息队列状态 | ✔ |  |  |
| 短信额度 | ✔ |  |  |
| 数据同步 | ✔ |  |  |

4.2 系统运行概况

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **主要参数** | **检查结果** |
| 1 | 华亭湖 | 第三方开发对接数量 | *3* |
| 门户数量 | *4* |
| 小程序数量 | *42* |
| 人员数量 | *17101* |

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **主要参数** | **检查结果** |
| 2 | 消息中心 | 第三方系统对接数量 | *9* |
| 已发短信 | *28636* |
| 剩余短信额度 | *24214* |
| 人员数量 | *17112* |

##### 巡检结果

1. 运行环境

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **巡检结论** | **问题** | **处理** |
| 系统安全性检查 | **正常** |  |  |
| 系统资源检查 | **正常** |  |  |
| 数据库检查 | **正常** |  |  |

1. 运行环境Html巡检报告

|  |  |
| --- | --- |
| **服务器IP** | **运维巡检** |
| 172.18.126.24 |  |
| 172.18.126.23 |  |
| 172.18.126.22 |  |
| 172.17.5.120 |  |
| 172.17.5.119 |  |
| 172.17.5.118 |  |
| 172.17.5.117 |  |
| 172.17.5.116 |  |

1. 业务系统可用性

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **巡检结论** | **问题列表** | **处理** |
| 华亭湖 | 正常 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **巡检结论** | **问题列表** | **处理** |
| 消息中心 | 正常 |  |  |

##### 五、业务运维事项列表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名** | **任务类型** | **问题描述** | **处理方案** | **发现时间** | **处理时间** |
| *1* | 消息中心 | 漏洞修复 | 请求添加超时范围 | / | 2024/1/11 13:27 | 2024/1/11 |
| *2* | 华亭湖 | 故障恢复 | 首页底部资讯未展示、课程表无数据 | 处理显示 | 2024/3/7/17：00 |  |
| *3* | / | 技术支持 | SSL证书更新 | 更新 | 2024/4/24/10:30 | 2024/4/24/11:30 |
| *4* | 华亭湖 | 漏洞修复 | APP权限同步和源头不一致 | 修改同步逻辑，数据量偏少直接删除后重新添加 | 2024/5/17/11:00 | 2024/5/17/16:00 |
| *5* | 华亭湖 | 漏洞修复 | 数据同步代码逻辑有问题 | 修改同步逻辑，数据量少，直接删了重新添加 | 2024/5/27/10:00 | 2024/5/27/10:00 |
| *6* | 华亭湖 | 漏洞修复 | 权限同步出现空指针 | 添加空指针判断 | 2024/6/6/13:00 | 2024/6/6/17:30 |

##### 六、系统运维统计报告





##### 七、优化建议

系统运行环境状态良好，未发现安全与性能问题；

消息中心平台当前运行概况良好，未发现业务问题；

华亭湖当前运行状态良好，未发现业务问题；