## 敏感点和权衡点

#### 敏感点

|  |  |  |
| --- | --- | --- |
| S1 | 对用户信息进行加密 | 保护用户信息，影响了安全性(正面)，是**安全性的敏感点** |
| S2 | 在系统服务收到访问时验证用户身份，授权给用户应有的权限 | 有利于保证系统服务仅受到合法访问，是**安全性的敏感点** |
| S3 | 自动攻击侦测 | 出现攻击时可以自动侦测到，提高了安全性，是**安全性的敏感点**，同时会增加服务器负担，降低性能，是**性能的敏感点** |
| S4 | 心跳 | 一个组件定期发出一个心跳信息，另一个组件收听该信息。可以用来识别错误，是**可用性的敏感点**。同时可能占用资源，导致性能的下降，是**性能的敏感点** |
| S5 | 主动冗余 | 所有的冗余组件都以并行的方式对事件作出响应，错误发生时，使用该战术的系统停机时间通常是几毫秒，是**可用性的敏感点**。但备份占用了系统资源，影响了性能，是**性能的敏感点** |
| S6 | 使用DDOS分防火墙 | 对各种常见的攻击行为进行识别，并通过集成的机制实时对这些攻击流量进行处理及阻断，是**安全性的敏感点**。 |
| S7 | 划分模块 | 将系统模块化，在修改时可以有效缩小要修改的范围，是**可修改性的敏感点** |
| S8 | 增加可用资源 | 使用速度更快的处理器、额外的处理资源、额外的内存、速度更快的网络，可提高性能，是**性能的敏感点**。但会影响成本 |
| S9 | 采用分布式数据服务器 | 分布式数据服务器的性价比显著优于单台商业中型机和大型机，能够提供较为优质的数据服务，是**性能的敏感点（正面）**。但是由于数据分散存储，技术门槛较高，对维护工作，特别是数据完整性、一致性的维护提出了较高的要求，是**可维护性的敏感点（负面）** |
| S10 | 使用HLS(HTTP Live Streaming)协议 | 兼容性较好，提高了可移植性，是**可移植性的敏感点**。但延时比较高，影响了性能，是**性能的敏感点**。 |
| S11 | 独立存储密钥数据的模块 | 将密钥数据独立存储，可以提高可修改性，是**可修改性的敏感点** |
| S12 | 采用GlusterFS分布式文件系统 | 具有线性横向拓展能力，提高了可拓展性，是**可拓展性的敏感点**。增加了客户端的负载，占用了相当的CPU和内存，降低了性能，是**性能的敏感点**。 |
| S13 | 抽取并裁剪接口 | 针对请求响应交换的数据不一致情况，分别通过接口与外部系统相交互，是**互操作性的敏感点** |
| S14 | 使用FFMPEG转码 | FFMPEG转码提供了录制、转换以及流化音视频的完整解决方案，有助于播放清晰的视频，是**性能的敏感点**(正面),同时它包含了非常先进的音频/视频编解码库libavcodec，保证了高可移植性，是**可移植性的敏感点** |

#### 权衡点

|  |  |  |
| --- | --- | --- |
| T1 | 自动攻击侦测 | 提高了安全性，但会增加服务器负担，降低性能，是**安全性和性能的权衡点** |
| T2 | 主动冗余 | 错误发生后恢复时间短，提高了可用性，但备份占用了系统资源，影响了性能，是**可用性和性能的权衡点** |
| T3 | 分布式数据服务器 | 性价比高，以相同成本提供更佳的容量和读写速率，但是维护工作技术门槛高，是**性能和可维护性的权衡点** |
| T4 | 使用gHLS(HTTP Live Streaming)协议 | 兼容性较好，提高了可移植性，但延时比较高，影响了性能，是性能和可移植性的权衡点 |
| T5 | 采用GlusterFS分布式文件系统 | 提高了可拓展性，同时降低了性能，是**可拓展性和性能的权衡点** |
| T6 | 心跳 | 提高了可用性，但降低了性能，是**可用性和性能的权衡点** |

## 风险和非风险

#### 风险

|  |  |  |
| --- | --- | --- |
| R1 | 自动攻击侦测 | 攻击不经常发生，系统一直自动侦测攻击，可能导致对资源的很大浪费，影响性能 |
| R2 | 心跳 | 可能造成性能负担，影响系统性能 |
| R3 | 主动冗余 | 备份占用了系统资源，可能会影响系统性能 |
| R4 | 增加可用资源 | 可提高性能，但成本较高 |
| R5 | 分布式数据服务器 | 分布式数据服务器技术门槛高，提高人力成本。如果维护不当，数据的完整性和一致性可能出现问题。 |
| R6 | 使用gHLS(HTTP Live Streaming)协议 | 延时比较高，可能影响系统性能 |
| R7 | 采用GlusterFS分布式文件系统 | 可能会增加客户端的负载，占用相当的CPU和内存，降低性能 |

#### 非风险

|  |  |  |
| --- | --- | --- |
| N1 | 对用户信息进行加密 | 多用户系统和涉密系统的标准配置 |
| N2 | 在系统服务收到访问时验证用户身份，授权给用户应有的权限 | 多用户系统和涉密系统的标准配置 |
| N3 | 使用DDOS分防火墙 | 可以有效识别并阻断攻击，有效提高安全性 |
| N4 | 划分模块 | 成熟的设计原则，显著利于增强可修改性、可移植性 |
| N5 | 独立存储密钥数据的模块 | 同上 |
| N6 | 抽取并裁剪接口 | 通过接口与外部系统交互，提高了互操作性 |
| N7 | 使用FFMPEG转码 | 提高了性能和可移植性 |

## ATAM分析

#### 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A1** | 经过授权的个人用户希望进入系统报名参与讲座，但系统无法提供正确的反馈，系统记录错误日志并在5s之内从错误中恢复 | | | |
| **质量属性** | 可用性 | | | |
| **环境** | 联网状态 | | | |
| **刺激** | 希望进入系统报名参与讲座时系统无法提供正确的反馈 | | | |
| **响应** | 系统记录错误日志并从错误中恢复 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 心跳 | S4 | T6 | R2 |  |
| 主动冗余 | S5 | T2 | R3 |  |
| **理由说明** | 系统出错后恢复的速度会极大影响用户体验，心跳可在2s内检测到故障，主动冗余可以保证在出现故障后，系统的停机时间只有几毫秒。虽然会降低部分性能，但提高了可用性，也是值得的。 | | | |
| **相关架构图** |  | | | |

#### 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A2** | 系统受到恶意攻击，系统侦测到攻击后，防火墙会识别攻击并阻断攻击 | | | |
| **质量属性** | 安全性 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 外部攻击 | | | |
| **响应** | 系统侦测到攻击后，防火墙识别攻击并阻断攻击 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 在系统服务收到访问时验证用户身份，授权给用户应有的权限 | S2 |  |  | **N2** |
| 自动攻击侦测 | S3 | T1 | R1 |  |
| 使用DDOS分防火墙 | S7 |  |  | N3 |
| **理由说明** | 本项目与学生的校园卡相关，并于教务网相关联，所以安全性尤为重要，所以对用户进行权限设置。  攻击者若不能通过用户认证，可能使用各种方式对系统发动攻击。为安全起见，自动侦测攻击并使用防火墙阻止攻击。虽然可能降低部分性能，但是这种风险是可以接受的，而泄密的风险是不可接受的。 | | | |
| **相关架构图** |  | | | |

#### 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A3** | 系统发起/收到与校园卡系统/教务网系统/现场PC端采集系统的请求/响应，希望与其进行请求/响应数据交换 | | | |
| **质量属性** | 互操作性 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 系统希望与外界系统进行请求/响应数据交换 | | | |
| **响应** | 请求被成功获取并成功交换数据 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 抽取并裁剪接口 | S13 |  |  | N6 |
| **理由说明** | 本项目拥有校园卡支付，校园卡签到，教务网信息导入等功能，所以互操作性是很重要的质量属性。采用合适的接口，可以方便与外界进行数据交换，提高互操作性。 | | | |
| **相关架构图** |  | | | |

#### 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A4** | 开发者修改系统用户界面、数据标准、控制逻辑等 | | | |
| **质量属性** | 可修改性 | | | |
| **环境** | 设计、开发系统时 | | | |
| **刺激** | 开发者希望修改系统用户界面、数据标准、控制逻辑等 | | | |
| **响应** | 需要修改的模块被正确修改，并不影响其他功能的实现 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 划分模块 | S7 |  |  | N4 |
| 独立存储密钥数据的模块 | S11 |  |  | N5 |
| **理由说明** | 对于一个复杂的系统来说，系统的可修改性和可维护性都是非常重要的。采用模块划分的决策，增强内聚，可以有效缩小要修改的范围，是成熟的设计原则，可增强可修改性。并独立存储密钥数据的模块，可提高可维护性 | | | |
| **相关架构图** |  | | | |

#### 5.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A5** | 有500名用户同时在系统上进行讲座报名操作/查看讲座直播 | | | |
| **质量属性** | 性能（负载） | | | |
| **环境** | 联网状态 | | | |
| **刺激** | 学生用户希望在系统上进行讲座报名操作/查看讲座直播 | | | |
| **响应** | 系统能够正常工作，为每一个用户提供相应 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 增加可用资源 | S8 |  | R4 |  |
| 使用分布式数据库服务器 | S9 | T3 | R5 |  |
| **理由说明** | 使用速度更快的处理器、额外的处理资源、额外的内存、更快的网络，可以保证在负载方面提高系统性能。但这会使得成本偏高，造成风险。因此需要在可以负担的范围内尽可能增加可用资源。分布式数据服务器的性价比显著优于单台商业中型机和大型机，能够提供较为优质的数据服务，提高性能。 | | | |
| **相关架构图** |  | | | |

#### 6.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A6** | 用户在系统上观看讲座直播 | | | |
| **质量属性** | 性能 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 学生用户希望在系统上观看讲座直播 | | | |
| **响应** | 系统直播视频清晰流畅，延时短 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 使用HLS（ HTTP Live Streaming）协议 | S10 | T4 | R6 |  |
| 使用FFMPEG转码 | S14 |  |  | N7 |
| **理由说明** | 使用HLS(HTTP LIVE STREAMING)协议，延时虽然较高，但仍在可接受的范围内。且兼容性比较好，提高了可移植性。在性能和可移植性兼备的情况下，选择了HLS新协议。使用FFMPEG转码，可以保证视频质量，同时提高了可移植性 | | | |
| **相关架构图** |  | | | |