PageEye页面监视工具需求分析

编辑：陈瑞涵、顾一帆 日期：2024/6/25

## 用户需求

1. **用户认证与管理**
   1. **用户注册**：用户可以通过提供邮箱、用户名和密码进行注册。系统可以通过发送验证邮件进行邮箱验证。
   2. **用户登录**：用户可以通过用户名/邮箱和密码登录。支持两步验证（可选）。
   3. **忘记密码**：用户可以通过邮箱找回密码，系统发送重置链接。重置密码时需要验证用户身份。
2. **监视器创建**
   1. **监视器设置**：用户可以创建不同类型的监视器，系统提供模板或自定义选项。每种监视器都可以设置详细的参数和监控规则。监控的目标需要具体到页面的一个Element。
   2. **监视器应用场景**
      1. **票务监视**：用户可以选择支持的购票网站进行监控，指定监控的票种类、数量、价格区间、购票时间等。用户可以设置通知方式（邮件、短信、推送等）和通知频率。
      2. **评论监视**：用户可以选择支持的社交媒体、论坛、视频平台等进行监控，指定特定帖子的评论区、动态的评论、视频的评论等。关键字过滤、情感分析、评论数统计等功能。通知设置：用户可以设置通知方式和通知频率。
      3. **抢课（抢票）**：系统监视网站是否开放权限（监测是否有课的element），检测到有课后，立刻执行选课操作（点击某个按钮等）。
      4. **商品价格监控**：监控某个商品的价格变化，当价格降低到预期范围时，添加到购物车，并通知用户及时购买。总体上就是，监控用户关注的element，在发生变化后，通知用户，或者执行用户希望执行的操作（脚本执行、api调用等）。
      5. **数据分析和报告**：监控统计：提供统计数据，如页面变化频率、通知发送次数等。报告生成：生成定期报告，供用户下载或通过邮件发送。
      6. **高级监控功能**：内容变化检测：不仅仅是元素存在与否的变化，还可以检测元素内容的具体变化，如文本内容的增加或减少。定制化监控规则：用户可以设置复杂的规则，如特定条件下才触发通知或操作。
      7. **多用户协作**：团队功能：支持团队协作，多个用户可以共享 Watcher，协同监控和操作。权限管理：不同用户可以有不同的权限级别，如管理员、编辑、查看者等。
3. **监视器管理**
   1. **监视器列表**：用户可以查看已创建的监视器列表及其状态。
   2. **监视器编辑**：用户可以修改监视器的设置、参数和通知方式。
   3. **监视器删除**：用户可以删除不需要的监视器。
   4. **监视历史**：用户可以查看监视器的历史数据和监控记录。
4. **账户管理**
   1. **账户信息**：用户可以查看和修改账户信息（用户名、邮箱、密码等）。
   2. **计费信息**：用户可以查看计费信息、消费记录和账单详情。

## 管理员需求

1. **用户管理**
   1. **用户列表**：管理员可以查看所有注册用户的列表。
   2. **用户状态管理**：管理员可以禁用或解禁用户账户。
   3. **用户信息查看**：管理员可以查看用户的详细信息和活动记录。
   4. **计费信息查看**：管理员可以查看用户的计费信息和消费记录。
2. **监视器管理**
   1. **监视器列表**：管理员可以查看所有用户创建的监视器列表及其状态。
   2. **监视器状态管理**：管理员可以禁用或解禁监视器。
   3. **监视器异常检测**：管理员可以查看是否有工作异常的监视器，并进行处理。
   4. **日志记录**：系统应记录所有监视器的操作日志，便于管理员追踪问题。
3. **系统管理**
   1. **通知管理**：管理员可以设置全局通知策略和频率。
   2. **数据备份与恢复**：系统应定期进行数据备份，管理员可以进行数据恢复操作。
   3. **权限管理**：管理员可以分配和管理其他管理员的权限。

## 技术需求

1. **计费功能**
   1. **用户计费**：根据用户的监视器运行时间进行计费，考虑定价策略和平台的盈利分析。
2. **性能与扩展性**
   1. **可用性需求**：系统应具有高可用性，支持自动扩展和负载均衡。客户端Web浏览器。
   2. **性能需求**：监视器应在高并发情况下保持性能稳定。数据量不少于10k，在1000并发的场景下，响应时间<3s。考虑提升性能与降低成本的权衡。
   3. **兼容性需求**：适应用于客户端不同的分辨率/尺寸。
3. **安全性**
   1. **数据加密**：用户数据和监视数据应进行加密存储和传输。
   2. **安全防护**：系统应具有防护机制，防止DDoS攻击、SQL注入等安全威胁。
   3. **系统安全**：应对各种系统故障。
4. **接口与集成**
   1. **第三方服务集成**：系统应支持与第三方服务（如支付网关、通知服务等）的集成。
   2. **API接口**：系统应提供开放的API接口，方便其他系统的接入和扩展。