CMS新功能 - 业务应用审计

**功能需求：**

* 产生一个演示项目，展示CMS系统能够支持“业务应用审计”功能
* 审计是从某一应用系统在用户选定时间范围内来查询所有账号访问历史（登录/退出）和操作行为（如：上传/下载，查询等）

**CMS 用户界面设计：**

1. 从应用列表中点击一项应用，目前只保证一个应用支持业务审计功能，如点击CMS / OneDrive 进入下一应用访问session summary列表：(下面列表用假数据描述)，列表中每一条记录是一次登录记录，如果登录时长为空值，说明这次访问还没有结束。

**Application Name业务名称：Holonet**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **登录账号 Account Name** | **登录 Login** | **登录时间 Login Time** | **登录时长Duration** | **总流量Volume** | **上传Upload** | **下载Download** | **查询Search** |
| [pli@holonetsecurity.com](mailto:pli@holonetsecurity.com) | success | 18-06-06 09:21 | 4h33m | 3.4KB | 3 | 1 | 5 |
| [pli@holonetsecurity.com](mailto:pli@holonetsecurity.com) | success | 18-06-06 09:22 |  | 4.4KB | 3 | 10 | 5 |
|  |  |  |  |  | 3 | 1 | 5 |
| [hacker@somewhere.com](mailto:hacker@somewhere.com) | failure | 18-06-06 09:21 |  | 0 |  |  |  |
| [hacker@somewhere.com](mailto:hacker@somewhere.com) | failure | 18-06-06 09:22 |  | 0 |  |  |  |
| [hacker@somewhere.com](mailto:hacker@somewhere.com) | failure | 18-06-06 09:23 |  | 0 |  |  |  |
| [hacker@somewhere.com](mailto:hacker@somewhere.com) | failure | 18-06-06 09:24 |  | 0 |  |  |  |
| [chunqing@holonetsecurity.com](https://dev-test.holonetsecurity.com/main#/users/single/?userId=chunqing) |  |  | 1h22m | 3.7KB | 3 | 1 | 5 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. 点击某一用户登录账号（User Account）得到具体一个session 的所有activity 记录。如下表格所示

**用户登录账号User Login Account: pingli@holonetsecurity.com**

|  |  |  |
| --- | --- | --- |
| **活动类型Activity** | **活动对象Objects** | **活动发生时间Activity Time** |
| download | DSC\_3894.jpg | 18-06-06 11:21 |
| upload | DSC\_3895.jpg | 18-06-06 11:28 |
| search | **holonet** | 18-06-06 12:28 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**后台支持：**

* 需要提供对某一应用登录/退出记录数据 – 登录账号，时间，登录成功/失败，总流量（optional）等
* 提供每次登录的session 数据，以便上面数据在一个session过程中
* 提取activity数据提供search执行的信息： 查询字串(string)和执行时间

**实现计划：**

以Holonet Security公司内部应用- holonet 为业务进行审计分析

**业务应用审计案例：**

* 应用访问URL: <https://dev-cms.holonetsecurity.com/>
* 活动行为追踪：
  + **登录用户/密码：**[demo@stratusee.com](mailto:demo@stratusee.com) /abcd1234 or 某个人用户账号

需要捕捉用户账号，登录时间和是否成功登录

* + **业务查询：**点击搜索🔍按钮， 输入：”holonet” 并从pull-down menu中选择一项可获得一次search activity

需要获得当前用户查询字串和行为请求时间

* **文件下载：**点击左上方“Report”按钮进入报表列表页面，选择任何一个文件点击下载按钮，即可得到download activity

需要获取当前用户下载文件名，行为请求时间

* **文件上传：** 点击右上方”Setting”按钮，点击“Cutomized IP-MAC Entry”弹出对话窗口，点击”Choose File”按钮选择本地文件之后点击”Import” 按钮执行上传行为（目前该功能只可以用个人账号登录实现，目前我们demo账号没有赋予上传权限）

需要获得上传文件名和上传时间

* **退出应用：**
  + *用户点击”Logout”退出应用* – 获取该用户退出时间
  + *系统自动终止应用* (session timeout) – 不知是否可以根据该应用内部设置的timeout 时间来判断？可能需要在”业务审计”功能上增加configuration用户界面输入参数（待讨论）
  + *用户关闭browser强行退出* – 这时无法捕捉用户离开应用的准确时间， 不知是否可以根据用户idle时间来设定退出时间。Idle时间确定可以通过configuration用户界面由用户输入参数定义，系统提供缺省值