TIES456 demo 4

Aleksi Pekkala (alvianpe@student.jyu.fi)

2.10.2017

Analytics REST API

- 4 resources:
  - Events
  - Categories
  - Users
  - Alarms
- Each event has a category
- Each alarm has a category and a owner (user)
- docs at http://petstore.swagger.io/?url=https://analytics-rest.herokuapp.com/api-docs

JWT Authentication

- 1. User registers via a POST request to /users
  - password gets hashed and salted on user creation
- 2. User fetches token via a POST request to /tokens
  - request body consists of `email` and `password`
  - user object is encoded in token payload
- 3. User makes an authenticated request by adding an Authorization header
  - `Authorization: Bearer <token>`
- 4. Token gets parsed and verified on the server
  - if signatures match, user's identity and role are read from token payload
  - otherwise return a 401 error

Authorization

- Role-based & user-restricted authorization
- 3 roles: anonymous, user & admin
- Anonymous users can create a user and access events
- Users can list all resources, create new items and manage their own items
- Admins can access everything apart from managing other admin users