OPifex Entertainment API

INTRODUCTION

Requirements

- NodeJs – www.NodeJs.org
- Windows/Linux
- MongoDB / MongoLab / MongoVUE

Topics

- NodeJs
- MongoDB
- RESTful
- HMAC SHA1

NODEJS

What?

- Non-Blocking - callbacks.
- Cross-Platform
- Socket Communication
- Javascript Google's V8 Engine

Why?

- Quick Development
- Scalable
- Re-use of code in web development
- Large community
- Not a perfect solution
    - Bad at large processing (It's javascript)
    - Pointless for up-to-date real time traffic (FPS)

Examples

- Cmd Line
    - Node.exe
    - var d = new Date();d
    - d.toLocaleTimeString()
- HTTP
    - Require
    - Create Server
    - Listen
    - Show

```
var http = require('http');
http.createServer(function (request, response) {
    response.writeHead(200, { 'Content-Type' : 'text/html' });
    response.end('<h1>Hello World!</h1>');
}).listen(8080);
console.log('Server Running');

```

- TCP
    - Require
    - Listen
    - Telnet

```
var http = require('http');
http.createServer(function (request, response) {
    response.writeHead(200, { 'Content-Type' : 'text/html' });
    response.end('<h1>Hello World!</h1>');
}).listen(8080);
console.log('Server Running');

```

REST

What?

- **Re**presentational **S**tate **T**ransfer
- REST is *an architecture style* for designing networked applications. The idea is that, rather than using complex mechanisms such as CORBA, RPC or SOAP to connect between machines, simple HTTP is used to make calls between machines.
- Uses HTTP Verbs (GET, PUT, POST, DEL)

Why?

- Easy to use
- Widely supported

HMAC SHA1

- Easy to generate in most languages
- Ensures you are who you say you are
- Private Key
- Data
- Time

```
1  function ValidateRequest(request, key)
2  {
3      var urlRequestData = request.url.href.split('&data=');
4      var req = urlRequestData[0];
5      var data = urlRequestData[1];
6      var hmac = crypto.createHmac('sha1', String(key));
7      var hash = hmac.update(req).digest('hex');
8      if (data == hash) return true;
9      return false;
10 }
```

DATABASE - MONGODB

Why?

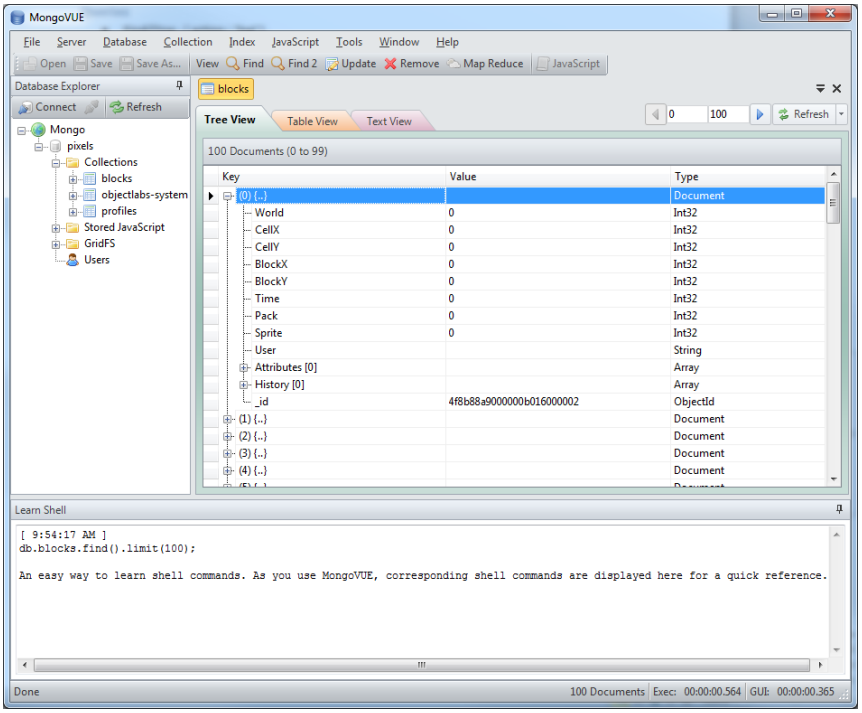
- JSON
- Very easy to work with
- Scalable

Queries

- Find/One - { action : 'log' }
- Update - { username:'ghoofman', {$set { verified: true } } }
- Insert – { object: 'data' }
- Remove – { query }

MongoVue

- Collections
- Documents



MongoLab

- Cheap (Free)
- Easy to move to the cloud later

Mongolian

- npm install Mongolian
- Very similar to the MongoDB syntax so it's quick to pick up on
- Always has a callback of function(err, data)

CONCLUSION

Database – MongoDB – Collections

http://www.opifexentertainment.com/wiki/index.php?title=MongoDB_Design

- Accounts

```
{
    _id:ObjectId,
    username:string,
    password:string,
    verified:bool,
    personal: {
        firstname:string,
        lastname:string,
        email:string
    },
    permissions : [...string...],
    preferences : {
        newsletter:bool,
    },
    points:{
        opifexpoints:long,
        hoardpoints:long
    },
    verificationcode:string,
}
```

- Account_Requests

```
{
    _id:ObjectId,
    data:string,
    time:long,
}
```

API

- [PUT] User
- [GET] User
- [DEL] User
- [POST] User/Reset

Request Verification

```
// Determine if the request made was valid
function ValidateRequest(request, key, time, callback)
{
    var urlRequestData = request.url.href.split('&data=');
    var req = urlRequestData[0];
    var data = urlRequestData[1];

    // Ensure the request came in the last 5 minutes (UTC/GMT Time)
    // 5 minutes because time can vary slightly per system.
    var currTime = new Date().getTime();
    var timeDiff = currTime - time;
    if(timeDiff < 300000 && timeDiff >= 0){ // Also prevent future time requests
        Requested(data, function(err, result){
            if(!err && result != null && !result){ // If the request hasn't been made before
                var hmac = crypto.createHmac('sha1', String(key));
                var hash = hmac.update(req).digest('hex');
                // See that the request has an equal value with the Private Key
                if (data == hash){
                    account_requests.insert({
                        data : data,
                        time : time
                    });
                    callback(false, true);
                }
                else{
                    callback(false, false);
                }
            }
        }
    }
    else{
        callback(false, false);
    }
}
```

References

- NodeJs - http://nodejs.org/
- MongoDB - http://www.mongodb.org/
- MongoLab - https://mongolab.com/home
- MongoVUE - http://www.mongovue.com/
- Mongolian - https://github.com/marcello3d/node-mongolian
- OPifex Website - http://www.opifexentertainment.com/Home
- REST - http://rest.elkstein.org/2008/02/what-is-rest.html
- Secure RESTfull API - http://www.thebuzzmedia.com/designing-a-secure-rest-api-without-oauth-authentication/

Samples

- http://www.opifexentertainment.com/uploader/data/API.zip