**MERN Stack Front to Back**

**MongoDB Setup**

1. Go to **cloud.mongodb.com** and sign up for an account to use **MongoDB Atlas** cloud database services
2. Click on the **CONTEXT** dropdown button next to the Atlas logo and press the **New Project** button to create a new MongoDB project
3. Create a database by clicking on the **Build a Database** button
4. Select a database type in the **Path Selector** menu
   1. Use the **Shared** free **Cluster** database for learning and experimenting
   2. Choose AWS as the cloud provider and select the closest region
   3. Click on the **Cluster Name** tab and provide a name for the database
   4. Click on the **Create Cluster** button
5. Choose an authentication method and add a database user
   1. **\***The first user will have permission to read and write any data in the project
   2. Select the **Username and Password** option to add a new user with a username and password
      1. **\*\***Creds for course: **Admin/20notches**
   3. Select the **My Local Environment** option in the **Connect From** menu to allow IP address **Whitelisting**
      1. Only whitelisted IP addresses may access the database
   4. Add IP addresses to the whitelist to permit them access
      1. Click the **Add My Current IP Address** button to add the current IP you’re using
6. Once the database is created, press the **CONNECT** button (inside the database’s panel) to access the **Connection String** for the database
   1. Select **Connect your application** as the connection method
   2. Choose **Node.js** as the driver at the desired version
   3. Click on the **Browse Collections** button to view the database’s collections (data tables)

**Express Setup**

1. To start an Express project:
   1. Create a folder and name it the name of the project (i.e. “devconnector”)
   2. Type **npm init** in a bash window inside the project folder
      1. Follow the npm prompts and provide the necessary information
         1. Use **server.js** as the file name of the **entry point**
      2. This will create a **package.json** file for the project containing the settings entered in the init prompts
   3. Use **yarn add** to add the following packages:
      1. **express** – used to instantiate an express server
      2. **express-validator** – used to validate data in express
      3. **bcryptjs** – used for password encryption
      4. **config** – used to create global variables
      5. **gravatar** – used to access online (GitHub) user avatars
      6. **jsonwebtoken** – used for auth token validation
      7. **mongoose** – A document relational mapping framework for MongoDB
      8. **request** – Allows an express server to make HTTP requests to another API
   4. Use the command **yarn add -D** to add the following packages to the project’s **devDependencies**:
      1. **nodemon** – Used to refresh the express server with latest code changes upon save
      2. **concurrently** – Allows for multiple dev servers (i.e. express and react servers) to run at the same time with a single command
   5. Create a **server.js** file as the main entry point of the express server
   6. To setup an active express server in the server.js file:
      1. Require the ‘express’ library and assign it to a const
      2. Call **express()** and assign the returned object to an **app** constant
      3. Create a **PORT** constant and assign it to **process.env.PORT** OR a desired port number
      4. Call **app.listen()** to initiate the express server and listen for incoming requests
         1. Pass in the PORT variable as the first parameter
         2. Pass in a function to execute (i.e. console.log()) once the express server has started as the second parameter
      5. Ex.:

**const express = require('express');**

**const app = express();**

**const PORT = process.env.PORT || 5000**

**app.listen(PORT, () => console.log('Server started on port ${PORT}'));**

1. Call the command **node [entry\_point\_file],** where entry\_point\_file is the name of the server file (i.e. server.js), in command line to invoke the express server and have it listen for incoming requests
   1. The .js extension at the end of the file name is optional
2. In a dev environment, use the command **nodemon [entry\_point\_file]** to invoke a nodemon server that will update the server’s code every time a file has changed
3. In the **package.json** file, edit the **“scripts”** property adding:
   1. A **“start”** script that invokes the express server in a production environment
      1. Use the command line command node [entry\_point\_file], in quotes, for production
   2. A **“server”** script that invokes the express server in a development environment
      1. Use the command nodemon [entry\_point\_file], in quotes, for development

**Connecting to MongoDB with Mongoose**

1. Use the **config** npm package to create global values that can be used though out the express application:
   1. In the root folder of the project, create a **config** folder
   2. In the config folder, create a new file called **default.json**
      1. This will store all the default values for the app
      2. Create a new JSON object and add a property called **“mongoURI”**
         1. Set this property equal to the connection string of the MongoDB used for the application
         2. If using an Atlas connection string, replace **<password>** with the actual password of the connecting user
   3. Create another file named **db.js** to establish the MongoDB connection:
      1. Require **mongoose** – a **Document Relational Mapper** used to connect to a MongoDB database and create schemas
      2. Require **config** to retrieve configuration values
      3. Declare a const called **db** and use the config.**get()** function to retrieve values from the default.json file
         1. Use this function to get the mongoURI value from the default.json file
      4. Use the **mongoose.connect()** function to instantiate a connection to the database
         1. This method is asynchronous
         2. Pass in db as the first parameter
         3. See code for detailed connection notes

**Route Files With Express Router**

1. All express routes can be placed inside of the server.js file, but this becomes long and messy
2. Break the express routes down into multiple files
   1. See code for examples
3. Use the **app.use()** function, where app is an instance of express(), to assign parent route paths to a route file
   1. Pass in the parent route path as the first parameter (optional)
   2. Pass in the required file, using require(), as the second parameter
      1. **\*\***When referring to the parent route inside a route file, start the **path** string with ‘**/**’ then add additional child routes
         1. This will start the route path right behind the path passed into the app.use() method stated above

**Using API Routes & JWT Authentication**

1. Create a folder called **Models** to house all the database schema models for the server
   1. See code for detailed examples
2. The JSON **body-parser** library is now absorbed into **express**
   1. Call the statement: **app.use(express.json({ extended: false }))** to enable body-parser on an express server to receive the JSON payload of each server request
      1. The **extended** option allows a dev to choose between parsing the URL-encoded data with the querystring library (when false) or the qs library (when true)
3. When making an API request in Postman to an express server:
   1. Set the **Content-Type** Header value to **application/json**
   2. Send JSON data {with curly braces} through the Body pane
4. Use the **express-validator** library as middleware to an express server request
   1. https://express-validator.github.io/docs/check-api/#checkfield-message
   2. Pass in validator methods (i.e. **check**, **body**, **header**, etc.) as the second parameter, **middleware**, to an **express.Router().Route()** function for the request object to be validated
      1. \*Validation functions may be passed in as an array OR separate parameters
   3. Validation results are returned in the **validationResult()** function imported from the express-validator library
5. Use the **bcrypt** library to encrypt passwords before saving them to the database
6. Use the **jsonwebtoken** (**JWT**) library to authenticate users and return a session-reusable web token to a user
   1. [https://jwt.io/](https://jwt.io/#debugger-io)
   2. JWT is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object
      1. This information can be verified and trusted because it is digitally signed
         1. JWTs can be signed using a secret with HMAC algorithm or RSA or ECDSA public/private key pairs
   3. JWT is most often used to transmit authorization information between server and client
   4. JWT mints a **token** that is passed between the client and server for each authorized request
      1. Once a user has logged in, each subsequent request will include the JWT token allowing the user to access routes and resources he/she has permission to view
      2. The token can easily be **verified** to ensure that no client has tampered with it
   5. JWT has 3 parts separated by periods (.):
      1. **Header** – The JWT header typically consists of 2 parts:
         1. **alg** – Defines the signing algorithm: HMAC, SHA256, or RSA
         2. **typ** – The type of token (always **“JWT”**)
      2. **Payload** – Contains **claims** which are statements about an entity (typically, the user) and additional metadata about the JWT itself
         1. There are 3 types of claims:
            1. **Registered Claims** – A set of predefined claims which are not mandatory but recommended, to provide a set of useful, interoperable claims. Some of them are: **iss** (issuer), **exp** (expiration time), **sub** (subject/user ID), **aud** (audience/Calling API domain) and [more](https://www.rfc-editor.org/rfc/rfc7519#section-4.1)
            2. **Public Claims** – A value that contains a Collision-Resistant Name

In order to prevent collisions, any new Claim Name should either be registered in the IANA "JSON Web Token Claims" registry or be a Public Name

The definer of the name or value needs to take reasonable precautions to make sure they are in control of the part of the namespace they use to define the Claim Name

* + - * 1. **Private Claims** – A producer and consumer of a JWT MAY agree to use Claim Names that are Private Names: names that are not Registered Claim Names

Unlike Public Claims Names, Private Claim Names are subject to collision and should be used with caution

* + 1. **Signature** – The signature is used to verify the message wasn't changed along the way, and, in the case of tokens signed with a private key, it can also verify that the sender of the JWT is who it says it is
       1. The signature is created by taking the encoded header, the encoded payload, a (user defined) secret, and **sign**ing them all with the algorithm specified in the header

1. Use bcryptjs's **hash()** function to encrypt any password with 184 bit encryption
   1. Pass in any password as the first parameter
   2. Pass in a **salt** (phrase that will distinguish this hash from any other) as the second parameter
2. Use bcyptjs's **compare()** function to poll if a plain text password is equal to its hashed value
3. An **Access Token** is given in response to an access token request (typically an authentication request)
   1. This token is used to access APIs and various backends
   2. It is typically issued by an authorization server or a third party vendor (server)
   3. An access token should have a short lifetime and should only be accepted while still valid
   4. Access tokens can be revoked, typically during user logout
4. A **Refresh Token** allows a user to gain an access token without signing in using their username/password
   1. This token should be saved to an application user collection in a database and verified upon auth requests
   2. A web service can request access tokens on behalf of the user without the user being present
   3. A refresh token should have a longer lifetime than an access token
   4. **\***The refresh token should be stored in a database for security purposes
5. Use the **jsonwebtoken.sign()** method to produce a "JSON Web Token"
   1. Pass a JSON object as payload data into the first parameter
   2. This JSON data typically contains info about the user and can contain "claims" i.e. "iss" (issuer), "exp" (expiration time), "iat" (issued at), etc: https://www.rfc-editor.org/rfc/rfc7519#section-4.1
   3. Pass in a **secretOrPrivateKey** as the second parameter
      1. This can be a secret for HMAC algorithms or the PEM encoded private key for RSA and ECDSA
      2. In case of a private key with passphrase an object { key, passphrase } can be used
   4. Pass in a JSON object for JWT **options** (JWT header/claims) OR an array containing options and a **callback** function for async processing
      1. These options are defined in the JWT docs: https://www.npmjs.com/package/jsonwebtoken
      2. The default "algorithm" option is "HMAC SHA256"
      3. The default "typ" option is "JWT"
      4. The "expiresIn" option can be a number (interpreted in seconds) OR a string describing a time span vercel/ms, i.e. 60, "2 days", "10h", "7d"
   5. \*\*If claims are passed in the payload, they CANNOT be passed in the options parameter
   6. \*\*The header can be customized via the options.header object
   7. \*\*Generated JWTs will include an iat (issued at) claim by default unless noTimestamp is specified
   8. \*\*The secretOrPrivateKey parameter can be read from an external file i.e. fs.readFileSync('private.key')
   9. \*\*It is common practice to pass in a version number to the refresh token's payload object so that the exact same refresh token will not be created twice
6. \*The default Authorization Header type for JWT is the **Bearer Token**, where an **Authorization** HTTP header is added to the request and its value is the word "Bearer" plus an empty space plus the JWT value
7. When making requests against a JWT enabled server, use the **x-auth-token** in the request header and assign it to the JWT key generated for the application
8. Use the **jsonwebtoken.verify()** method to decode the payload of a JWT
   1. Pass in the JWT to decode as the first parameter
   2. Pass in the **secretOrPublicKey** as the second parameter
      1. This should be a secret for HMAC, OR the PEM encoded public key for RSA and ECDSA algorithms
   3. Pass in optional "options" as the third parameter OR an array containing options and a callback for async processing as the third parameter; options available here: https://www.npmjs.com/package/jsonwebtoken
   4. This function returns an object which is the decoded contents of the JWT's payload
   5. **\*\***Claims data is returned in the payload
   6. \*\*Errors such as "TokenExpiredError" or "JsonWebTokenError" are implicitly thrown from this method if the header/payload/signature of the JWT are in error

**More on API Routes**

1. Use the **type** and **ref** schema property attributes, while creating a Mongoose model, to create a foreign key to (reference) another document (object) defined in another Mongoose model
   1. The **type** attribute should be assigned to **mongoose.Schema.Types.ObjectId**
   2. Add a **ref** attribute to this property and assign it to the name of the MongoDB **model** being referenced (i.e. ‘user’)
   3. Ex.: **const ProfileSchema = new mongoose.Schema({**

**user: {**

**type: mongoose.Schema.Types.ObjectId,**

**ref: 'user'**

**},**

1. When performing a query operation on a model for a referenced (joined) model object, pass the referenced property's name in the query and assign it to the ID of the referenced document (object)
   1. Ex.: **const profile = await Profile.findOne({user: req.user.id});**
2. Use Mongoose's **Query.populate()** method to specify fields that will be populated by the referenced document
   1. This changes the referenced property from just an ID to and object containing all fields specified
   2. Ex: **const profile = await Profile.findOne({user: req.user.id}).populate('user', ['name', 'avatar']);**
3. Use the **findOneAndUpdate**() method to find the first doc that fits given filter and update it or insert a new one (upsert)
   1. Pass in a JSON object containing the **filter criteria** as the first parameter
   2. Pass in a JSON object containing the fields to update as the second parameter
      1. **\*\***Use MongoDB's **$set** operator as a key and assign it to a whole object to update vs setting each doc field one-at-a-time
         1. **\*\***If the field does not exist, $set will add a new field with the specified value, provided that the new field does not violate a type constraint
   3. Pass in a JSON object containing "options" as the third parameter
      1. Set the **new** option to **true** to return the document AFTER its been updated vs un-updated values
      2. Set the **upsert** option to **true** to insert the doc if no doc fitting the criteria is found
         1. An upsert combines the filter and update parameters to save all given fields to the doc
         2. Set the **rawResult** option to true in order to return an object containing both the updated/new doc along with a **lastErrorObject** which contains metadata about the update/new doc
            1. Use the **updatedExisting** field of this object to determine whether the doc was updated or inserted
   4. \*This method is "Atomic" meaning the doc will not change between finding it and updating it (unless the doc is upserted)
4. Use the **Request.params** object, inside a router method, to access the **URL Parameters** (values in the route that are prefixed with a colon [:]) passed into the request
   1. These URL parameters should be passed into the **path** parameter of a Router.[verb]() method, where [verb] is get, post, put, etc.
   2. URL parameter names should follow RESTful API standards
5. When logging errors or trouble shooting a route, use the statement **error.kind === 'ObjectId'** to poll if the kind of error is a malformed **MongoDB Object ID**
6. Use Mongoose's **Model.findOneAndDelete()** method to find a document that matches a given criteria and remove it
   1. Pass in a JSON object as the **condition** or filter criteria as the first parameter
   2. Pass in a JSON object as **options** to delete the doc as the second argument
      1. Use the **sort** option to set the sort order to deleting the first doc if multiple docs are found
7. **\*\***Sub-Documents (JSON objects) inside arrays of other documents are automatically assigned IDs by MongoDB
8. Saving a top-level document also saves the state of all sub-documents (collections/arrays) as well
9. When content is being removed/deleted from a database, even in sub-document(s) it is good practice to declare an express **Router.delete()** method instead of a PUT request
10. When deleting sub-documents inside a sub-document array:
    1. Use **Array.map()** to map the sub-documents to an array of IDs
    2. Use **Array.indexOf()** to find the index of the sub-document ID passed to the request
    3. Use **Array.splice()** to remove the sub-document at given index
    4. Ex.: **const profile = await Profile.findOne({user: req.user.id});**

**const removeIndex = profile.experience**

**.map(itm => itm.id)**

**.indexOf((req.params.exp\_id));**

**profile.experience.splice(removeIndex, 1);**