1. Add the private keys to bundle-ssl, under the respective folders: ca, elasticsearch, kibana, logstash. The filenames are ca.key, elasticsearch.key etc

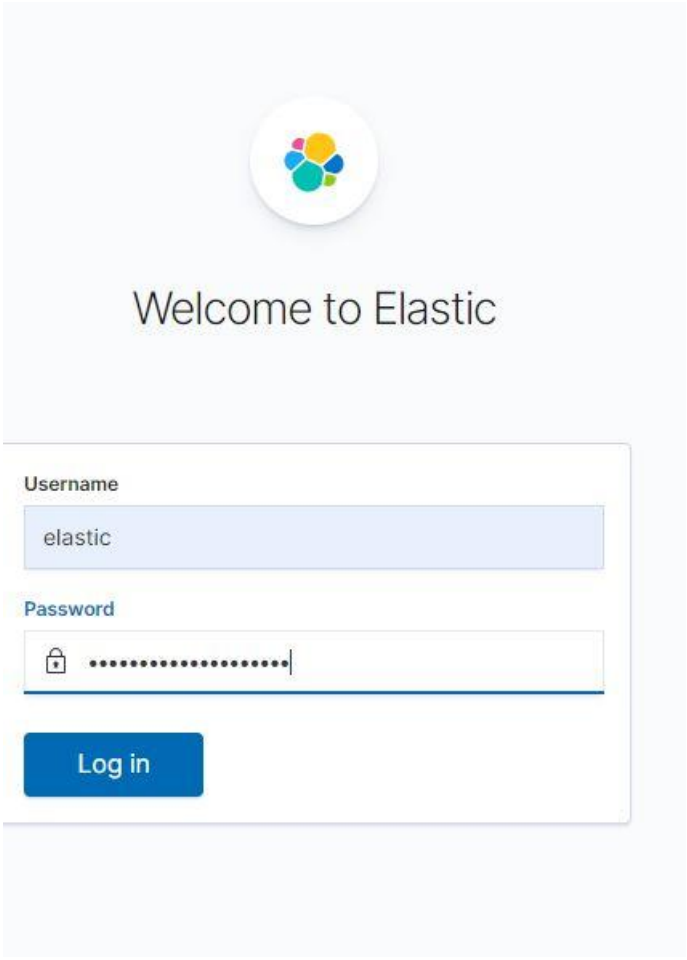
2. Go to microservicecloud dir, type ‘docker-compose exec elasticsearch bash’

```
\ARCHSS Practice Module\repos\travel-plan-api\microservicecloud>docker-compose exec elasticsearch bash
```

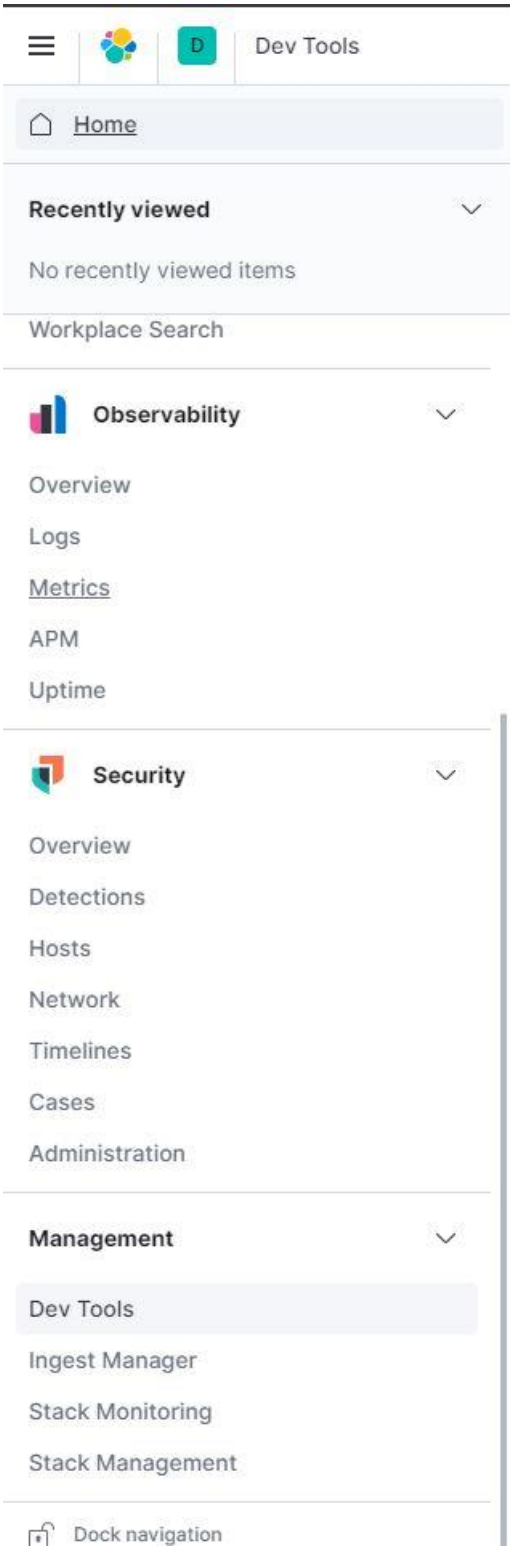
3. Generate usernames and passwords for all users by typing ‘./bin/elasticsearch-setup-passwords auto -u “https://localhost:9200”’
   Copy out the username and password into external file

```
[root@elasticsearch elasticsearch]# ./bin/elasticsearch-setup-passwords auto -u "https://localhost:9200"
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,logstash_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y


Changed password for user apm_system
PASSWORD apm_system = IRbrYaNa750MN63A7yEx

Changed password for user kibana_system
PASSWORD kibana_system = 8SsCkC6FWGdFyhfNeMax

Changed password for user kibana
PASSWORD kibana = 8SsCkC6FWGdFyhfNeMax

Changed password for user logstash_system
PASSWORD logstash_system = 85VSkrzCE6VwEXA4OJ63

Changed password for user beats_system
PASSWORD beats_system = t1NduzECd404fh0MOigq

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = J8OiZPH3fllfbo0D7DJR

Changed password for user elastic
PASSWORD elastic = mm4yL8ORAE0yVZIeX1WI
```

4. Overwrite password for kibana_system user in kibana.yml
5. Overwrite password for logstash_system user in logstash.yml
6. Go to kibana UI, you should be able to access https link: https://localhost:5601. Log in as elastic user (password from step 3)


Welcome to Elastic
Username
elastic
Password
Log in

7. Go to Dev Tools under Management Tab



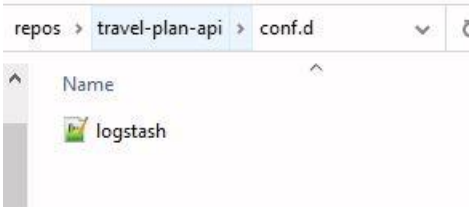
8. Create logstash_write_role in dev tab:

```
POST /_security/role/logstash_write_role
{
  "cluster": [
    "monitor",
    "manage_index_templates"
  ],
  "indices": [
    {
      "names": [
        "micro*", "log*", "metric*"
      ],
      "privileges": [
        "write",
        "create_index"
      ],
      "field_security": {
        "grant": [
          "*"
        ]
      }
    }
  ],
  "run_as": [],
  "metadata": {},
  "transient_metadata": {
    "enabled": true
  }
}
```

9. Create logstash_writer user. NOTE: for password field you can enter any password, I just use logstash_system user password as default.

```
POST /_security/user/logstash_writer
{
 "username": "logstash_writer",
 "roles": [
  "logstash_write_role"
 ],
 "full_name": null,
 "email": null,
 "password": "<logstash_system password>",
 "enabled": true
}
```

10. Go to logstash.conf under travel-plan-api/conf.d



11. Open logstash.conf file. Update logstash_writer password with logstash_system password

```
output {
    elasticsearch {
        hosts => ["elasticsearch:9200"]
        index => "%{appName}-%{+YYYY.MM.dd}"
        manage_template => false
        document_type => "appLogs"
        ssl => true
        cacert => '/etc/logstash/config/ca.crt'
        ssl_certificate_verification  => true
        user => logstash_writer
        password => 85VSkrzCE6VwEXA4OJ63
    }
```

12. Restart docker-compose