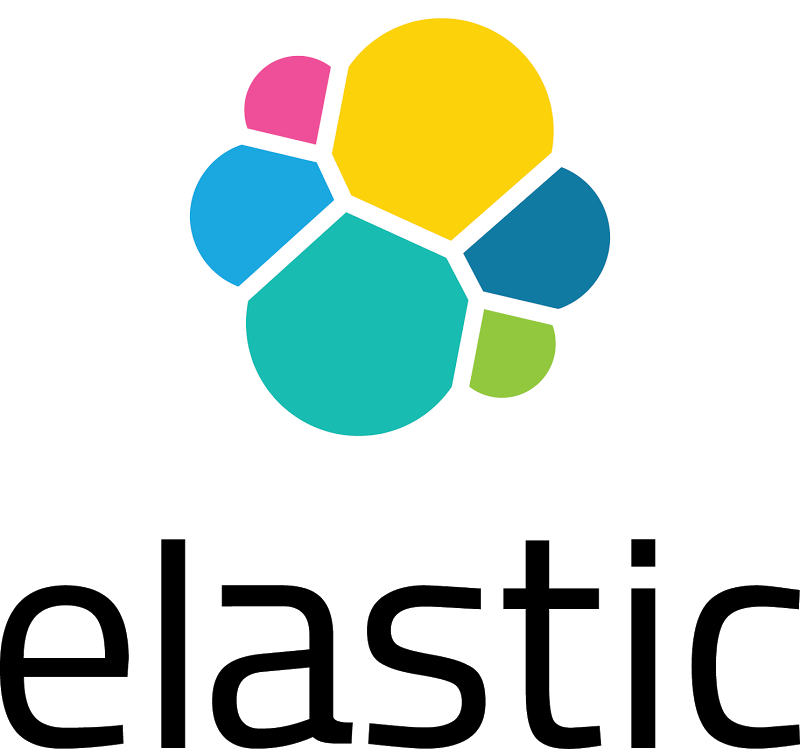
Security 5.5 Hands On Lab ****

## Goal:

To create a basic configuration for X-Pack Security for Elasticsearch and Kibana using the Native Realm.

## Step 1: Create and Test Role and User for Kibana

|  |  |
| --- | --- |
| 1. | Log into your Kibana instance, using elastic/changeme as username/password |
| 2. | The new user we are creating will be responsible for reporting on flight data. We have an index called flights-\* that contains some example data we will use throughout these exercises. It should already be mapped to an index pattern in Kibana. |
| 3. | Click on the Management icon on the left bar and then select Roles under the Security section. You can now see a list of the roles that are available.  One of these is kibana\_user, which provides access to the .kibana index, but not any data. We can use this for our kibana user, but will need to create a role that provides just read access to the flights-\* index pattern.  Click on the Create Role button in the top right corner to create this new role. This opens up a screen like shown below.    Give the role the name flights\_admin and grant read only privileges to the flights-\* index pattern. Then click Save. |
| 4. | Now select Users in the menu at the top. This shows a list of the currently defined users. Click on the Create User button in the top right corner.  Create a user with the name flights\_admin\_user and assign the roles kibana\_user and flights\_admin to this user. Pick a suitable password that is at least 6 characters long and provide an email address.    Then click Save. |
| 5. | Log out and then verify it is possible to log in as the newly created flights\_admin\_user. (ALSO CAN USE A NEW PRIVATE BROWSER WINDOW AND SWITCH BETWEEN THEM) |
| 6. | Click on the Dev Tools icon on the left bar. This opens up the Console interface which allows us to work with data in Elasticsearch.    GET /flights-\*/\_search  {  "query": {  "match\_all": {}  }  }  Type in the text shown above and click in the green arrow. Verify that this brings up results in the right pane and that the total number of hits is 5349111.    Now attempt to delete one of the records by typing  DELETE /flights-2015.01/flights/AVi2Yfzs0lp\_JbjrMG7Z  in the left pane and click on the green arrow.  As this user only have read privileges against this index pattern, this should result in a security\_exception. X-Pack Security has protected the data from being modified by this unauthorized user. |
| 7. | Make sure to set flights-\* as the default index pattern for the user flights\_admin\_user. Note that you will also need to change the time frame when using the data potentially. The default is “Last 15 minutes”. |

## Step 2: Field and Doc Level Security

For this exercise we are going to use the flights-\* index again. This data set has lots of fields available, and we are going to lock them down with field level security. We are also going to create document level security based on a query.

|  |  |
| --- | --- |
| 1. | If you already have a Console or Kibana session open, choose “Logout” in the lower left hand corner. Login using elastic/changeme  Click on the Management icon on the left bar and then select Roles under the Security section. Click on the Create Role button in the top right corner to create this new role. This opens up a screen like shown below.    Create a role names flights\_field\_level and give this read and view\_index\_metadata privileges on the flights-\* index pattern.  Remove the \* field specification and explicitly give the role access to the following fields:   * DEST\_AIRPORT\_ID * DEST\_CITY\_NAME * ORIGIN\_AIRPORT\_ID * ORIGIN\_CITY\_NAME * DEP\_DELAY * ARR\_DELAY * CARRIER * @timestamp   Make sure the other fields are left out as we want to restrict access to these.  Click Save. |
| 2. | Go to Users and click Create User.    Create a new user named flights\_field\_user and assign this user the kibana\_user and flights\_field\_level roles. |
| 3. | Log out and then log back in as flights\_field\_user. Go to Discover and verify that you only have access to the fields defined in flights\_field\_level. You should notice, however, that you can view the index metadata, just not the data in the fields you have access to. |
| 4. | Log out again and log back in as the elastic super user.  Go to Discover and view the flights-\* data. Verify that all fields are visible for this user. |
| 5. | Go to Management and select Security, then Roles. We are now going to create a new role, flights\_AA\_role, where we will use document level security to restrict access only documents where the carrier field is “AA”.    Assign the role read and view\_index\_metadata privileges and specify the following query:  {"match": {"CARRIER": "AA"}}  Click Save. |
| 6. | Now go to Users and create a new user named flights\_aa\_user, which is associated with the kibana\_user and flights\_aa\_role roles. |
| 7. | Log out and then log in again as flights\_aa\_user. Go to Discover and view the flights-\*. Do a query to verify the document count is now much smaller (**681,925**  ) and includes only documents whose carrier is ‘AA’.  This search in console:  GET /flights-\*/\_search  {  "query": {  "match\_all": {}  }  } |
| 8. | Congrats! You are done with the lab! If you have time, try creating other types of roles and users to restrict data access. You could do it by airport, airline, etc. Or create users that can only access numeric fields for analysis. |
| 9. | Make sure you log back in as elastic for the next lab. |