Elasticsearch is used for many purposes, it is used by many organizations to store and retrieve intricate data structures which are serialized as JSON documents. Technically, JSON documents (Data objects) that are stored in the elastic search, every field in the data is indexed by default. The stored documents can be retrieved, accessed and update data from any node in the cluster based on the authorized access of the user. Also, user can perform certain operations based on role-based access control on the data.

The misuse case mainly focused on the unauthorized access to elastic cluster, logging into master cluster by stealing user credentials. Sometimes, taking preventions from stealing user credentials is not enough and so came up with kind of second layer protection that is on preventing way to control what data users have access to and what tasks they can perform based on the security privileges mentioned in the page <https://www.elastic.co/guide/en/elastic-stack-overview/6.4/security-privileges.html>

**Security requirements:**

* Role-based access control should be enabled to prevent users from performing unauthorized CURD actions on the data
* Enable the IP filtering feature to prevent blacklisted IP’s from joining the cluster or accessing the data documents. For example, the application clients, node clients, or transport clients that are attempting to join the cluster without permissions.

Elasticsearch seems to have these security features that are packaged in X-Pack module. These features must be enabled by the user based on the organization usage. Role based access controls and security privileges are very clearly documented in their documentation page. [Role based access controls] (<https://www.elastic.co/guide/en/elastic-stack-overview/6.4/authorization.html>) and [Cluster Security Privileges] <https://www.elastic.co/guide/en/elastic-stack-overview/6.4/security-privileges.html>.

### From my observation, Elasticsearch failed in securing the customer data which is stored in the elastic cluster from the Ransomware attack. [Ransomware Attack on Elastic Cluster](<https://www.zdnet.com/article/elasticsearch-ransomware-attacks-now-number-in-the-thousands/>). But, they have a feature of IP filtering through which only whitelisted ones only can access and perform CRUD operations on data documents. The way this feature works is documented in the [Ip filtering page] (<https://www.elastic.co/guide/en/elastic-stack-overview/6.4/ip-filtering.html>)

### ##### User access to the elastic cluster, role based access to data and actions performing on the data.

### Task 1 - Description, link to misuse case, list security requirements, reflection (including links to documentation)

### Elasticsearch is used for many purposes, it is used by many organizations to store and retrieve intricate data structures which are serialized as JSON documents. Technically, JSON documents (Data objects) that are stored in the elastic search, every field in the data is indexed by default. The stored documents can be retrieved, accessed and update data from any node in the cluster based on the authorized access of the user. Also, user can perform certain operations based on role-based access control on the data.

### The misuse case mainly focused on the unauthorized access to elastic cluster, logging into master cluster by stealing user credentials. Sometimes, taking preventions from stealing user credentials is not enough and so came up with kind of second layer protection that is on preventing way to control what data users have access to and what tasks they can perform based on the security privileges mentioned in the documentation.

### Security Requirements:

### \* Encrypting the User credentials that are sent for authentication between Elasticsearch and a Lightweight Directory Access Protocol (LDAP) realm.

### \* Role-based access control should be enabled to prevent users from performing unauthorized CURD actions on the data.

### \* Enable the IP filtering feature to prevent blacklisted IP’s from joining the cluster or accessing the data documents. For example, the application clients, node clients, or transport clients that are attempting to join the cluster without permissions.

### Elasticsearch seems to have these security features that are packaged in X-Pack module. These features must be enabled by the user based on the organization usage. Validating the user authentication with LDAP realm and encrypted user credentials data are communicated between elastic search and LDAP server which is clearly explained in Elasticsearch documentation [Encrypting communications between Elasticsearch and LDAP](https://www.elastic.co/guide/en/elasticsearch/reference/6.4/configuring-tls.html#tls-ldap). Role based access controls and security privileges are very clearly documented in their documentation [Role based access controls](https://www.elastic.co/guide/en/elastic-stack-overview/6.4/authorization.html) page and [Cluster Security Privileges] (https://www.elastic.co/guide/en/elastic-stack-overview/6.4/security-privileges.html) page. The details of enabling and disabling of IP filtering and in what way this feature can secure their cluster/node from joining the unauthorized application clients/ nodes is documented in the [Ip filtering page](https://www.elastic.co/guide/en/elastic-stack-overview/6.4/ip-filtering.html).