5: Security

***Section Description (from the outline):*** This section covers securing an ElasticSearch cluster

|  |
| --- |
| **Metadata**: Spot the problem, highlight it, and design the solution in 3 core steps  (To be covered in the video) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Video Number** | **Video Title** | **Problem / Solution (Not more than 50 words)** | **Step 1 (Not more than 10 words)** | **Step 2(Not more than 10 words)** | **Step 3(Not more than 10 words)** |
| 5.1 | Authentication and Authorization | While many engineers understand the basics of authentication and authorization, itʼs necessary to exceed the basics to properly implement security in an ElasticSearch cluster | Understand built-in users in ElasticSearch | Learn to change and disable default passwords for built-in users | Look at external security constructs that play well with ElasticSearch |

Metadata for Section 5

Section Description (from the outline): Describe what this section intends to cover- decided during outline discussion.

|  |
| --- |
| **Metadata**: Spot the problem, highlight it, and design the solution in 3 core steps  (To be covered in the video) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Video Number** | **Video Title** | **Problem / Solution (Not more than 50 words)** | **Step 1 (Not more than 10 words)** | **Step 2(Not more than 10 words)** | **Step 3(Not more than 10 words)** |
|  |  |  |  |  |  |
| 5.2 | User Management API | Of all the security constructs (realms) in ElasticSearch, arguably the most popular is the Native Realm. Understanding the native realm is critical to oneʼs ability to effectively implement security in ElasticSearch | Learn about the Native Realm in User Management API | Gain understanding of password management | See examples of User Management API |
| 5.3 | Authorization | While authentication deals with login credentials, authorization handles what an authenticated person can and canʼt do. Understanding authorization is critical for cluster security and management | Gain understanding of authorization in ElasticSearch | Learn about role based access control | Get thorough authorization breakdown |
| 5.4 | Communication between Nodes | All information passed between nodes, including passwords, are done in plain text. For this reason, in production, node to node encryption is required. | Understand the requirements for node to node communication | Learn how SSL is used to encrypt traffic between nodes | Create a certificate signing request with certgen |
| 5.5 | IP Filtering | One viable security option involves controlling the ip addresses  that can access a production cluster, as well as setting up nodes to communicate via private ip addresses | Understand how IP filtering works in ElasticSearch | Learn options of disabling http versus disabling transport | See example of dynamically filtering a subnet of IPs |