# KPLABS Course

## Splunk 2021 - Beginner to Architect

## Domain 9

**ISSUED BY**

Zeal

**REPRESENTATIVE**

instructors@kplabs.in

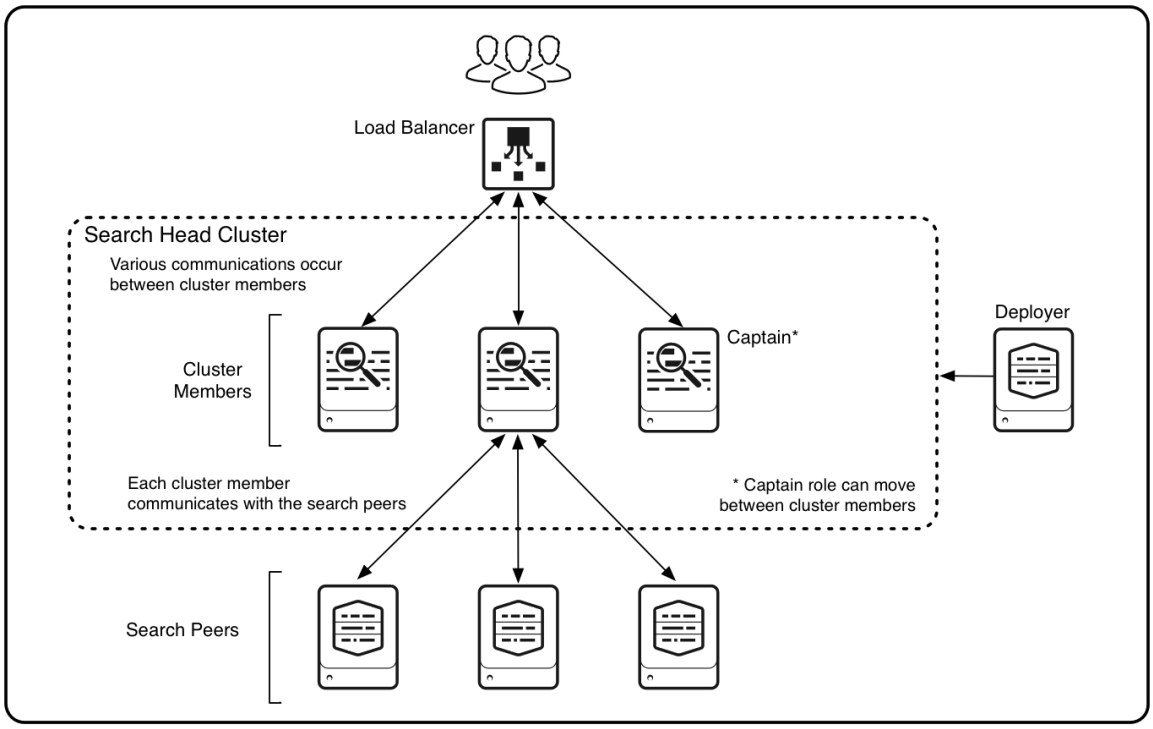
# Domain 9 - Search Head Clustering

## Module 1: Overview of Search Head Clusters

A search head cluster is a group of Splunk Enterprise search heads that serves as a central resource for searching

You can run the same searches, view the same dashboards, and access the same search results from any member of the cluster.

The following diagram denotes the architecture of the Search Head Clustering setup.




It is important to understand what type of data gets replicated by default.

Some of the replicated data include:

- Alert Actions
- Data Models
- Workflow actions
- Saved Searches
- Macros
- Lookups
- Event Types
- Many Many more

## Module 2: Pushing Artifacts through Deployer

The deployer is a Splunk Enterprise instance that you use to distribute apps and certain other configuration updates to search head cluster members. The set of updates that the deployer distributes is called the configuration bundle.

The deployer distributes the configuration bundle in response to your command, according to the deployer push mode that you select. The deployer also distributes the bundle when a member joins or rejoins the cluster.

The deployer has these main roles:

- It handles migration of app and user configurations into the search head cluster from non-cluster instances and search head pools.

- It deploys baseline app configurations to search head cluster members.

- It provides the means to distribute non-replicated, non-runtime configuration updates to all search head cluster members.

You do not use the deployer to distribute search-related runtime configuration changes from one cluster member to the other members. Instead, the cluster automatically replicates such changes to all cluster members. For example, if a user creates a saved search on one member, the cluster automatically replicates the search to all other members.