

Splunk Enterprise Cluster Administration

Course Summary:

The course provides the fundamental knowledge of deploying and managing Splunk Enterprise indexer and search head clusters.

Course Duration:

13.5 Hours (3 Days)

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration
- Troubleshooting Splunk Enterprise

Additional courses and/or knowledge in these areas are also highly recommended:

- Enriching Data with Lookups
- Data Models

Course Outlines:

Module 1 – Overview of Large-scale Splunk Deployment

- Identify factors that affect large-scale deployment design
- Describe approaches to scaling Splunk Enterprise
- Configure Splunk License Manager

Module 2 – Deploying Single-site Indexer Clusters

- Identify indexer cluster states
- Define replication factor and search factor
- Implement a single-site indexer cluster

Module 3 – Deploying Multisite Indexer Clusters

- Define site replication factor and site search factor
- Define search affinity
- Implement a multisite indexer cluster

Module 4 – Updating Indexer Cluster Peer Configurations

- Distribute configurations and apps across peers

Module 5 – Managing and Monitoring Indexer Clusters

- Enable replication for clustered indexes
- Configure Monitoring Console for indexer cluster environment

Module 6 – Configuring Indexer Discovery on Forwarders

- Configure indexer discovery
- Configure indexer acknowledgment
- Configure forwarder site failover

Module 7 – Deploying Search Head Clusters

- Configure a search head cluster
- Connect clustered and non-clustered indexers

Module 8 – Managing and Monitoring Search Head Clusters

- Deploy configuration bundles to search head cluster members
- Manage captaincy and member addition, removal and upgrades

Module 9 – Using KV Store in a Search Head Cluster

- Enable KV Store collection replication in a search head cluster
- Monitor KV Store status with Monitoring Console

Module 10 - Implementing Cluster Manager Redundancy

- Configure Cluster Manager redundancy in a multisite indexer cluster

Audience:

- Splunk Administrators