Splunk Cluster Administration

This 13.5-hour course is for experienced Splunk Enterprise administrators new to Splunk Clusters. The course provides the fundamental knowledge of deploying and managing Splunk Enterprise in a clustered environment.

While Splunk Clusters are supported in Windows environments, the class lab environment is running Linux instances only.

Course Topics

- Large-scale Splunk Deployment Overview
- Single-site Indexer Cluster
- Multisite Indexer Cluster
- Indexer Cluster Management and Administration
- Forwarder Configuration
- Search Head Cluster
- Search Head Cluster Management and Administration
- KV Store Collection and Lookup Management
- SmartStore Implementation Overview

Prerequisite Knowledge

To be successful, students should have a solid understanding of the following courses:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration
- Troubleshooting Splunk Enterprise

Course Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

- Identify factors affecting large-scale Splunk deployments
- Deploy and configure single- and multi-site indexer clusters
- Deploy and configure a Splunk search head cluster
- Deploy apps and configuration bundles in Splunk clusters
- Manage KV store collections and lookups in Splunk clusters
- Monitor and identify clustering issues with Monitoring Console
- Scale Splunk indexer cluster with SmartStore

Module 1 – Large-scale Splunk Deployment Overview

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

Module 2 – Single-site Indexer Cluster

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

Module 3 – Multisite Indexer Cluster

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

Module 4 – Indexer Cluster Management Administration

- Distribute configurations and apps across peers
- Enable replication for clustered indexes
- Configure Monitoring Console for indexer cluster environment

Module 5 – Forwarder Management

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

Module 6 – Search Head Cluster

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

Module 7 – Search Head Cluster Management and Administration

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

Module 8 – KV Store Collection Management

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

Module 9 – SmartStore Implementation

- Identify use cases for deploying SmartStore
- Implement SmartStore in indexer cluster

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.