



# Splunk Cluster Administration

This 3-virtual day course is for an experienced Splunk Enterprise administrator who is new to Splunk Clusters. The course provides the fundamental knowledge of deploying and managing Splunk Enterprise in a clustered environment. It covers installation, configuration, management, and monitoring of Splunk clusters.

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

## Course Prerequisites

Required:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

Strongly Recommended:

- Troubleshooting Splunk Enterprise
- Working Linux knowledge
- 3 months of hands-on Splunk administration experience

## Class Format

Instructor-led lecture with labs.

Delivered via virtual classroom or at your site.

## Course Modules

### Module 1 – Large-scale Splunk Deployment Overview

- Factors that affecting deployment design
- How Splunk Enterprise can scale
- Splunk License Master

### Module 2 – Single-site Indexer Cluster

- How Splunk single-site indexer clusters work
- Indexer cluster components and terms
- Splunk single-site indexer cluster configuration
- Splunk indexer cluster log channels

### Module 3 – Multisite Indexer Cluster

- How Splunk multisite indexer clusters work
- Multisite indexer cluster terms
- Multisite indexer cluster configuration
- Optional multisite indexer cluster configurations

### Module 4 – Indexer Cluster Management and Administration

- Peer offline and decommission
- Master app bundles
- Indexer cluster storage utilization options
- Site mapping
- Monitoring Console for indexer cluster environment

### Module 5 – Forwarder Management

- Indexer discovery
- Optional indexer discovery configurations
- Volume-based forwarder load balancing

### Module 6 – Search Head Cluster

- Splunk search head cluster overview
- Search head cluster configuration

### Module 7 – Search Head Cluster Management and Administration

- Search head cluster deployer
- Captaincy transfer
- Search head member addition and decommissioning
- Monitoring Console for Search Head Cluster

### Module 8 – KV Store Collection and Lookup Management

- KV Store collection in Splunk clusters
- KV Store monitoring with Monitoring Console

### Module 9 – SmartStore Implementation

- SmartStore architecture overview
- Deploy and manage SmartStore

## About Splunk Education

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

### Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to <http://www.splunk.com/goto/education>

To contact us, email [education\\_AMER@splunk.com](mailto:education_AMER@splunk.com)

## About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at [www.splunk.com](http://www.splunk.com) to download your own free copy.

Splunk Inc.  
270 Brannan  
San Francisco, CA 94107  
866.GET.SPLUNK  
(866.438.7758)  
[sales@splunk.com](mailto:sales@splunk.com)  
[support@splunk.com](mailto:support@splunk.com)