



## Core Implementation

This course is an in-person, five-day instructor-led class that covers how to make Splunk Enterprise run efficiently in setting up large clustered Splunk environments using best practices. The class evaluates your ability to successfully deploy Splunk Enterprise in several scenarios, including Search Head Cluster, Indexer Cluster, and distributed environments. We also create advanced dashboards and alerts to ensure customers get the most value from their Splunk environment.

### Course Topics

- Splunk architecture
- Monitoring Console
- Deployment Server
- LDAP integration
- Collecting and forwarding data
- Indexing and Searching
- Clustering indexers
- Clustering Search Heads

### Course Format

Instructor-Led or Virtual Instructor-Led: lectures with hands-on, graded labs

### Prerequisite Certification(s):

*Splunk Core Certified Power User*  
*Splunk Core Certified Advanced Power User (or recommended courses\*)*  
*Splunk Enterprise Certified Admin*  
*Splunk Enterprise Certified Architect*

### Prerequisite Course(s):

*Core Consultant Labs*  
*Services Core Implementation*  
*Required:*  
Splunk Certified Architect +

## Course Objectives

### Module 1 – Deploying Splunk

- Introduce the Splunk Validated Architectures
- Review how Splunk can grow from a standalone environment to a distributed environment with indexer and search head clustering
- Explain High Availability and Disaster Recovery
- Discuss migrating Splunk from on-premises to the Cloud

### Module 2 – Monitoring Console

- Discuss the best instance to configure as the Monitoring Console
- Configure the MC for a single or distributed environment
- Examine how the MC uses the server roles and groups assigned to instances
- Discuss health checks and how they are run

### Module 3 – Configuration Management

- Define deployment apps
- Provide overview of Deployment Server
- Describe deployment system configuration
- Discuss how to manage Deployment Server at scale

### Module 4 – Access & Roles

- Discuss how to manage Deployment Server at scale
- Identify authentication methods
- Describe LDAP concepts and configuration
- Discuss SAML and SSO options
- Define roles and how they are used to protect data

### Module 5 – Data Collection

- Examine Splunk to Splunk (S2S) communication and the different ways data is sent from forwarder to indexer
- Describe the types and configuration of data inputs
- Discuss ways to troubleshoot data inputs

### Module 6 – Indexing

- Review indexing artifacts and locations
- Discuss event processing and data pipelines
- Understand the underlying text parsing and indexing process
- Examine data retention controls



### Module 7 – Search

- Examine the inter-workings of a search
- Discuss how to use search job inspection
- Look at the different search types and how to maximize search efficiency
- Review sub-searches and how they work
- Examine some example searches and how to make them more efficient

### Module 8 – Index Clustering

- Provide an architecture overview
- Describe deployment and component configuration
- Review upgrade strategy
- Discuss data buckets and lifecycle
- Examine failure modes and recovery processes
- Introduce multi-site clustering
- Explain migration procedures

## 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 Splunk Education's course offerings, or to register for a course, go to <http://www.splunk.com/education>

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

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

[Contact sales](#)