splunk>

# 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 Prerequisites

Splunk Certified Architect +

## Class Format

Instructor-led lecture with labs, delivered in person.

## 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
- Lab 0: Grade Me

**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
- Lab 1 - Discovery

**Module 3 – Configuration Management**

- Define deployment apps
- Provide overview of Deployment Server
- Describe deployment system configuration
- Discuss how to manage Deployment Server at scale
- Lab 5: Scale DS

**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
- Lab 2: LDAP Integration

**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
- Lab 3: Triage broken forwarder

**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
- Lab 4: Triage indexing issue

**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
- Understand migration procedures
- Lab 6: Upgrade Index Cluster
- Lab 7: Expand Cluster & Migrate Indexer data

**Module 9 – Search Head Clustering**

- Provide overview of Search Head clustering
- Explain how to manage and deploy a cluster
- Describe content management using the Deployer
- Review the role of cluster members and the Captain
- Lab 8 – Install SHC

**Appendix A – REST API**

- Define the Splunk REST API
- Discuss requests, endpoints, and namespaces
- Examine tools and methods for using the API

splunk>

| Module # | Module Name | Module Length | Lab Name | Lab Length | Day |
|---|---|---|---|---|---|
| Module 0 | Introductions | 0:30 | | | Day 1 |
| Lunch | | | | 1:00 | |
| Module 1 | Deploying Splunk | 0:45 | Lab 0 | 0:05 | |
| Module 2 | Monitoring Console | 0:45 | Lab 01: Discovery | 1:30 | |
| Module 3 | Configuration Management | 2:00 | Lab 05: Scale DS | 2:30 | Day 2 |
| Lunch | | | | 1:10 | |
| Module 4 | Access & Roles | 1:20 | Lab 02: LDAP Integration | 1:30 | |
| Module 5 | Data Collection | 1:45 | Lab 03: Triage broken forwarder | 2:30 | Day 3 |
| Lunch | | | | 1:00 | |
| Module 6 | Indexing | 1:40 | Lab 04: Triage indexing issue | 2:30 | |
| Module 7 | Search | 1:40 | | | Day 4 |
| Module 8 | Index Clustering Part 1 | 1:25 | Lab 06: Upgrade Index Cluster | 1:00 | |
| | Lunch | | | 1:00 | |
| | Index Clustering Part 2 | 1:45 | Lab 07: Expand Cluster & Migrate Indexer data | 1:30 | |
| Module 9 | Search Head Cluster | 2:00 | Lab 08: Install SHC | 3:00 | Day 5 |

## 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 course offerings or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education_AMER@splunk.com

Splunk Inc.
250 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@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 to download your own free copy