



Architecting Splunk

This 9-hour course focuses on large enterprise deployments. Students learn steps and best practices for planning, data collection and sizing for a distributed deployment. Workshop-style labs challenge students to make design decisions about an example enterprise deployment.

Course Topics

- Splunk deployment planning
- Index and resource planning
- Clustering Overview
- Forwarder and Deployment
- Integration
- Performance Monitoring and Tuning
- Use Cases

Prerequisite Knowledge

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

- Fundamentals 1 & 2

Or the following single-subject courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions

Students should also understand the following courses:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration
- Splunk Enterprise Cluster Administration

Course Format

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

Course Objectives

Module 1 – Splunk Deployment Planning

- Define the responsibilities of a Splunk Architect
- Introduce the Splunk deployment planning process and tools
- Identify the information that is needed for deployment decisions
- Identify use cases
- Provide lists and resources to aid in collecting requirements
- Review the network topology for Buttercup Games

Module 2 – Index Design

- Define index implementation
- Design indexes
- Estimate storage requirements for indexes
- Identify relevant apps and document impact on inputs and indexes

Enterprise Deployments

Module 3 – Resource Planning

- Determine sizing based on Splunk usage
- Define reference server requirements for Indexers, Search heads, and other Splunk
- Describe deployment options such as virtualization and cloud
- Describe the impact of acceleration and apps on resource sizing

Module 4 - Clustering Overview

- Review indexer clustering, including single-site and multi-site clusters
- Define clustering requirements, best practice, and SmartStore
- Review search head clustering
- Defined search head clustering requirements and best practices

Module 5 - Forwarder and Deployment Best Practices

- Review forwarder types
- Manage forwarder installation in an enterprise environment using Deployment Server, Cluster Manager, and SHC Deployer

Module 6 - Integration

- Describe and identify common integration methods

Module 7 – Performance Monitoring and Tuning

- Use the Monitoring Console (MC) to track performance of your test environment before going into production
- Identify options to optimize the production environment
- Overview of Workload Management

Module 8 – Use Cases

- Provide example architecture topologies
- Discuss different architecture options based on use case

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

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

[Contact sales](#)