Core Implementation

This expert-level course is an immersive five-day assessment-based bootcamp used to give attendees the opportunity to cement their knowledge in working with the Splunk core platform effectively and at-scale using Professional Services (PS) best-practice techniques. **This course represents a significant step-up in difficulty versus earlier courses in a Splunk consultant's learning path. Passing the course is only possible if the required preparation and practice is put into place before attending.**

In-person (or virtual) instructor-led training will cover how to make Splunk Enterprise run efficiently in large clustered environments and will give a more in-depth understanding of the inner-workings of Splunk.

Attendees will apply best-practice techniques in an attempt to complete a number of practical assessment labs **(individually — with no peer and minimal instructor technical assistance)**. These labs pose various technical challenges in simulated distributed customer environments.

To be successful during the assessed labs, candidates will need to demonstrate a masterful grasp on how to manage configuration at scale, troubleshoot problems, perform environment discovery, and ultimately understand what is necessary to make Splunk Customers successful, all under time pressure. This includes being able to engage with customers with an instructional and collaborative PS mindset, to fully clarify requirements before planning and implementing solutions.

Course Format

Instructor-led or virtual instructor-led lectures with a hands-on graded lab following each presentation module.

Course Topics

- Splunk architecture
- Monitoring Console
- Configuration Management
- Authentication, Authorization & LDAP integration
- Collecting and forwarding data
- Indexing and Searching
- Clustering indexers
- Clustering Search Heads

Prerequisite Certifications:

To qualify for registration, candidates must hold all of the following certifications —

- Splunk Core Certified Power User
- Splunk Core Certified Advanced Power User*
- Splunk Enterprise Certified Admin
- Splunk Enterprise Certified Architect

Prerequisite Courses:

To qualify for registration and be successful in this highly technically complex course, candidates must have completed —

- Core Consultant Labs

Experience in attending a PS shadowing engagement is not required, but is highly recommended, as is extensive practice in a lab-based environment

**Completion of the following courses are considered an acceptable substitute for the Splunk Core Certified Advanced Power User badge:*

- *Using Fields*
- *Working with Time*
- *Comparing Values*
- *Result Modification*
- *Leveraging Lookups and Subsearches*
- *Correlation Analysis*
- *Multivalue Fields*
- *Search Optimization*
- *Creating Knowledge Objects*
- *Creating Field Extractions*
- *Enriching Data with Lookups*
- *Data Models*
- *Introduction to Dashboards*
- *Dynamic Dashboards*

Prerequisite Linux Skills

Attendees must be comfortable and competent in core Linux skills such as:

- File & permission management
- Service configuration
- Installation best-practices
- ssh & scp

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

splunk>

Course Objectives

Module 1 – Deploying Splunk

- Introduce the Splunk Validated Architectures

Module 2 — Monitoring Console

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

Module 4 — Access and 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 inner-workings of a search
- Discuss how to use search job inspection
- Look at the different search types and how to maximize search efficiency
- Review subsearches and how they work
- Examine some sample 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