SPLUNK EDUCATION

# Splunk Enterprise Deployment Practical Lab

Summary

This course is for Splunk Administrators and aspiring Architects.

The course requires students to build a mock deployment that meets specified requirements, while demonstrating a thorough understanding of Splunk recommended practices. Upon completion, the instructor will evaluate the work and provide constructive feedback.

Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
    - Intro to Splunk
    - Using Fields
    - Introduction to Knowledge Objects
    - Creating Field Extractions
    - Scheduling Reports and Alerts
    - Visualizations
    - Introduction to Dashboards
    - Splunk Enterprise System Administration
    - Splunk Enterprise Data Administration
    - Troubleshooting Splunk Enterprise
    - Splunk Cluster Administration
    - Architecting Splunk Enterprise Deployments
- Additional courses and/or knowledge in these areas are also highly recommended:
    - Basic Linux skills
    - Editing text files in Linux using vi or nano

Format:
- Instructor-led
- Timed Lab

Duration: 24 Consecutive Hours

Audience:
- Administrators
- Aspiring Architects

Course Outline

Instructor Led Introduction

- Explanation of the proof-of-concept scenario
- Deployment requirements (statement of work)
- Topology and hostnames
- Advice for success

24 Hour Independent Timed Lab

- Build a fully functional Splunk environment that satisfies the requirements specified in the document provided by the instructor.
- The following skills are required to successfully complete this course::
    - Installing Splunk
    - Configuring an indexer cluster
    - Creating indexes with high availability
    - Managing forwarders with a deployment server
    - Testing and configuring data inputs

- ○ Creating a custom sourcetype
- ○ Creating field extractions
- ○ Installing apps and add-ons
- ○ Creating reports
- ○ Creating simple dashboards
- ○ Monitoring a Splunk environment

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.