

**SPLK-DPLYPRACLAB: Splunk Enterprise  
Deployment Practical Lab**

Course Code: SPLK-DPLYPRACLAB

Duration: 1 day

Instructor-led Training (ILT) | Virtual Instructor-  
led Training (VILT)**OVERVIEW**

This 24-hour practical lab exercise is designed to take you through the tasks of a complete mock deployment. Each participant is given access to a specified number of Linux servers and a set of requirements. Participants then perform a mock deployment according to requirements which adhere to Splunk Deployment Methodology and best-practices.

**SKILLS COVERED**

- Please refer to course overview.

**WHO SHOULD ATTEND?**

Everyone can attend.

**PREREQUISITES**

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

- Splunk Fundamentals 1
- Splunk Fundamentals 2

OR the following single-subject courses:

- What Is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Introduction to Knowledge Objects
- Creating Field Extractions
- Introduction to Dashboards

Students should also have completed the following courses:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration
- Architechting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Enterprise Cluster Administration

**MODULES****Module 1: Installation and Infrastructure**

- Install forwarders, indexers, search head, deployment server and license master

**Module 2: Configuration and Collection**

- Configure an index cluster
- Deploy all specified configurations via deployment server
- Configure inputs from forwarders
- Configure and confirm index-time knowledge
- Create search time field extractions

**Module 3: Searching and Reporting**

- Create searches for each required use case

**END OF PAGE**