Splunk Deployment Practical Lab (SDPL)

ID SDPL **Prix** sur demande **Durée** 1 jour

Cette formation prépare à la/aux certifications

Splunk Enterprise Certified Architect (SPECA)

Pré-requis

- Splunk Fundamentals 1 (Retired)
- Splunk Fundamentals 2 (Retired)

Or the following single-subject courses:

- What is Splunk? (Retired)
- Intro to Splunk (ITS)
- Using Fields (SUF)
- Scheduling Reports & Alerts (SRA)
- Visualizations (SVZ)
- Intro to Knowledge Objects (IKO)
- Creating Field Extractions (CFE)
- Introduction to Dashboards (ITD)

Students should also understand the following modules:

- !Splunk Enterprise System Administration (SESA)
- Splunk Enterprise Data Administration (SEDA)
- Architecting Splunk Enterprise Deployments (ASED)
- Troubleshooting Splunk Enterprise (TSE)
- Splunk Enterprise Cluster Administration

Objectifs

Installation and Infrastructure

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

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 fields

Searching and Reporting

- Create searches for each required use case
- Get indexer event acknowledgements

Contenu

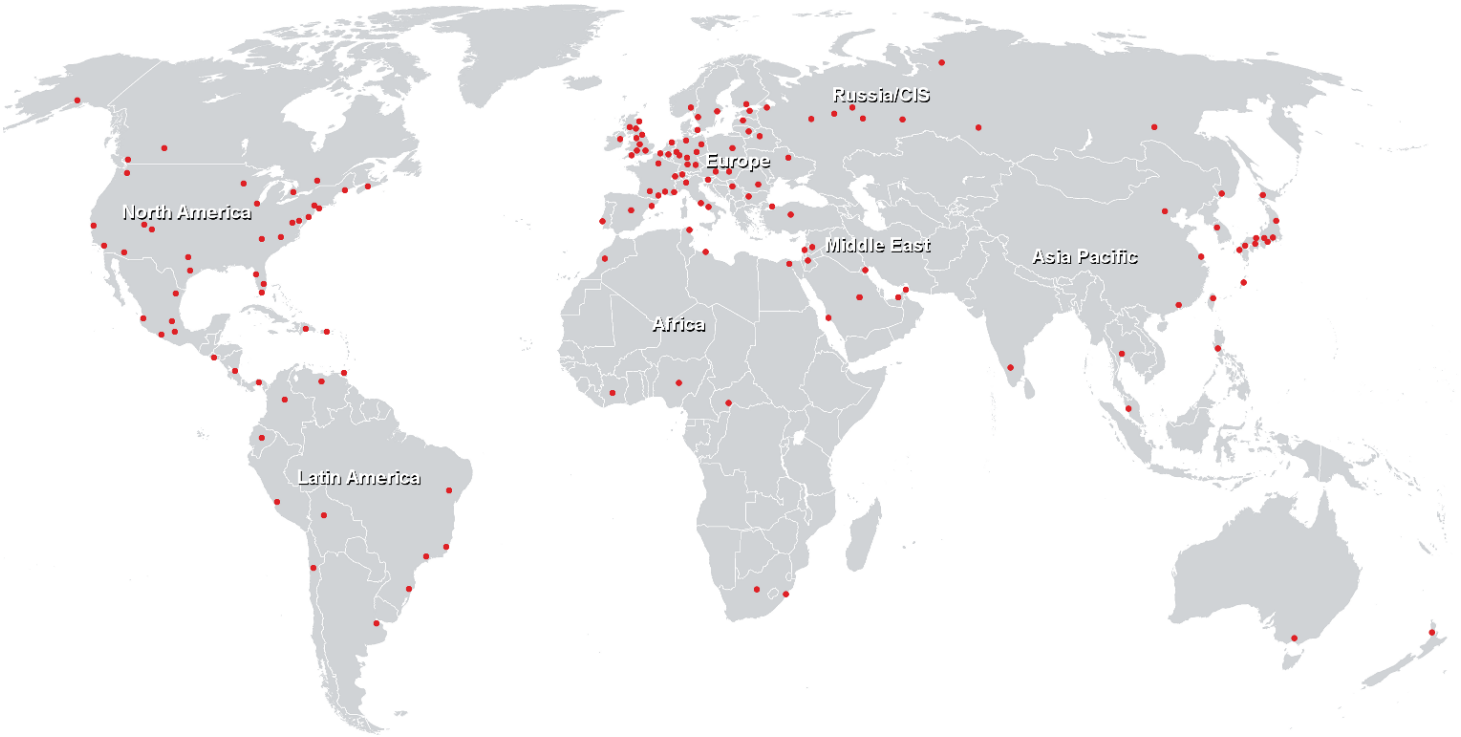
This 24-hour practical lab exercise is designed to take you through the tasks of a complete mock deployment. Each participant is given access to a specified number of Linux servers and a set of requirements. Participants then perform a mock deployment according to requirements which adhere to Splunk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

The instructor will introduce the lab challenge, give opportunities for discussion about the lab etc, provide student lab server details, explain how the assessment will be conducted, how to get support during the 24 hours etc. Then students are left to work for 24 hours on the technical lab challenge, which as pasted below in the trail, involves completing a number of tasks typically involved in establishing a Splunk distributed (on-prem) deployment and use-case implementation/initial data onboard. Once the 24 hours is up, the students' work is graded by the instructor to determine if the configuration work is up to the required standards and best practices are followed.

Students will have access to instructor for 4.5 hours, with time to then complete the lab activities and submit for grading.

Splunk Deployment Practical Lab (SDPL)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch