SPLK-ENTCADM8.2: Splunk 8.2 Cluster Administration

Course Code: SPLK-ENTCADM8.2
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This 3-virtual day course is for an experienced Splunk Enterprise administrator who is new to Splunk Clusters. The course provides the fundamental knowledge of deploying and managing Splunk Enterprise in a clustered environment. It covers installation, configuration, management, and monitoring of Splunk clusters. While Splunk Clusters are supported in Windows environments, the class lab environment is running Linux instances only.

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
- Leveraging Lookups and Subsearches
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards

Students should also have completed the following courses:

- Splunk System Administration
- Splunk Data Administration
- Troubleshooting Splunk Enterprise

MODULES

Module 1: Large-scale Splunk Deployment Overview

- Factors that affecting deployment design
- How Splunk Enterprise can scale
- Splunk License Master

Module 2: Single-site Indexer Cluster

- How Splunk single-site indexer clusters work
- Indexer cluster components and terms
- Splunk single-site indexer cluster configuration
- Splunk indexer cluster log channels

Module 3: Multisite Indexer Cluster

- How Splunk multisite indexer clusters work
- Multisite indexer cluster terms
- Multisite indexer cluster configuration
- Optional multisite indexer cluster configurations

Module 4: Indexer Cluster Management and Administration

- Peer offline and decommission
- Master app bundles
- Indexer cluster storage utilization options
- Site mapping
- Monitoring Console for indexer cluster environment

Module 5: Forwarder Management

- Indexer discovery
- Optional indexer discovery configurations
- Volume-based forwarder load balancing

Module 6: Search Head Cluster

- Splunk search head cluster overview
- Search head cluster configuration

END OF PAGE