Splunk Cluster Administration

This 13.5-hour 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.

Course Topics

- Large-scale Splunk Deployment Overview
- Single-site Indexer Cluster
- Multisite Indexer Cluster
- Indexer Cluster Management and Administration
- Forwarder Configuration
- Search Head Cluster
- Search Head Cluster Management and Administration
- KV Store Collection and Lookup Management
- SmartStore Implementation Overview

Prerequisite Knowledge

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 Sub-searches
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards

Student should also have completed the following courses:

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

Course Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

- Large-scale Splunk Deployment Overview
- Identify factors affecting large-scale Splunk deployments
- Set up Splunk indexer clusters
- Deploy and configure a Splunk search head cluster
- Add new nodes into an existing cluster
- Decommission nodes from an existing cluster
- Deploy apps and configuration bundles in Splunk clusters
- Manage KV store collections and lookups in Splunk clusters
- Monitor and identify clustering issues with Monitoring Console
- Scale Splunk indexer cluster with SmartStore

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 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

Module 7 – Search Head Cluster Management and Administration

- Search Head Cluster Deployer
- Captaincy Transfer
- Search Head Member Addition and Decommissioning
- Monitoring Console for Search Head Cluster

Module 8 – KV Store Collection and Lookup Management

- KV Store Collection in Splunk Clusters
- KV Store Monitoring with Monitoring Console

Module 9 – SmartStore Implementation

- SmartStore architecture overview
- Deploy and manage SmartStore

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