



Splunk Enterprise Cluster Administration

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.

Course Topics

- Large-scale Splunk Deployment Overview
- Single-site (high-availability) Indexer Cluster
- Multisite (disaster-recovery) Indexer Cluster
- Indexer Cluster Management and Administration
- Indexer Discovery Forwarder Configuration
- Search Head Cluster
- Search Head Cluster Management and Administration
- KV Store Collection and Lookup Management

Course Prerequisites

Required:

- Splunk System Administration
- Splunk Data Administration

Strongly Recommended:

- Troubleshooting Splunk Enterprise
- Architecting Splunk Enterprise Deployments
- Working Linux knowledge
- 3 months of hands-on Splunk administration experience

Class Format

Instructor-led lecture with labs.

Delivered via virtual classroom or at your site.

Course Modules

Module 1 – Large-scale Splunk Deployment Overview

- Factors that affecting deployment design
- Splunk cluster overview
- License Master

Module 2 – Single-site Indexer Cluster

- Splunk single-site indexer cluster configuration
- Optional single-site indexer cluster configurations

Module 3 – Multisite Indexer Cluster

- Splunk multi-site indexer cluster overview
- Multi-site indexer cluster configuration
- Optional multi-site indexer cluster configurations
- Cluster migration and upgrade considerations

Module 4 – Indexer Cluster Management and Administration

- Indexer cluster storage utilization options
- Peer offline and decommission
- Master app bundles

- Monitoring Console for indexer cluster environment

Module 5 – Forwarder Management

- Indexer discovery
- Optional indexer discovery configurations

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

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 of Splunk Education's course offerings, or to register for a course, go to <http://www.splunk.com/goto/education>

To contact us, email education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
270 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com