SPLUNK EDUCATION

Course Description

Splunk Enterprise System Administration

Summary

This course is for system administrators who are responsible for managing a Splunk Enterprise environment.

The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.

Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
  - Exploring Splunk Platform Ecosystem
  - Splunk User track

Format: Instructor-led

Duration: 12 hours

Audience: Administrators

Course Outline

Module 1 – Deploy Splunk

- Provide an overview of Splunk
- Identify Splunk Enterprise components and deployment types
- List Splunk installation prerequisites
- List the steps to install Splunk
- Use Splunk CLI commands
- Explore security recommended practices

Module 2 – Monitor Splunk

- Use Splunk Health Report
- Enable and use the Monitoring Console
- Use Splunk Diag and Rapid Diag

Module 3 – License Splunk

- Identify the different Splunk license types
- Describe license violations
- Install a Splunk License
- Configure a Splunk License Manager
- Configure License Peers
- Configure License Pools
- Manage License warnings
- Monitor license usage using the Monitoring Console and the Splunk Chargeback app

Module 4 – Use Configuration Files

- Describe Splunk configuration directory structure
- Explore the configuration layering process
  - Index time process
  - Search time process
- Use Splunk tools to examine configuration settings such as btool

Module 5 – Use Apps

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

Module 6 – Create Indexes

- Describe how Splunk indexes function
- Identify the types of index buckets
- Create and work with indexes
- Describe metrics indexes

Module 7 – Manage Indexes

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the fishbucket
- Restore a frozen bucket

Module 8 – Manage Users

- Describe user roles in Splunk
- Add Splunk users using native authentication
- Create a custom role
- Manage users in Splunk

Module 9 – Configure Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the agent management

Module 10 – Configure Distributed Search

- Configure distributed search
- Define the roles of the search head and search peers
- Use Monitoring Console to monitor search activity
- Explain when and how to quarantine search peers
- Identify options and considerations for using multiple search heads
- Identify distributed search recommended practices
- Explain the use cases for Federated Search and how it is configured

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email splunk_training@cisco.com.