

Splunk OverDrive

Course ID: SOD1802



Course Description

This training covers how together, Splunk and Cisco, enable organizations to realize the potential of Operational Intelligence across the organization and gain real-time business insights that create a strategic advantage. We will cover how Splunk software scales to collect and index hundreds of terabytes of data per day, across multi-geography, multi-data center and cloud-based infrastructures. Using Cisco's Unified Computing System (UCS) Integrated Infrastructure for Big Data offers linear scalability along with operation simplification for single-rack and multiple-rack deployments. To facilitate faster and more predictable deployments, Cisco has published multiple reference architectures for Splunk software plus a comprehensive Cisco Validated Design that provides prescriptive, step-by-step guidance for deploying Splunk Enterprise on Cisco UCS.

Learning Objectives

- + Harnessing the power of your machine data enables you to make decisions based on facts, not intuition or best guesses.
- + Reduce the time you spend investigating incidents by up to 90%!
- + Find and fix problems faster by learning new technical skills for real world scenarios.
- + Get started with Splunk Enterprise, from installation and data onboarding to running search queries to creating simple reports and dashboards
- + Accelerate time to value with turnkey Splunk integrations for dozens of Cisco products and platforms
- + Ensure faster, more predictable Splunk deployments with a proven Cisco Validated Design and the latest Cisco UCS server

Who Should Attend

- + Network Engineers
- + Support Engineers
- + Wireless Engineers
- + Field Engineers

Prerequisites

- + Familiarity with Cisco products

Splunk OverDrive

(1 Day)

Course Content

Module 1: Cisco Integrated Infrastructure for Big Data and Splunk

- + What is Cisco CPA (v4)
- + Architecture benefits for Splunk
- + Components of IIBD and relationship to Splunk architecture
- + Cisco UCS Integrated Infrastructure for Big Data with Splunk Enterprise
- + Splunk – Big Data Analytics: Solution Overview
- + NFS Configurations for the Splunk Frozen Data Storage
- + NFS Client Configurations on the Indexers

Module 2: Splunk - Start Searching

- + Introduce Splunk and the Search app
- + Run basic searches
- + Identify the contents of search results
- + Control a search job
- + Set the time range of a search
- + Use the output of a search to refine your search

Module 3 Saving Results and Searches

- + Export search results
- + Save and share search results
- + Save searches
- + Schedule searches

Module 4: Splunk – Fields, Tag, and Events

- + Understand fields
- + Use fields in searches
- + Use the fields sidebar
- + Understand tags
- + Create tags and use tags in a search
- + Describe event types and their uses
- + Create and use event types in a search

Module 5: Splunk - Creating Alerts and Reports

- + Describe alerts
- + Create an alert
- + View fired alerts
- + Create reports and charts
- + Create dashboards and add reports
- + Create and edit dashboards

Module 6: Intro to Splunk Apps for Cisco

- + Cisco UCS Data In Splunk
- + Cisco Integrations with Splunk

Module 7: UCS Director Express for Big Data

- + Splunk Deployment with UCSDE for Big Data
- + Splunk Management with UCSDE for Big Data
- + Creating a Splunk Cluster with UCSDE for Big Data

Lab 1: Installing and Navigating Splunk

Lab 2: Importing Data into Splunk

Lab 3: Exploring Search Views in Splunk

Lab 4: Basic Searches and Search Results

Lab 5: Field Lookups and Events

Lab 6: Creating Reports and Charts

Lab 7: Creating Dashboard

Lab 8: Cisco UCS and Splunk Integration

Lab 9: Cisco ACI (or maybe IOS) and Splunk Integration

Lab 10: UCS Director Express for Big Data – Splunk Deployment



**Where Technology
Means More®**

**To register for an ePlus cloud
training course, contact us
today.**

Call: 888.482.1122

Email: CloudServices@eplus.com

Web: www.eplus.com/cloud