SP-SCA - Splunk Cloud Administration

Hours: 18

Prerequisites: Students should understand Intro to Splunk, Using Fields, Intro to Knowledge Objects, Creating Knowledge Objects, and Creating Field Extractions or possess equivalent experience.

Audience: New Splunk Cloud administrators and technical professionals responsible for users, data ingestion, configuration, monitoring, and support in a Splunk Cloud environment.

Description: This 18-hour hands-on course prepares new Splunk administrators to manage users and ingest data in Splunk Cloud. Students configure inputs and forwarders, manage indexes and user access, tune event processing, install applications, and apply monitoring and troubleshooting practices that support a productive Splunk SaaS deployment.

Course Objectives: Upon completion of this course, students will:

- Describe Splunk Cloud topology and cloud-administrator responsibilities.
- Manage indexes, retention, user authentication, authorization, and configuration files.
- Configure cloud ingestion with forwarders, APIs, scripted inputs, HEC, and applications.
- Fine-tune inputs and validate event parsing with Data Preview.
- Transform raw data and manage applications and add-ons.
- Use monitoring, diagnostics, and Splunk Cloud Support resources to isolate problems.

OUTLINE:

MODULE 1: SPLUNK CLOUD OVERVIEW

- Cloud topology and administrator responsibilities
- Splunk Cloud versus Splunk Enterprise
- Self-Service Cloud versus Managed Cloud

MODULE 2: INDEX MANAGEMENT

- Define and create indexes
- Delete data
- Monitor indexing activity

MODULE 3: USER AUTHENTICATION AND AUTHORIZATION

- Administer users and roles
- Integrate LDAP, Active Directory, or SAML

MODULE 4: SPLUNK CONFIGURATION FILES

- Files, directories, and precedence
- Index-time and search-time processes

MODULE 5: CLOUD INGESTION USING FORWARDERS

- Cloud ingestion strategies
- Forwarders in data ingestion
- Configure forwarding and monitor connectivity

MODULE 6: FORWARDER MANAGEMENT

- Deployment Server and forwarder management
- Deployment clients and deployment apps

MODULE 7: MONITOR INPUTS

- Splunk data-input process
- File and directory monitor inputs
- Optional monitor settings

MODULE 8: API, SCRIPTED, AND HEC INPUTS

- API ingestion
- Scripted inputs
- HTTP Event Collector ingestion

MODULE 9: APPLICATION-BASED INPUTS

- Inputs in apps and add-ons
- Splunk Stream
- Cloud inputs on an Inputs Data Manager

MODULE 10: FINE-TUNING INPUTS

- Default input-phase processing
- Sourcetype tuning and character encoding

MODULE 11: PARSING AND DATA PREVIEW

- Parsing-phase processing
- Event line breaking
- Timestamps and time zones
- Validate event creation with Data Preview

MODULE 12: MANIPULATING RAW DATA

- Data transformations
- props.conf and transforms.conf
- SEDCMD

MODULE 13: INSTALLING AND MANAGING APPS

- App and add-on vetting and installation
- Create apps to distribute configurations

MODULE 14: SUPPORT AND TROUBLESHOOTING

- Troubleshoot deployments

- Collect diagnostics and monitoring data
- Prepare relevant information for Splunk Cloud Support