Splunk 8.2 Cloud Administration Training

Course Outline

Module 1 – Splunk Cloud Overview

- Describe Cloud topology
- Describe tasks managed by the Splunk cloud administrator
- List the primary differences between Splunk Cloud and Splunk Enterprise
- List differences between Self-Service Cloud and Managed Cloud

Module 2 – Index Management

- Define a Splunk Index
- Create indexes in cloud
- Delete data from an index
- Monitor indexing activities

Module 3 – User Authentication and Authorization

- Administer Splunk user roles
- Integrate Splunk with LDAP, Active Directory, or SAML

Module 4 – Splunk Configuration Files

- Review Splunk Configuration files and directories
- Review configuration file precedence
- Review index and search time processes

Module 5 – Cloud Ingestion - Using Splunk Forwarders

- Review cloud ingestion strategies
- Understand the role of forwarders in GDI
- Configure forwarding to Splunk Cloud
- Monitoring forwarder connectivity
- Explore optional forwarder settings

Module 6 – Forwarder Management

- Describe Splunk Deployment Server
- Explain the use of forwarder management
- Configure forwarders to be deployment clients
- Managing forwarders using deployment apps

Module 7 – Monitor Inputs

- Describe the Splunk process for inputting data
- Create file and directory monitor inputs
- Use optional settings for monitor inputs

Module 8 – Cloud Ingestion - Using API, Scripted and HEC Inputs

- Understand how data is ingested using API
- Know how to deploy scripted inputs
- Describe how to use HEC for ingestion

Module 9 – Cloud Ingestion - Application Based Inputs

- Understand how inputs are managed using in apps or add-ons
- Describe how customers may use Splunk Stream app
- Deploy Cloud inputs for use on an IDM

Module 10 – Fine-tuning inputs

- Describe the default processing that occurs during the input phase
- Configure input phase options, such as sourcetype fine-tuning and character set encoding

Module 11 – Parsing Phase and Data Preview

- Describe the default processing that occurs during parsing
- Optimize and configure event line breaking
- Explain how timestamps and time zones are extracted or assigned to events
- Use Data Preview to validate event creation during the parsing phase

Module 12 – Manipulating Raw Data

- Explain how data transformations are defined and invoked
- Use transformations with props.conf and transforms.conf to modify raw data
- Use SEDCMD to modify raw data

Module 13 – Installing and Managing Apps

- Understand how apps and add-ons are vetted and installed in Cloud
- Create apps to managing and distribute configurations

Module 14 – Splunk Cloud Support and Troubleshooting

- Troubleshooting Splunk deployments
- Collecting data and use diagnostics or monitoring to investigate
- Overview of how to submit requests with the relevant data for support to troubleshoot

Appendix Explore diagnostic tools and isolation troubleshooting used to investigate and solve issues