Transitioning to Splunk Cloud

Course Description:

This course is for experienced on-prem administrators and anyone needing to ramp-up on Splunk Cloud to get more knowledge and experience of managing Splunk Cloud instances.

The course discusses the differentiators between on-prem Splunk and the different Splunk Cloud offerings. Modules include topics on how to migrate data collection and ingest from on-prem Splunk to Splunk Cloud as well as highlighting Splunk Cloud specific differences and best practices to manage a productive Splunk SaaS deployment. For Splunk Administrators who have undertaken the System and Data Administration learning pathways, this course highlights key differences between Splunk Enterprise deployed on-premises and Splunk Enterprise Cloud to allow them to ramp up their data and system management skills to transition to Splunk Cloud. The hands-on lab provides access to and experience of managing a Splunk Cloud instance.

Note: Splunk Cloud Administration and Transitioning to Splunk Cloud SHOULD NOT be taken together as both are designed to develop Splunk Cloud-specific skills and as such there is some overlap.

Course Duration:

2 Days

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

Additional courses and/or knowledge in these areas are also highly recommended:

- Enriching Data with Lookups
- Data Models

Course Outlines:

Module 1 – Splunk Cloud Overview

- Describe Splunk and Splunk Cloud features and topology
- Identify Splunk Cloud administrator tasks
- Describe Splunk Cloud purchasing options and differences between Classic and Victoria experience
- Secure Splunk deployments best practices
- Explain Splunk Cloud data ingestion strategies

Module 2 – Splunk Cloud Migration

- Understand the Splunk Cloud migration journey
- Determine Splunk Cloud migration readiness
- Identify Splunk Cloud migration preparation tasks, strategies, and possible challenges

Module 3 – Managing Users

- Identify Splunk Cloud authentication options
- Add Splunk users using native authentication
- Create a custom role
- Integrate Splunk with LDAP, Active Directory or SAML
- Use Workload Management to manage user resource usage
- Manage users in Splunk

Module 4 – Managing Indexes

- Understand cloud indexing strategy
- Define and create indexes
- Manage data retention and archiving
- Delete and mask data from an index
- Monitor indexing activities

Module 5 – Managing Apps

- Review the process for installing apps
- Define the purpose of private apps
- Upload private apps
- Describe how apps are managed

Module 6 – Configuring Forwarders

- List Splunk forwarder types
- Understand the role of forwarders
- Configure a forwarder to send data to Splunk Cloud
- Test the forwarder connection
- Describe optional forwarder settings

Module 7 – Common Inputs

- Describe forwarder inputs such as files and directories
- Create REST API inputs
- Create a basic scripted input
- Create Splunk HTTP Event Collector (HEC) agentless inputs

Module 8 – Additional Inputs

- Understand how inputs are managed using apps or add-ons
- Explore Cloud inputs using Splunk Connect for Syslog, Data Manager, Inputs Data Manager (IDM), Splunk Edge Processor, and Splunk Edge Hub

Module 9 – Using Ingest Actions

- Explore Splunk transformation methods
- Create and manage rulesets with Ingest Actions
- Mask, filter and route data with Ingest Action rules

Module 10 – Managing Splunk Cloud

- Secure ingest with Splunk Cloud Private Connectivity with AWS
- Describe Federated Search functionality
- Describe Splunk connected experience apps such as Splunk Secure Gateway
- Monitor and manage resource utilization by business units and users using Splunk App for Chargeback
- Perform self-service administrative tasks in Splunk Cloud using the Admin Config Service

Module 11 – Supporting Splunk Cloud

- Know how to isolate problems before contacting Splunk Cloud Support
- Use Isolation Troubleshooting
- Define the process for engaging Splunk Support

Target Audience:

- Splunk Enterprise Administrators