Splunk Cloud Administration

Course Description:

This course is for administrators new to Splunk Cloud and those wanting to become more experienced in managing Splunk Cloud instances.

The course provides administrators with the opportunity to gain the skills, knowledge and best practices for data management and system configuration for data collection and ingestion required in a Splunk Cloud environment to create a productive Splunk SaaS deployment. The hands-on labs provide the opportunity to learn and ask questions on how to manage and maintain the platform, the users and how to effectively get data into Splunk Cloud. Modules include data inputs and forwarder configuration, data management, user accounts, and basic monitoring and problem isolation.

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

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 – 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 3 – 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 4 – Using Configuration Files

- Describe Splunk configuration directory structure
- Describe the configuration layering process with index and search time precedence
- Use Splunk tools to examine configuration settings such as btool

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 – Managing Forwarders

- Describe Splunk Deployment Server (DS)
- Manage forwarders using deployment apps
- Configure deployment clients and client groups
- Monitor forwarder management activities

Module 8 – Forwarder Inputs

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

Module 9 – Common Inputs

- Create REST API inputs
- Create a basic scripted input
- Identify Linux-specific inputs
- Identify Windows-specific inputs
- Create Splunk HTTP Event Collector (HEC) agentless inputs

Module 10 – 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 11 – Fine-tuning Inputs

- Describe the default processing that occurs during the input phase
- Configure input phase options, such as source type fine-tuning and character set encoding
- Reset file check pointers on a forwarder using the btprobe command

Module 12 – Parsing Phase and Data Preview

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

Module 13 – Manipulating Input Data

- Explore Splunk transformation methods
- Mask, filter and route data with SEDCMD and TRANSFORMS
- Override sourcetype or host based upon event values
- Create and manage rulesets with Ingest Actions
- Mask, filter and route data with Ingest Action rules

Module 14 – 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 15 – 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 Cloud Administrators