Transitioning to Splunk Cloud

This 9-hour virtual 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 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 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 Topics

- Splunk Cloud overview and migration
- Managing user authentication and authorization in Splunk
- Managing Splunk indexes
- Configuring Splunk forwarders for Cloud
- Configuring inputs to Cloud, including API, Scripted, HEC and Application based inputs
- Exploring GDI performance considerations
- Installing and managing applications
- Problem isolation and working with Splunk Cloud support

Prerequisite Knowledge

To be successful, students should have a working knowledge of the topics covered in the following courses:

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

Course Format

Instructor-led lecture with labs, delivered via virtual classroom, or at your site.

Course Objectives

Module 1 – Splunk Cloud Overview

- Describe Splunk Cloud features and topology
- Identify Splunk Cloud administrator managed tasks
- Explain the differences between Splunk Enterprise on-premise and 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
- Integrate Splunk with LDAP, Active Directory or SAML
- Create a custom role
- Manage users in Splunk
- Use Workload Management to manage user resource usage

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 – 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 6 –API, Scripted and HEC Inputs

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

Module 7 – Application Based Inputs

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

Module 8 – GDI Performance Considerations

- 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
- Explain how data transformations are defined and invoked

Module 9 – Installing and Managing Apps

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

Module 10 – Managing Splunk Cloud

- 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
- Improve Mean Time to Resolution (MTTR) by using clear communication, diagnostic tools, monitoring and the CMC

Appendix

Explore Splunk security fundamentals

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales