Transitioning to Splunk Cloud

Category: AI, Data & Analytics | **Vendor:** Splunk

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course is for 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 toSplunk 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.

Please note that this course may run over two days, with 4.5 hour sessions each day.

About This Course

This course is for 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 toSplunk 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.

Please note that this course may run over two days, with 4.5 hour sessions each day.

Who Should Attend

Splunk Enterprise Administrators

Prerequisites & Entry Requirements

General Prerequisites:

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

- What is Splunk?
- Intro to Splunk
- Using Fields (SUF)
- Intro to Knowledge Objects
- Creating Knowledge Objects (CKO)
- Creating Field Extractions (CFE)
- Splunk Enterprise System Administration (SESA)
- Splunk Enterprise Data Administration (SEDA)

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

- Basic understanding of common operating systems such as Linux
- Enriching Data with Lookups (EDL)
- Data Models (SDM)

Detailed Course Outline

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
- 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 – 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), and Splunk Edge Processor

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

Appendix

- Explore Splunk security fundamentals

Frequently Asked Questions

Q: What delivery options are available for Transitioning to Splunk Cloud?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day Transitioning to Splunk Cloud course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Transitioning to Splunk Cloud training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Transitioning to Splunk Cloud?

Yes, we provide corporate training, dedicated training, and closed classes for Transitioning to Splunk Cloud. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Transitioning to Splunk Cloud, Splunk Cloud Administrator, TSC

Q: Why choose Nexus Human for Transitioning to Splunk Cloud?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Transitioning to Splunk Cloud training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)