splunk>

Splunk Cloud Administration

This 3-day hands-on course prepares administrators to manage users and get data in Splunk Cloud. Topics include data inputs and forwarder configuration, data management, user accounts, and basic monitoring and problem isolation. The focus in this class is the knowledge, best practices, and configuration details for Splunk Cloud.

*Search head clustered deployment topics will NOT be covered in this class.

Course Topics

- Splunk Cloud overview
- Splunk index management
- Users, roles, and authentication
- Universal forwarder
- Forwarder management
- Data inputs in detail
- Event Parsing with data preview
- Manipulating raw data
- Installing apps
- Problem isolation and Splunk Cloud support

Course Prerequisites

Required:

- Splunk Fundamentals 1

Strongly Recommended:

- Splunk Fundamentals 2

Class Format

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

Course Modules

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

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
- Enable Duo security Multi Factor Authentication (MFA)

Module 4 – Getting Data in

- List Splunk input options
- Describe the basic settings for an input
- Review Splunk configuration files
- Use a test environment to verify data

Module 5 – Getting Data in Cloud

- List Splunk forwarder types
- Describe the role of forwarders
- Configure a forwarder to Splunk Cloud
- Test the forwarder connection
- Describe 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 – Network and Other Inputs

- Create network (TCP and UDP) inputs
- Create a basic scripted input
- Describe optional settings for network inputs
- Identify Windows input types and uses
- Use the HTTP Event Collector (HEC) to get data into Splunk

Module 9 – 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 10 – 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 11 – Manipulating Raw Data

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

Module 12 – Installing and Managing Apps

- Describe self-service app installs vs. manual app installs
- Provide steps to install apps
- Describe how apps are managed

Module 13 – Working with Splunk Cloud Support

- Isolate problems before contacting Splunk Cloud Support
- Define the process for working with Splunk Cloud Support

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

To contact us, email Education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.
Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
270 Brannan St.
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com