SPLUNK EDUCATION

Course Description

MASTERING SPLUNK DATA MANAGEMENT TECHNIQUES

Summary

This course is for experienced Splunk administrators.

Every organization opting to use Splunk needs to understand the best way to ingest data from various sources. While the most direct route to the Splunk indexers is best for the success of any Splunk deployment, in an environment where data creation is skyrocketing, you must consider intermediate-forwarding solutions to meet your unique business challenges. This Instructor-led course (four-days, 4.5 hours each) is designed for those with foundational knowledge in Splunk data administration who wish to deepen their expertise. It focuses on technical skills related to data management processes and will benefit professionals involved in designing, building, and optimizing Splunk data ingestion pipelines.

Note: The topics covered in this course apply to hybrid environments spanning Splunk Enterprise, Splunk Cloud, and other non-Splunk storage options.

Prerequisites

To be successful, you must the following prerequisites:

- On-the-job experience managing Splunk deployments including:
  - Splunk ingestion pipelines
  - Splunk troubleshooting methodologies
- Completed the following course:
  - Splunk Cloud Administration, OR
  - Splunk System Administration and Splunk Data Administration

Format: Instructor-led with exercise labs

Instructor-led Duration: 18 Hours

Audience: Splunk Administrators

Course Outline

Module 1 – Splunk Data Processing Introduction

- Review and discuss the classic Splunk GDI architecture
  - Highlight the benefits and the implementation parameters
  - Explain how Splunk ingestion pipeline scales
- Understand the role of Splunk data ingestion processing solutions
  - List the data flow attributes in inputs.conf and outputs.conf

Module 2 – Data Processing with Intermediate Forwarders

- List the benefits and challenges of processing data at the edge
- Deploy and manage intermediate forwarders
- Use classic parsing techniques to transform events
  - Explore strategies for optimizing data flow

Module 3 – Data Processing with Ingest Actions

- Set up Ingest Actions in your environment

- Create pipeline rulesets with Ingest Actions
- Understand the underlying conf file attributes
- Manage and deploy ingest Actions rulesets

Module 4 – Data Processing with Edge Processor

- Describe what Edge Processor is and how it works
- Configure the Edge Processor control plane
    - Set up data sources and destinations
- Deploy and manage Edge Processor instances
- Use SPL2 for ingest pipeline authoring and deployment
    - Masking, filtering, enriching and routing of data
- Monitor data plane health using the control plane UI

Module 5 – Data Processing with Ingest Processor

- Describe what Ingest Processor is and how it works
- List the differences between Edge Processor and Ingest Processor
- Use SPL2 for ingest pipeline authoring and deployment
- Convert a log source into metrics and route them to Splunk Observability Cloud
- Monitor data plane health of Ingest processor pipelines

Module 6 – Data Management Solution Integration

- Identify the best practices for using Splunk ingestion solutions
- Understand how different pipelines work together in Splunk
- Identify critical events in the logs for troubleshooting
- List the steps to decommission Data Management Experience pipelines

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.