



# Implementing Splunk Data Stream Processor (DSP)

This 4-day course is designed for the experienced Splunk administrators who are new to Splunk DSP. This hands-on class provides the fundamentals of deploying a Splunk DSP cluster and designing pipelines for core use cases. It covers installation, source and sink configurations, pipeline design and backup, and monitoring a DSP environment.

## Course Topics

- Introduction to Splunk DSP
- Deploying a DSP cluster
- Prepping Sources and Sinks
- Building Pipelines - Basics
- Building Pipelines - Deep Dive
- Working with 3rd party Data Feeds
- Working with Metric Data
- Monitoring DSP Environment

## Course Prerequisites

Required:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

Nice to have:

- Architecting Splunk Enterprise Deployments
- Working knowledge of Apache Kafka (user level), Apache Flink (user level), and Kubernetes (admin level)

## Class Format

This course is an instructor-led lecture with labs, delivered via virtual classroom or at your site. The lab environment is Linux only.

### Important:

Students must be able to access SSH on port 22 and HTTPS on port 30000, 30002, and 31000 from his or her computer.

## Course Modules

### Module 1 – Introduction to DSP

- Review Splunk deployment options and challenges
- Describe the purpose and value of Splunk DSP
- Define DSP concepts and terminologies

### Module 2 – Deploying a DSP Cluster

- List DSP core components and system requirements
- Describe installation options and steps
- Check DSP service status
- Learn to navigate in DSP UI
- Use scloud

### Module 3 – Prepping Sources and Sinks

- Ingest data with DSP REST API service
- Configure DSP source connections for Splunk data
- Configure DSP sink connections for Splunk indexers
- Create Splunk-to-Splunk pass-through pipelines

### Module 4 – Building Pipelines - Basics

- Describe the basic elements of a DSP pipeline

- Create data pipelines with the DSP canvas and SPL2
- List DSP pipeline commands
- Use scalar functions to convert data types and schema
- Filter and route data to multiple sinks

### Module 5 – Building Pipelines - Deep Dive

- Manipulate pipeline options:
  - Extract
  - Transform
  - Obfuscate
  - Aggregate and conditional trigger

### Module 6 – Working with 3rd party Data Feeds

- Read from and write data to pub-sub systems like Kafka
- List sources supported with the collect service
- Transform data from Kafka and normalize
- Write to S3

### Module 7 – Working with Metric Data

- Onboard metric data into DSP
- Transform metric data for Splunk indexers and SignalFx
- Send metric data to Splunk indexers
- Send metric data to Splunk SignalFx

### Module 8 – Monitoring DSP Environment

- Back up DSP pipelines
- Monitor DSP environment
- Describe steps to isolate DSP service issues
- Scale DSP
- Replace DSP master node
- Upgrade DSP cluster

## 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](mailto: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](http://www.splunk.com) to download your own free copy.

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