Splunk Enterprise Data Administration

This 3 virtual day course is designed for system administrators who are responsible for getting data into Splunk Indexers. The course provides the fundamental knowledge of Splunk forwarders and methods to get remote data into Splunk indexers. It covers installation, configuration, management, monitoring, and troubleshooting of Splunk forwarders and Splunk Deployment Server components.

Course Topics

- Deploy forwarders with Forwarder Management
- Splunk Configuration Files
- Configure common Splunk data inputs
- Customize the input parsing process

Course Prerequisites

Required:

- Splunk Fundamentals 1

Strongly Recommended:

- Splunk Fundamentals 2
- Splunk Enterprise 6.6 System Administration

Class Format

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

Course Modules

Module 1 – Introduction to Data Administration

- Splunk overview
- Identify Splunk data administrator role

Module 2 – Getting Data In – Staging

- List the four phases of Splunk Index
- List Splunk input options
- Describe the band settings for an input

Module 3 – Configuring Forwarders

- Understand the role of production Indexers and Forwarders
- Understand the functionality of Universal Forwarders and Heavy Forwarders
- Configure Forwarders
- Identify additional Forwarder options

Module 4 – Forwarder Management

- Explain the use of Forwarder Management
- Describe Splunk Deployment Server
- Manage forwarders using deployment apps
- Configure deployment clients
- Configure client groups
- Monitor forwarder management activities

Module 5 – Monitor Inputs

- Create file and directory monitor inputs
- Use optional settings for monitor inputs
- Deploy a remote monitor input

Module 6 – Network and Scripted Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs
- Create a basic scripted input

Module 7 – Agentless Inputs

- Identify Windows input types and uses
- Understand additional options to get data into Splunk
  HTTP Event Collector
  Splunk App for Stream

Module 8 – Fine Tuning Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options, such as sourcetype fine-tuning and character set encoding

Module 9 – Parsing Phase and Data

- Understand 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 10 – Manipulating Raw Data

- Explain how data transformations are defined and invoked
- Use transformations with props.conf and transforms.conf to:
  Mask or delete raw data as it is being indexed
  Override sourcetype or host based upon event values
  Route events to specific indexes based on event content
  Prevent unwanted events from being indexed
- Use SEDCMD to modify raw data

Module 11 – Supporting Knowledge Objects

- Create field extractions
- Configure collections for KV Store
- Manage Knowledge Object permissions
- Control automatic field extraction

Module 11 – Creating a Diag

- Identify Splunk diag
- Using Splunk diag

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

splunk>

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
San Francisco, CA
94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com